ZBORNIK RADOVA

5. MEĐUNARODNE ZNANSTVENO-STRUČNE KONFERENCIJE -
Istraživački dani Visoke policijske škole u Zagrebu
Unaprjeđivanje sigurnosne uloge policije primjenom novih tehnologija i metoda
Zagreb, Hrvatska, 21. - 22. travnja 2016.

PROCEEDINGS

OF THE 5TH INTERNATIONAL SCIENTIFIC AND PROFESSIONAL CONFERENCE
The Police College Research Days in Zagreb
New Technologies and Methods Used for Improvement of the Police Role in Security Matters
Zagreb, Croatia, 21-22 April 2016

Visoka policijska škola u Zagrebu
Police College, Zagreb
Zagreb, 2016.

Nakladnik/Publisher
Ministarstvo unutarnjih poslova Republike Hrvatske, Policijska akademija /
Ministry of the Interior of the Republic of Croatia, Police Academy

Za nakladnika/On behalf of the Publisher
Želimir Radmilović

Urednici/ Editors
Joško Vukosav
Ksenija Butorac
Joško Sindik

Lektorice/Language Consultants
Gabrijela Gorše
Antonija Rakuljić
Slava Rosandić

Priprema i tisak/Design and printing
Služba za razvoj policijskog obrazovanja i nakladničko-knjižničnu djelatnost
Service for Development of Police Education and Publishing

ISBN 978-953-161-299-9

5TH INTERNATIONAL SCIENTIFIC AND PROFESSIONAL CONFERENCE
'POLICE COLLEGE RESEARCH DAYS IN ZAGREB'
New Technologies and Methods Used for Improvement of the Police Role in Security Matters
ZAGREB, CROATIA
21-22 April 2016

PROGRAMME COMMITTEE

Chair

Assist. Prof. Joško Vukosav, Dean of the Police College, Police Academy, MoI, Zagreb, Croatia

Members

Zvonimir Vnučec, General Police Director, Ministry of the Interior, Zagreb, Croatia

Krunoslav Borovec, PhD, Assistant General Police Director, Ministry of the Interior, Zagreb, Croatia

Želimir Radmilović, Head of the Police Academy, Ministry of the Interior, Zagreb, Croatia

Zvonimir Dujmović, PhD, Assistant Head of the Police Academy, Ministry of the Interior, Zagreb, Croatia

Full Prof. Kimmo Himberg, Police University College, Tampere, Finland

Full Prof. Thorsten Heyer, Police College, Wiesbaden, Germany

Full Prof. Gorazd Meško, Faculty of Criminal Justice and Security, University of Maribor, Ljubljana, Slovenia

Full Prof. Nihad Bunar, Stockholm University, Sweden

Full Prof. Oliver Baćanović, Faculty of Security, Skopje, Macedonia

Full Prof. Zoran Đurđević, The Academy of Criminalistics and Police Studies, Belgrade-Zemun, Serbia

Full Prof. Nedžad Korajlić, Faculty for Criminalistics, Criminology and Security Studies, University of Sarajevo, Bosnia and Herzegovina

Assoc. Prof. Eduardo Manuel Ferreira, Escola de Polícia Judiciária, Loures, Portugal

Assoc. Prof. Gabor Kovacz, National University for Public Service, Budapest, Hungary

Assoc. Prof. Želimir Kešetović, Faculty of Security Studies, University of Belgrade, Serbia

Assist. Prof. Mile Šikman, Department for Police Education, Ministry of Interior, Banja Luka, Republic Srpska

Robert Šumi, PhD, Center for Research and Social Skills, Police Academy, Ministry of the Interior, Ljubljana, Slovenia

Full Prof. Petar Veić, Faculty of Law, University of Rijeka, Croatia

Full Prof. Predrag Zarevski, Faculty of Humanities and Social Sciences, University of Zagreb, Croatia

Full Prof. Ljiljana Mikšaj Todorović, Faculty of Education and Rehabilitation Sciences, University of Zagreb, Croatia

Full Prof. Duško Modly, Zagreb, Croatia

Assist. Prof. Predrag Pale, Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia

Assist. Prof. Tihomir Katulić, Faculty of Law, University of Zagreb, Croatia

Assoc. Prof. Irena Cajner Mraović, Centre for Croatian Studies, University of Zagreb, Croatia

Assist. Prof. Anna-Maria Getoš Kalac, Faculty of Law, University of Zagreb, Croatia

Assist. Prof. Joško Sindik, Institute for Anthropological Research, Zagreb, Croatia

Assoc. Prof. Ksenija Butorac, Police College, Zagreb, Croatia

Assoc. Prof. Krunoslav Antoliš, Police College, Zagreb, Croatia

Assist. Prof. Željko Karas, Police College, Zagreb, Croatia

Assist. Prof. Josip Pavliček, Police College, Zagreb, Croatia

Stjepan Gluščić, PhD, Police College, Zagreb, Croatia

Ante Orlović, PhD, Police College, Zagreb, Croatia

ORGANISING COMMITTEE

Chair
Davor Štrk, MSc, Police College, Zagreb, Croatia

Members
Davorka Martinjak, PhD, Police College, Zagreb, Croatia
Ruža Karlović, PhD, Police College, Zagreb, Croatia
Lana Milivojević, PhD, Police College, Zagreb, Croatia
Davor Solomun, MSc, Police College, Zagreb, Croatia
Renata Odeljan, MSc, Police College, Zagreb, Croatia
Hrvoje Filipović, MSc, Police College, Zagreb, Croatia
Nikola Protrka, Police College, Zagreb, Croatia
Damir Maračić, Police College, Zagreb, Croatia
Izidora Radek, Police College, Zagreb, Croatia
Marina Heski, M.A., Police College, Zagreb, Croatia
Nikša Jelovčić, M.A., Police Academy, Zagreb, Croatia

SADRŽAJ/TABLE OF CONTENTS

Predgovor **10**

Foreword **11**

Policijski procesi – nove tehnologije i policijsko obrazovanje / Police Work – New Technologies and Police Training **12**

Daniel James, Mark van der Giessen, Petra Saskia Bayerl, Gabriele Jacobs, Ruža Karlović, Garik Markarian: Concept development of ICT tools and applications within the Unity Project 13

Nikolina Grbić Prprović: Specifičnosti saslušanja djece i maloljetnika oštećenih krivičnim djelom 32

Josip Medved, Ante Orlović, Jure Tadić: Sigurnost cestovnog prometa primjena suvremene tehnologije i metoda u preventivno-represivnom djelovanju prometne policije 43

Davor Labaš, Krešimir Filipić: Kriminalistička istraživanja provalnih krađa u dom - mogućnosti procesnog pristupa upravljanja rizikom 58

Tanja Kaurin, Zdravko Skakavac: Značaj digitalne forenzike mobilnih uređaja u otkrivanju i dokazivanju krivičnih djela organizovanog kriminaliteta 75

Ksenija Butorac, Irena Cajner Mraović, Hrvoje Filipović: Učinkovitost video nadzora u smanjenju kriminaliteta – pregled istraživanja 100

Vladica Babić, Zdravko Skakavac: Sustavi nadzora suvremenih tehničkih sredstava i njihova učinkovitost 114

Alen Sambolec, Davor Solomun: IMINT i zrakoplovna tehnologija prikupljanja podataka i sigurnosnog djelovanja 124

Davorka Martinjak, Anita Matijević, Renata Odeljan : Obrazac za procjenu rizika od ponavljanja nasilničkog ponašanja u obitelji 150

Spomenko Relić: Uspoređivanje kontakata mobilnih uređaja ostvarenih preko ćelija baznih stanica 164

Mladen Vuković: Značaj i uloga mobilnih telefona prilikom rasvjetljavanja krivičnih djela 184

Krunoslav Borovec, Iva Balgač: Uvođenje policijskih kamera u rad službe policijske ophodnje – otvorena pitanja uspješne implementacije i egzaktne procjene učinka na rad policije 193

Zlatko Kovač, Nikola Protrka: Računalna analiza ljudskog glasa i govora 210

Goran Guska, Goran Blagojević: Savremeni metodi i sredstva u suprotstavljanju zloupotrebi platnih kartica 227

Igor Špoljarić, Ante Orlović, Gordan Mršić: Implementacija visoke tehnologije u forenzično-kriminalističkim istraživanjima – skenirajući elektronski mikroskop (stanje i perspektive) 242

Žarko Ćulibrk: Značaj visokih tehnologija i uloga policije u upravljanju vanrednim situacijama – faza informisanja 257

Davorka Martinjak, Danko Salopek, Renata Odeljan, Suzana Kikić: Doprinos otvorenih izvora na internetu i suvremenih informacijsko-komunikacijskih tehnologija u pronalaženju nestale djece 264

Vladimir Pivovarov, Marijan Nikolovski: Securing the Crime Scene – A Prerequisite for Successful Crime Scene Investigation 281

Mile Matijević, Aleksandar Miladinović: Kriminalistički aspekt Facebook-a 287

Joško Vukosav, Joško Sindik, Ivana Glavina Jelaš: Ličnost počinitelja nasilničkog i nenasilničkog kriminaliteta 300

Ruža Karlović, Danijela Petković, Karla Kiš Kamenjarin – Stavovi policijskih službenika o uvođenju novih tehnologija u policijskirad 313

Marina Malish Sazdovska: Application of New Software Solutions In Criminal Investigation 324

Robert Eberherr: E-Learning in the Bavarian Police – The Perspective of Further Education 338

Vesna Trajkovska: Use of the EU Legal Acts on Combating Cybercrime in Teaching English Vocabulary to Law Enforcement Students 349

Gabor Kovač: Common Public Service Excercise at the National University of Public Service 363

Ivica Labazan, Ivančica Varjačić, Joško Sindik, Martin Kolonić, Dejan Pastorčić: Stavovi policijskih službenika – studenata o stručnosti, kontroli, odlučivanju i rukovoditeljima 373

Snežana Mojsoska, Nikola Dujovski, Elena Dimovska: Concept of e-Police and e-Policing Services as a Part of e-Government: Future Development in the Republic of Macedonia 386

Policijski procesi – nove tehnologije, sigurnost i pravo/ Police work- new technologies, security and law 392

Stjepan Gluščić, Lana Milivojević: Uređenje instituta neovisnosti i učinkovitosti istrage i neovisnosti istražitelja u hrvatskom kaznenom postupku 393

Petar Veić, Igor Martinović: Izazovi policijskog postupanja u otkrivanju i dokazivanju računalnog kriminala..... 403

Snežana Nikodinovska-Stefanovska: EU's Data Protection Reform – Data Protection Challenges in the Field of Police and Law Enforcement 423

Damir Maračić: Web stranica European Judicial Network (EJN) kao pomoć pri uspostavi međunarodne pravosudne suradnje 435

Marjan Gjurovski, Lazar Gjurov:The Concept of Security of Critical Infrastructure in Terms of Risks and Crises 447

Prevencija kriminala – doprinos novih tehnologija/ Crime prevention - contribution of new technologies 455

Dragan Arlov, Milan Popović: Kvaliteta utvrđivanja opravdanosti i pravilnosti upotrebe sredstava prinude u funkciji jačanja odnosa policije i drugih građana 456

Željko Mršić: Uloga novih tehnologija i metoda u prevenciji kaznenih djela policijskih službenika..... 468

Gojko Pavlović: Suprotstavljanje sajber kriminalu u Evropskoj uniji u svjetlu Evropske bezbjednosne agende 495

Damir Kulišić: O aktualnim mogućnostima i problemima protueksplozijske detekcije i identifikacije eksplozivnih tvari/naprava 505

Darko Dundović: Neiskorištene mogućnosti privatnog sektora
u podizanju razine javne sigurnosti 533

Joško Sindik, Lucija Dodigović, Joško Vukosav: Predatorski
časopisi: sve veći problem znanstvene zajednice 545

**Nacionalna, urbana i računalna sigurnost – zaštita i sigurnost
podataka / National, Urban and Computer Security and
Data Protection 554**

Tihomir Šujster: Financiranje iz kriminalnog miljea, opasnost
za učinkovitost nacionalne sigurnosti 555

Matija Frčko, Davor Solomun: Unutarnja sigurnost Europske unije
u suvremenim uvjetima migracijske krize 566

Vojin Pilipović, Tanja Kaurin: Javnost u radu policije i zaštita
podataka o ličnosti 592

Ljubo Pejanović: Pretnje i zaštita informacionog sistema 610

Jure Tadić, Filip Dragović, Tonči Tadić: Migracijska i izbjeglička
kriza – sigurnosni rizici za EU 617

Tunjica Petrašević, Dunja Duić: Direktiva o evidenciji podataka
o putnicima (PNR) i zaštita podataka u EU 638

Dubravko Derk, Barbara Prprović, Nikolina Nemec: Utjecaj
aktualnih migracija na europsku sigurnost 653

Tatjana Gerginova: Role of Private Institutions for Security
in the National Security System 665

PREDGOVOR

Trend globalizacije i rapidnog razvoja tehnike, tehnologije i poslovnih procesa utemeljen je uglavnom na globalizaciji sustava vrijednosti. Ostvaruje se postupnim, neinvazivnim psihološkim pripremama i osvještavanjem građana, najčešće medijskim putem, ponajprije promicanjem važnih društvenih pravila, kao i sustava poželjnog i prihvatljivog ponašanja, kako bi se oni mogli osjećati sigurno i zaštićeno. Ovakav model, ponuđen kao novi oblik moći, može djelovati prirodno, a oni kojima je namijenjen ne trebaju ga osjećati nametnutim, već ga štoviše mogu doživjeti kao vlastiti slobodan izbor. S druge strane, virtualne tehnologije nadmašuju funkciju preventivnog utjecaja i normalizirajućeg modela društvene kontrole, a očituju se u aktivnim tehnikama nadziranja koje nadilaze standardnu „fizičku moć“ provođenja zakona.

S tehničkog i ekonomskog stajališta, može se ustvrditi da su suvremena tehničko-tehnološka rješenja postala isplativ i socijalno prihvatljiv instrument socijalnog inženjeringa, kao globalnog instrumenta prevencije kriminaliteta. Štoviše, funkcionalna snaga situacijske prevencije kriminaliteta podrazumijeva integrirano upravljanje situacijom, a tek potom ima funkciju kažnjavanja. Naime, današnjoj tehnologiji svojstvene su atribucije humanog odnosa i provođenja zakona, osobito u području zaštite ljudskih prava i osobnih podataka.

U okviru svoje sigurnosne uloge, policija se u svom svakodnevnom radu koristi brojnim strategijama, metodama i alatima, ovisno o konkretnom području svog djelovanja. U tom kontekstu, mijenjaju se i društveni odnosi, povećava interakcija s građanima i otvaraju novi komunikacijski kanali koji oblikuju inovativni pristup građanima, ovisno o nacionalnim, regionalnim i kulturalnim razlikama, te postojećim zakonodavnim rješenjima. Neki od primjera tehnološkog aspekta rada policije, zastupljenih i elaboriranih u ovom *Zborniku*, odnose se na korištenje nadzornih kamera, mobilne tehnologije, računalnih programa, društvenih mreža i drugih, sve u svrhu prevencije i kriminalističkog istraživanja niza kaznenih djela.

Stoga su policijska istraživanja usmjerena na proučavanje utjecaja društvenih i tehnoloških promjena, odnosno procesa modernizacije na policijski rad. Neka od njih bave se implementacijom novih vrsta informacija i komunikacijske tehnologije na svim ustrojstvenim razinama te načinom na koji utječu na policijsku kulturu i praksu. Druga se fokusiraju na tehnologije kontrole zbog rizičnog društva u kojemu živimo. Sve u svemu, radovi u ovom Zborniku razmatraju pozitivne i negativne aspekte uvođenja novih metoda, tehnika i tehnologija u radu policije. Oni upućuju na ključna područja evaluacije i istraživanja njihove učinkovitosti, u smislu povećanja sigurnosti građana, policijskog integriteta i legitimiteta te, općenito, dobrobiti društva u cjelini.

FOREWORD

The trend of globalization and of the rapid development of technics, technology and business processes is based mainly on the globalization of value systems. It is achieved by gradual, non-invasive psychological preparations and by raising awareness of citizens, usually through the media, primarily by promoting important social rules, as well as a system of desirable and acceptable behaviour, so they could feel safe and protected. This model, offered as a new form of power, can act naturally, and those for whom this model is intended for do not feel imposed by it, but can actually experience it as their own free choice. On the other hand, virtual technologies outweigh the function of preventive impact and of normalizing model of social control, and are reflected in the active surveillance techniques that go beyond the standard ‘physical power’ of law enforcement.

From a technical and economic point of view, it can be stated that modern technical and technological solutions have become viable and socially acceptable instrument of social engineering as a global instrument of crime prevention. Moreover, the functional power of situational crime prevention entails integrated management of the situation, while the function of punishment comes later. Namely, today's technology has an inherent attribution of human relations and law enforcement, particularly in the field of human rights and personal data protection

As a part of its security role, the police in their daily work use a number of strategies, methods and tools, depending on the particular area of their operations. In this context, social relations are changing, interaction with citizens is increased and new communication channels are being opened that are shaping an innovative approach to citizens, depending on national, regional and cultural differences and on existing legislative solutions. Some of the examples of the technological aspects of police work, elaborated and represented in this Proceedings book, refer to the usage of surveillance cameras, mobile technology, computer programmes, social networks and other, all with the purpose of prevention and crime investigation of a series of crimes.

Therefore, police researches are focused on studying the impact of social and technological changes that is the process of modernisation on police operations. Some of them deal with the implementation of new types of information and communication technologies on all organizational levels, and the ways in which they are affecting police culture and practice. Other researches are focused on control technologies due to the risky society we live in. Overall, the articles in this Proceedings book consider positive and negative aspects of introducing new methods, techniques and technologies in policing. They are referring to the key areas of evaluation and research, discussing their effectiveness, in terms of increasing the security of citizens, police integrity and legitimacy and, in general, the welfare of the entire society.

POLICIJSKI PROCESI – NOVE TEHNOLOGIJE I POLICIJSKO OBRAZOVANJE/ POLICE WORK - NEW TECHNOLOGIES AND POLICE TRAINING

RESEARCH PAPER

Daniel James[1]
Mark van der Giessen[2]
Petra Saskia Bayerl[3]
Gabriele Jacobs[4]
Ruža Karlović[5]
Garik Markarian[6]

CONCEPT DEVELOPMENT OF ICT TOOLS AND APPLICATIONS WITHIN THE UNITY PROJECT

Summary

Police forces are increasingly using mobile technologies for community policing (CP) purposes. In aiming to engage with citizens, the key concerns that need to be addressed in the design as well as in the practice of using mobile IT are the trust-building, information exchange, accountability and crime prevention. The Unity project uses key target areas of community policing identified during the project as focal points and key objectives.

The project aims at developing a novel approach that would enable efficient CP via a dedicated system utilising existing and emerging mobile technologies. The proposed system will be realised with generic architecture, allowing for adaptations to applications in various EU countries, taking into account the existing legal systems as well as regional and cultural differences. Several applications used both by citizens and police officers will be utilised to increase the level of interaction and open various new communication channels between the police and the community in a non-emergency environment. The application needs to take into account the requirements from both the police and citizens. For instance, a law enforcement application could receive, respond to, delegate and publish incident reports, while a citizen application could be used to provide incident reports with possible multimedia functions as well as to receive updates on incidents previously submitted, particularly highlighting the time and the manner in which incidents are being resolved. The existing applications showed success and we intend to analyse these solutions whilst developing trust indicators, creating web portals and a data-analytics engine behind a database. This paper

[1] Daniel James, Rinicom Ltd., Lancaster, UK, e-mail: Dan.james@rinicom.com
[2] Mark van der Giessen, Rotterdam School of Management, Erasmus University Rotterdam, Rotterdam, Netherlands, e-mail: vandergiessen@rsm.nl
[3] Petra Saskia Bayerl, Rotterdam School of Management, Erasmus University Rotterdam, Rotterdam, Netherlands, e-mail: bayerl@rsm.nl
[4] Gabriele Jacobs, Rotterdam School of Management, Erasmus University Rotterdam, Rotterdam, Netherlands, e-mail: gjacobs@rsm.nl
[5] Ruza Karlovic, General Police Directorate, Police Academy, Police College, Zagreb, Croatia, e-mail: rkarlovic@fkz.hr
[6] Garik Markarian, Rinicom Ltd., Lancaster, UK, e-mail: Garik@rinicom.com

will present the Unity project and the work we have done so far and it conceptualises the work to come in the form of architectural designs and specifications.

Key words: *application, community policing, cooperation, citizen-engagement, mobile-technology, unity.*

1. INTRODUCTION

In this paper we will show what the Unity project is about. We will demonstrate that community policing means different things to different countries and organisations, but can be linked back into a set of abstract objectives.

Unity is a European funded project as part of the European Union Horizon 2020 Programme (No 653729) programme. It has a lot of support from a wide variety of organisations with a wealth of experience in many different fields. We have universities, police forces, police colleges and businesses alongside an advisory board that will help when required. The *Unity* project set out to give the European member states a *unified* ideology when dealing with *local* community problems. The original aim of *Unity* was to "strengthen the connection between the police and the communities to maximise the *safety* and *security* of all citizens" (Unity Consortium, 2014, p. 4).

A community policing (CP) approach to policing has many key benefits such as preventing crimes before they happen, identifying worries within the community and helping them. The community, for the community with only a small part to play by the actual police forces, can do these things. Thus increasing the Community policing routes need to be explored in further works and integrated with a current technology, which will encourage the community to play their part in living in a nicer environment.

Information Communications Technology (ICT) has been a key catalyst all over the world over for at least the past 30 years. For the community, most will have a smartphone. In fact, over 66% of UK adults own one or more. That number jumps to 90% in the younger generation from 16-24, now even 50% of 55-64 year olds will own one (OFCOM, 2015). It makes sense to include this technological advance into the community as a community policing application to enhance and strengthen bonds between the police and community.

2. BRIEFLY ABOUT COMMUNITY POLICING AROUND THE WORLD

Defining CP is quite a challenging task. Although everyone seems to understand what CP is, not everyone can provide a definition of the concept of CP. According to European Code of Police Ethics, the main purposes of the police in a democratic society governed by the rule of law are: to maintain public tranquillity and law and order in society, to protect and respect the individual's fundamental rights and freedoms as enshrined, in particular, in the European Convention on Human Rights, to prevent and combat crime, to detect crime, to provide

assistance and service functions to the public[7]. Police scholars point out that community policing is one of the most widely adopted police strategy in the last several decades in most democratic societies (Weisburd, Eck, 2004). Ponsaers (2001) states that Friedmann is the author of one of the most realistic definition of community policing. I.e., "Community policing is a policy and a strategy aimed at achieving more effective and efficient crime control, reduced fear of crime, improved quality of life, improved police services and police legitimacy, through a proactive reliance on community resources that seeks to change crime causing conditions. This assumes a need for greater accountability of police, greater public share in decision making, and greater concern for civil rights and liberties" (Friedmann, 1994).

An often cited definition of community policing is the one written by Trojanowicz and Bucqueroux (1990): "Community policing is a new strategy of the police action based on the idea that the police officers and community members work together, and they used different innovative ways to solve ongoing problems at the local community level in connection with crime, fear of crime and other different social deviations. Achieving these goals requires from the police the development of new relationship with law abiding citizens, in which they will get the opportunity to define priorities and to include themselves in different activities in order to improve the quality of life in their neighbourhood. So, the community policing moves the focus of the police work from reacting to incidents to proactively solving the problems".

Types of police models are shown in Figure 1.

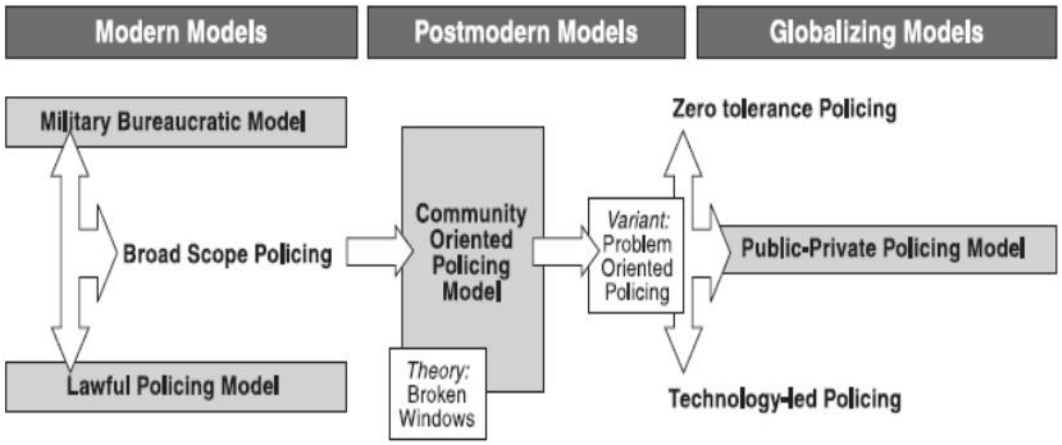


Figure 1: Types of police models (source: Ponsaers, 2001:473)

This author discusses models of policing that are the result of a detailed analysis of different definitions of community policing to be found in the literature. Ponsaers stresses that there are in fact only four central police models: the military-bureaucratic model, the lawful policing model, community-oriented policing, and public-private divide policing. The same author concludes that each concrete police system can be considered as a combination of police

[7] The European Code of Police Ethics 'Committee of Experts on Police Ethics and Problems of Policing' Recommendation Rec(2001)10

models. According to Joyce (2013), community policing means multi-agency approach, i.e. cooperation among police, citizens and other organizations with a goal to prevent the occurrence of crime. The overall objective of the project *Unity* is to create a new and sustainable citizen centred CP model, which strengthens police-community relations.

3. ABOUT UNITY

Unity is an EU Horizon 2020 funded project under the Secure Societies theme of the Fight against Crime and Terrorism on Community Policing in Europe.[8]

The project's implementation started on 1 May 2015 and is planned to end on 1 May 2018. The Unity consortium, coordinated by the Office of the Police and Crime Commissioner for West Yorkshire, consists of 16 partners from 10 European countries, precisely: Serco Europe, Erasmus University Rotterdam, Police University College of Finland, Sheffield Hallam University (Centre of Excellence in Terrorism, Resilience, Intelligence & Organised Crime Research (CENTRIC)), University of Dundee (Scottish Institute for Policing Research (SIPR)), European Institute, FHVR Fachbereich Polizei, RINICOM, Treelogic, Croatian Police College, Belgian Police, Estonian Police and Boarder Guard, St. Kliment Ohridski University.

3.1. Objectives of Unity

The *Unity* vision is to strengthen the connection between the law enforcement agencies (LEAs) and the community in order to create safer societies in Europe.

Unity shall create a new, community-centred approach to CP.

The *Unity* vision shall be delivered through the following strategic objectives (SO):

SO1 – CP Best Practice – capturing the best practices for cooperation between police and citizens

SO2 – CP Communications Technology- developing communications technology to improve the communication between citizens and the police

SO3 – CP Training and Awareness –training for LEAs and awareness raising activities about CP

Research will be conducted to identify best practices in CP, and after having identified them, *Unity* will develop CT tools to facilitate, strengthen and accelerate communications between LEAs and communities. The CT tools will be piloted in six EU MS (Croatia, Estonia, Germany, Belgium, Finland and UK). The tools will be supported by new CP training activities for LEAs, and by awareness raising activities for communities and other stakeholders.

Unity work plan is divided in 8 work packages that are all interrelated and interdependent, and whose objectives are described below:

[8] For more information see: www.unity-project.eu

WP1 – Project management

WP2 – Ethical, Legal and Community Issues – analysing the social, cultural, legal and ethical dimensions underlying best practices in CP and policing research.

WP3 - Policing and Community Requirements and Best/Effective practices – to capture current practices of community policing, including the identification of best practices in the interplay between communities, LEAs and other stakeholders.

WP4 – Community Policing Delivery Framework – identifying, analysing and mapping results of WP 2 and 3; mapping and building a register of roles and responsibilities, capabilities and capacities that can be accessed from all stakeholders to meet the CP initiatives; providing a clear scope of requirements for the Combined Effect CP initiatives to inform the CPAF, TOM and UCP and interactively validate the CONOPS.

WP5 – Technology Toolkit – providing technological components for supporting the Unity Communication Platform (UCP) and the Community Policing Architecture Framework (CPAF); designing UNITY's architecture toolkit

WP6 – Unity Integration Framework – developing a citizen-centred Unity Communication Platform (UCP)

WP7 - Test beds, Pilots, Evaluation – ensuring functionality and usability of the newly developed tools; evaluating the impacts of the tools with respect to the processes and outcomes of CP

WP8 – Dissemination, Exploitation and Training – ensuring information about project activities and results are effectively distributed; ensuring project results are effectively exploited (Unity Consortium, 2014)

4. RESEARCH CONDUCTED WITHIN UNITY

4.1. Philosophy

Unity aims to develop a community policing tool that is applicable in a wide range on contexts. Therefore, the *Unity* includes the systematic exploration of local contextual difference and their impact on the success of such a community policing tool. We also synthesize cross-context data to develop a tool that is usable not only in local contexts but also across a wide set of different contexts. Furthermore, *Unity* is based on participatory design, where potential users of a technology are including as early as possible; ideally from the original design and subsequent development stage. Conducting evaluations in this light is no trivial feat, as it needs to consider that technology also develops over time, and that the testing spans multiple countries and user groups. Diversity and flexibility are therefore inherent in the research methodology and design.

4.2. Conceptual approach

The iterative approach to the development of *Unity* with pilots moving across countries introduces considerable variation in national, political, economic, social and technological contexts as well as potential differences in terms of norms, experiences, knowledge, etc. These national and contextual differences challenge the comparability of concepts, processes and results across the pilot sites. It is therefore important to establish "Equivalent meaning of concepts and data in different social and cultural contexts" (Craig & Douglas, 2005). This perspective, inter-subjectivism, is shared across many social sciences as "the world is *socially constructed* […] based on shared meanings, interpretations, and culture" (Yeganeh & Su, 2006; Cunliffe, 2011).

The current methodologies for cross-cultural research strive for a balance between insider (emic) and outsider (etic) perspectives (Pike, 1971). These concepts originate from two sub-disciplines in linguistics: phonetics and phonemics. Phonetics concerns language signals, and aims at explaining their production and perception. Phonemics on the other hand concerns language system functions, structures, and distributions of phonemes (Pike, 1971).

Theorists who look for cross-cultural universalities often take an etic approach toward their research where they strive for collecting a large breadth of data (Berry, 1997). They strive to collect data from a variety of cultures, even though the instruments they use are generally developed in the culture of their own. Theorists who look for variations in behaviour on the other hand tend to prefer an emic approach, where they examine only one culture in-depth. Emic research originates from the disciplines of anthropology, cultural psychology and cultural sociology and contends that behaviour can only be understood and interpreted in its original context.

Unity however much extend beyond an exclusively culture-dimensional approach as this approach has shown to be insufficient to resolve many specific subtleties in cross-cultural dilemma's. Knowledge on cultural differences in light of the work of Hofstede (1980) for example reflects only a first heuristic to obtain cultural dissimilarities. These cultural dimensions were designed to acquire cultural understanding and to allow cross-cultural comparisons on a generic level. This approach is insufficient however when attempting to understand concrete behaviours. We therefore believe that the development of a tool and evaluation framework for Unity requires a wider range of research methods than is generally applied in the current literature. Simple dimensional characteristics are not sufficient to capture the social and cultural phenomena pervasive in community policing settings. An extended model, which incorporates situational and contextual information such as the socio-political context in which the police operates, is required to do justice to the complexity of the framework for understanding the local culture.

Research in the field of social psychology has indicated that there can be large differences between attitudes (such as value statements) and actual behaviours. The situational context often has a strong influence on the expression of cultural norms. Personal experiences with a specific person or specific demands of a social setting for example can greatly affect

behaviours (Bennett, 1999; Malhotra & McCort, 2001). Behaviours are generally better predicted by attitudes that concern specific behaviours rather than by general attitudes. Furthermore, the specific demands of particular situations, such as an individual's self-efficacy or specific performance and outcome expectations can strongly influence behaviour. These factors have important implications for the methodologies of cross-cultural research. Namely, cross-cultural research has to resolve the methodological problem of quantitative measurement equivalence, generally through qualitative measures (Poortinga, 1997; Berry, 1989).

4.3. Empirical methodology

The Unity platform is developed from concept to functioning prototype to final product through multiple iterations of pilots and evaluations. Furthermore, community policing is embedded in local communities by definition. The success factors and enablers of community policing and *Unity* are thus contingent on the requirements and expectations of these communities. Community policing through Unity can therefore only be effective if the generalizable principles of community policing are developed whilst taking the local context across countries, regions and cities into consideration. It is therefore required to investigate the best and effective practices in community policing in different contexts in order to determine important similarities and differences.

These best and effective practices of community policing in their local (cross-) cultural context are collected through both quantitative etic and qualitative emic methods. The first step in developing a comprehensive set of tool development and evaluation criteria for Unity, researchers from the participating countries started with emic research on the main research questions (to identify key elements such as goals, tasks, capabilities and success criteria of community policing). The researchers continued with an identification of which elements of community policing are generalizable and which are not, in order to develop a tool and evaluation framework which combines both generalizable components for all countries and country-specific components for each individual participating country. This exploratory development stage of the Unity platform pertains to the following goals:

- To capture current practices of community policing including the identification of best practices in the interplay between communities, LEAs and other relevant stakeholders.
- To provide a solid understanding of perspectives on - and expectations for community policing across relevant communities, LEAs and other stakeholders.
- To understand user requirements and challenges for the acceptance and use of community policing tools, taking into consideration diversity issues such as gender, cultural disparities, differences in interests as well as the specifics of national context.
- To identity potential conflicts among the understandings of - and expectations for CP by communities, LEAs and other stakeholders.

- To map out the national differences and similarities in practices, expectations and requirements among relevant communities across participating countries.

As stated previously, the design of the Unity platform will go through several iterations of pilots, evaluations and modifications and the technologies will thus mature over time. The first pilot took place 6 months into the project and concerned a proof-of concept and the final pilot will take place in month 31.[9] This iterative approach to development allows for testing technologies directly in the field at every stage of development, from the starting conceptual stage through to the last functional prototype. This ensures that the final tool is suitable for practical application in the field. Further, as the development includes multiple stakeholders and deployment in multiple countries, transferability across different contexts is an integral part of the Unity development. This multi-contextual design philosophy, i.e. taking into account "the co-existence of different use contexts" (Henfridsson & Lindgren, 2005, p. 96; Lindgren et al., 2008), is integral to Unity's vision to develop a flexible and scalable community policing model, which is applicable beyond application by the original consortium involved in the development.

The pilot evaluations are grounded in literature and theories on change evaluation, information system design, implementation and adoption and community policing. The evaluations include the following elements:

- *Consideration of changes over time*: single-point and longitudinal evaluations will be combined to determine how processes and outcomes (for example tool adoption rates and user satisfaction) vary with increasing maturity of the tool. The evaluation will also take into account that some effects (for example on trust or the reporting of crimes) may take some time to show after the intervention.

- *Multi-stakeholder view*: The Unity platform needs to be applicable for multiple communities and groups. At a general level, the Unity users can be divided into target citizen groups, potential intermediaries and the police forces in the pilot countries. In order to assess the Unity platform's usability and effects, and to understand the processes through which Unity can facilitate interactions between user groups, these multiple stakeholders are included simultaneously in the evaluation.

- *Multi-level approach*: Unity is predicted to have an impact at different levels of measurement; the individual level (for example acceptance due to user diversity), and the group – and organizational level (for example adoption rates due to disparate minority cultures and organizational structures). We also expect cross-level and multi-group interaction effects.

- *Triangulation of findings from various outcome levels*: As effects and impacts can express themselves in various ways and at different levels, from changes in affect, knowledge and skills to concrete behaviours. These different modalities are not

[9] For details on the *Unity* evaluation approach see Unity Deliverable 7.1 – Report on Evaluation Criteria, October 2015

necessarily congruent; a user who is keen on adopting technologies may still not do so if peers, superiors or the environment reject the technology or do not provide the appropriate infrastructure. We therefore assess multiple modalities and triangulate results.

To allow for comparisons of evaluations across the pilot countries, every country will research community policing related to the same type of community. The target community was selected based on the data collected for WP 3. The groups targeted across the pilot countries are:

- Young members of a minority group (above 18 years of age and below 26; the age limit of 18 ensures that minors are excluded, which was done for legal/ethical considerations); which minority group becomes the target community can be determined by each country itself.
- One intermediary, i.e., organization that supports police works in accessing or addressing this minority group.
- The local police force and subgroups within the police that deal with this minority group, respectively.

4.4. Ethical considerations

Considering the international scope of Unity and the goal to create a locally and internationally accountable community policing platform, at least in part through the development and deployment of relevant technologies, it is essential to incorporate an understanding of the (inter)national legal and ethical framework in which Unity has to be developed and implemented. Unity therefore includes the creation of a comprehensive legal and ethical framework to structure Unity's work in order to be able to operate in a legally and ethically robust way, at all times. This framework considers the following areas: data collection, processing, storing and sharing, the ethical limitations on the research into community policing and the prevention of harm for research participants and technology users. Furthermore, the legal framework will adhere to European as well as national legislation on data protection for each of the participating countries.

The ethical and legal framework is required to assure that both researchers and participants partaking in the Unity project adhere to the ethical and legal best practices, thus promoting confidence in the research and ensuring that findings and products do not violate existing legal and ethical restrictions. It should furthermore be noted that these ethical guidelines are more comprehensive and less explicit and uniform than the formal legal requirements, and include a lot of variation among member states. WP 2 therefore includes a systematic assessment of- and adherence to formal legal restrictions as well as ethical limitations and

legal and ethical best practices from each partner country, for both research practices and community policing through Unity.[10]

4.5. Key target areas of community policing

The country teams conducted emic studies within their own cultural context and summarized the data according to their own country's understanding in standardized reporting templates. The EUR team subsequently categorized the data (imposed etic) and derived an overall perspective through joint meetings with the individual country teams (Emic A vs. Emic B). In this section, we will present and discuss the first findings from this explorative stage across the eight countries Belgium, Bulgaria, Croatia, Estonia, Germany, Finland, Macedonia and the UK.[11] The country teams conducted a total of 323 interviews; 88 with police officials and 235 interviews with stakeholders with communities and intermediaries within these countries. The interviews detail observations regarding the following topics:

1. How to define community policing?
2. What are the main goals and tasks of community policing?
3. Which are the main target communities and stakeholder groups?
4. What are the main enablers, opportunities and threats for community policing within police forces as well as their environment?
5. What do you consider good and bad practices?
6. How could community policing performance and outcomes be measured?

4.5.1. Defining community policing

Definitions of community policing could be grouped into five general categories: policing performance, working together with local communities and partners, fostering trust, fostering confidence and understanding, focusing on human aspects of policing and empowering local communities, and area specific policing. Police officers primarily defined community policing in terms of performance, which included crime fighting, prevention, protection, intervention as well as understanding and dealing with local issues. However, the definitions offered by community members and intermediaries were similar, they additionally focused strongly on the importance of understanding and addressing local needs and issues.

4.5.2. Goals and tasks of community policing

The interviewees reported a total of 1630 goals and 1659 tasks. Goals were subdivided into five main categories: assistance and service, increasing and improving cooperation, managing information exchange, improving police-internal processes and structures, and policing performance and outcomes. Both police officials and external groups mentioned policing

[10] For more details see Unity Deliverable 2.1 – Unity Legal and Ethical Framework, October 2015

[11] For more information on the methodology and findings see Unity Deliverable 3.1 – Report on Existing Approaches and Best/Effective Practices to Community Policing, October 2015 and Unity Deliverable 3.2 – 1st Stakeholder Analysis – Shared Themes and Concepts, January 2016

performance and outcomes most frequently. Police officers showed considerable variation in their reporting of primary tasks for community policing, involving all of the previously mentioned categories. The external groups were more consistent in what they considered the primary tasks for community policing, emphasizing the availability and accessibility of the police and crime fighting to ensure safety and security.

4.5.3. Main target communities and stakeholders

Twenty-seven different stakeholder groups were mentioned. Interestingly, external groups mentioned primarily various citizen groups whereas police officers focused more on intermediaries. This suggests that police officers and external groups differ in which type of groups they consider most relevant for effective community policing, where citizens focus on their own interests and police members on organizations and parties that could facilitate community policing efforts. Furthermore, when evaluating which specific target groups are prioritized, police officers showed a lot of variation. Police officers frequently mentioned various age groups, migrant and minority groups and (to a lesser extent) the general public and (potential) victims. Community members on the other hand agreed and focused predominantly on specific age groups, and to a lesser extent on migrant and minority groups. When it comes to the most important intermediaries, police officers focused on government organizations, such as ministries, health, fire, transport, security, social services, political parties, politicians, intelligence services and other police forces. Though community members also predominantly focused on government services, they also mentioned a large number of private businesses and unions, media and charities and NGO's as important intermediaries.

4.5.4. Enablers, opportunities and threats for community policing within- and outside police forces

Interviewees mentioned a total of 1031 internal enablers, 1055 internal strengths and 855 internal weaknesses across all countries and groups. Internal enablers were subdivided into seven categories: contact and communication between police and external groups, cooperation and relationships, efforts in crime fighting, performance management, resources and capacities, and accountability and corruption reduction. Interviewees overwhelmingly mentioned resources and capabilities as the most important internal enablers, strengths and by extension also weaknesses. The main internal enablers concerned capacities of staff such as professional expertise, a positive attitude of officers, motivation and dedication, and (to a lesser extent) financial resources.

External enablers pertained to four categories: contact and communication, cooperation and relationships, trust and accountability, and contextual factors. Both police and community members most frequently mentioned the importance of cooperation and relationships, followed by contextual factors. Cooperation and relationships were mentioned most frequently with respect to external opportunities, followed by a lack of capacities and resources. When it comes to societal developments, community members mentioned a wider variety of threats than did police officers. External groups also focused more on the importance of police image and attitudes toward police than did the police officers

themselves. In general, all countries and groups showed considerable appreciation for the importance of a facilitating external environment. Cooperation and partnership, working with specific external parties, and support and understanding were mentioned most frequently as important external enablers.

4.5.5. Good and bad practices

Interviewees offered 620 examples of 'good' and 475 examples of 'bad' practices. Five categories of 'good' practices could be discerned: supporting relationship and trust building, providing the right and sufficient resources and capacities, fostering contact, communication and dialogue between police and communities, fostering cooperation and collaboration and practices leading to good outcomes and performance. Examples of 'bad' practices generally pertained to the same aspects, but inversed (a lack of, etc.).

Furthermore, a difference in 'good' and 'bad' practices does not necessarily denote a difference in what is considered 'good' or 'bad' between countries. Rather, it could also be an indication of relative importance or a closer perceived connection to community policing within a country. That said, we found considerable overlap in perceived practices across different countries and groups. Nearly all countries and groups agreed that managing consistent contact and communication between groups is paramount and negative attitudes and a lack of respect among officers, issues with internal structures and cultural elements such as lack of authority, a lack of priority for community policing, a lack of proactivity were consistently mentioned as examples of 'bad' practices.

4.5.6. Measuring community policing performance and outcomes

Interviewees identified ten different elements of community policing performance and outcomes to be measured, including citizen perceptions of safety, reductions in crime rates, and the recruitment of motivated and skilled police staff. Both police and external groups prominently mentioned crime reduction as an important indicator. A second category pertained to different features of police organizations and individual police officers. This included aspects such as officers' perception of community policing as integral part of the organization and the skills, abilities and knowledge of individual officers. Another important indicator across countries and groups was the quality of relationships.

5. A COMMUNITY ORIENTED COMMUNICATION PLATFORM AS AN OUTCOME

The outcome of the *Unity* project is focused on the technical tools to work in parallel to the community policing methods that are used today. Within this chapter, technical features of the proposed solution are discussed in relation to the current stage of the Unity project. A review of our methodology is shown in brief, on how the Unity project conceptualised the proposed components and the justification behind them.

5.1. High Level Features as Key Target Areas

The key objective from a technical perspective is to "develop a communications technology to facilitate, strengthen and accelerate the communication between citizens and police." Focusing on a "User centric approach" to "report their concerns to the police". (Unity Consortium, 2014, p. 4) This is the second strategic objective aforementioned.

Utilizing this information and keeping up to date with what community policing is defined as within the scope of Unity, enables the main high-level features and requirements for a tailored functional system to be designed.

The methodology to define these features is shown in Figure 2.

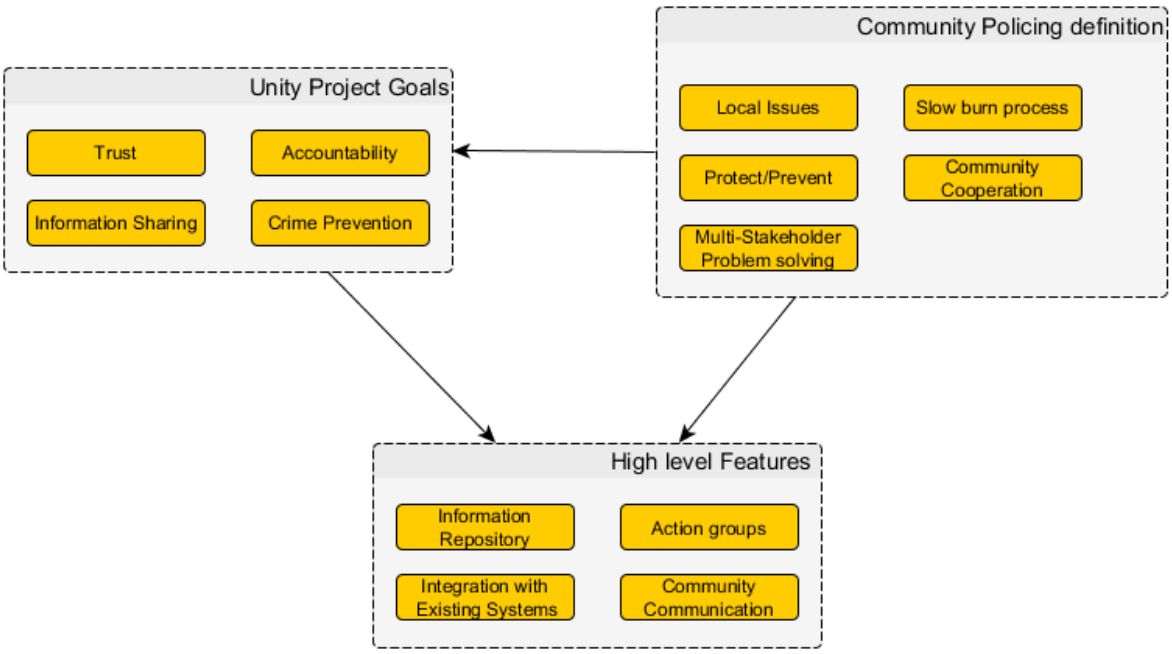


Figure 2: High level Feature requirement gathering

The system must act as an information repository, allowing an amalgamation of issues, solutions and action plans for local issues. The system must also facilitate communication between the police and the community to improve relations and strengthen trust.

5.1.1. Information repository

The first key features that the Unity technology needs to achieve is the idea of an information repository, allowing information to pool in a central, accessible place, which is relevant for all local community issues. This repository will increase the awareness of both the community and the police, which is the first step in tackling any problem.

5.1.2. Communication platform

The secondary key feature objective is the idea that there is an effective communication platform between the community and the police, specifically for dealing with community

policing issues. This includes giving the community the platform to communicate with each other in a safe environment where actions will be done at the end of the process with LEA support.

5.1.3. Integration with existing systems

Integration of the system with existing police systems is another key feature objective. This will enhance reporting and therefore unite the incumbent police system and processes with the Unity community policing tools. In effect relying on the community to identify issues, would drastically reduce the burden on the LEAs and allow them to focus on addressing and resolving issues. The overlying problem with integration is that all current LEA systems are independent with limited similarities. The aim of the proposed system is to create the data sets and interfaces which will allow individual LEA's to easily adapt their current systems to work with the proposed Unity system.

5.1.4. Action Groups

The action groups will be tasked with a particular issue in which they will be required to find a resolution using the communication platform and information repository as facilitators. The emphasis here will be the group mechanism; how notifications, actions and potential solutions fit into the group environment.

5.2. Proposed Features

5.2.1. Community features

The Community side of the application has been planned to provide the citizen's with access to view ongoing areas of trouble. It provides them with the means to report a new subject topic and a allow them to generate ideas and discussions on the best course of action for the community issues.

The citizen should be able to view what current issues are around their local community. There are possibilities for either textual list based or map based reports. Certain issues can be overlaid onto a map view to see issues pertinent to specific locations, how widespread they are and whether there are any patterns. This can be done with either individual specific issues or a combined view, given specific situational awareness within the local community.

Citizens should be able to report an issue in their local area, ideally, they would be able to pinpoint the problem area on a map. They will be able to include additional data in the submission including text clarifications, audio, video or images. This will improve the knowledge base and allow the issue to be targeted with a greater understanding supporting any future actions.

Each user should have a "profile" which may contain as much or as little information as they wish. All that is required is a username (email for validation) and password. This profile will be the foundation for trust between the community and the Unity platform. For users to maintain full anonymity would create problems for trust, accountability and system security

and should be avoided. The profile may contain optional personal information; the user has total control of which information they choose to share with the platform, and aims to improve user comfort and trust. The profile may include but is not limited to information such as name/s age, contact details, job title and picture.

Location is an important metric that should be sent when reporting or registering, often it is required to pin point an exact point where local issues take place, for example, where hooligans congregate. However, some community issues may be area-wide and are not constrained to a specific location. We should be allowed to send location where each issue happens and then can create an overall view of where the problem lies, and the spread of the issue. Where GPS is not available, allowing the user to select a location is required so that it can be included in the incident report. This can be in the form of GPS location or street names. Textual descriptions can supplement this but would be difficult to combine with an analytical engine and they are therefore recommended only to the user when the above methods are not feasible/available.

Reporters will have the option to opt in on their action group updates as the issue progresses. Keeping up with conversations, action points, targets and community effort would be examples of the types of notifications they can receive. This feature should always have the option to be switched off as sometimes it can become increasingly frustrating when notifications are unwanted (Poppinga, Heuten, & Boll, 2014). This option will be an essential part of the system for community stakeholders looking to take a more active role in helping their local community solve pertinent issues.

5.2.2 LEA features

The LEA version of the Unity tool is going to be similar to the community side with some slight variations. Due to the LEA's position of authority, we have designated them to be the community policing coordinator, which will include moderation responsibilities, and posting status of issues beyond the information, which the community can provide.

When a new issue is reported, the LEA application should review (moderate) it and then change the status and amend who can view it. If the issue is rejected for a specific reason, the status will be changed accordingly and permission would not be public; the original reporter of the issue will be notified of the rejection unless they opted out of the notifications for this report. If evidence or criminal activity is recorded, depending on the nature of the data and pending further discussion, the evidence may be placed into the public database or kept private based on a supervising LEA moderator's discretion.

The LEA application will have a similar view of open issues in the community. They will have additional permissions, which will allow them to see the rejected and private issues. An LEA feature may allow for the invitation of fellow officers to an issue if more support is needed or delegation is required. The Unity app will try and keep as much of the burden off the police forces as possible.

Users of the LEA Unity application should be identified with at least a name or possibly force identification number (FIN). This will enable officers to be identifiable and therefore increase familiarity alongside the aim of maintaining the officer's professional behaviour, improving trust with the community and increasing accountability.

5.2.3 Core server logic

The key component in the Unity system will be the server. It is the link that will join the components together. This can be seen in our architecture in Figure 3 below.

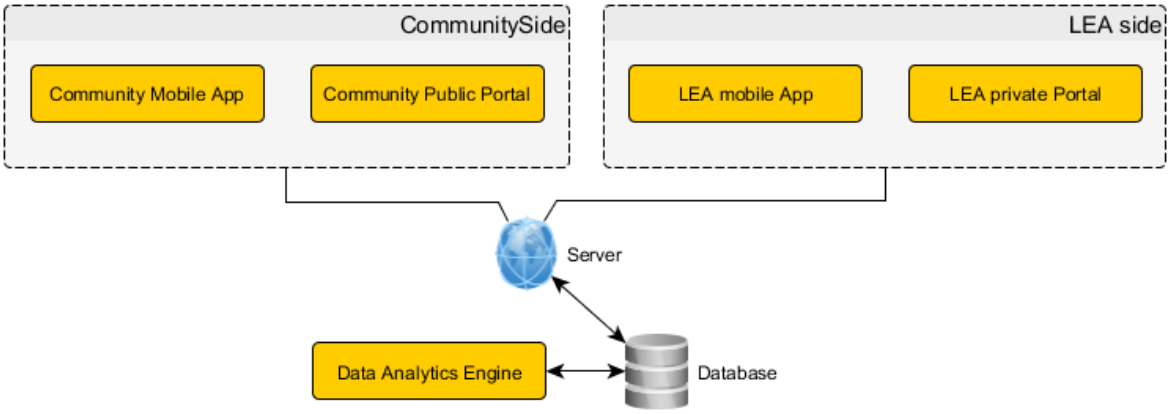


Figure 3: System architecture concept

The server will be glue that binds the different areas of the Unity toolkit together. It will provide connectivity between the community allowing communication and information flow. The server should be the component that contains the core logic of the system. The server will contain several components as seen in Figure 4.

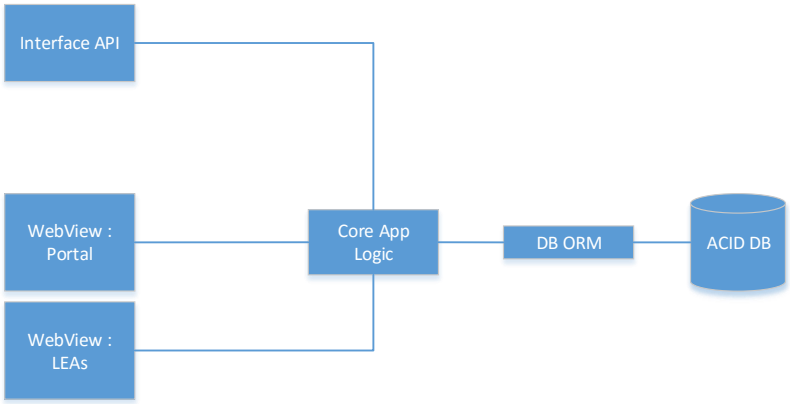


Figure 4: Server architectural conceptualisation

It will contain a web view for the specific entities and an interface API for applications to push data through. This will give applications a way of pushing data into the server through various requests.

The Core App logic should provide functionality that will process the various requests from the various endpoints, community portals, LEA portals or otherwise. It should handle the

incoming requests whether the requests are open to an action group to discuss an issue, contribute a solution or add further discussion to an existing system or to set up.

The Core will be responsible for determining the trust level of users and making decisions based on their trust and permission level. The Core logic will be responsible for notifying the relevant (subscribed) users on updates to their action group, or issue they are following. The Core app logic will also focus on receiving, processing and relaying on the incoming requests, acting as a medium between the database and the clients.

5.2.4 Data analytics engine

The data analytics engine will process the data captured within the database, it will use algorithms to develop patterns and statistical analysis on data that the human brain cannot see by looking at the raw data. Possibilities are discussed so far but they are not limited to:

- Risk heat maps,
- Trending concerns,
- Evolution of concerns,
- User base analytics.

5.3 Technical Challenges

One of the most challenging aspects of this project is the routing of the reporting system to the correct local issue. Within the scope of the Unity project, this will not be an issue, as the pilots will happen independently of each therefore all uses will occur in a single region. In an emergency environment, there is extra legislation and components within the access networks that will allow application providers to route to the correct PSAP. In this community policing environment, our resources are limited and it would require a simple geographical boundary to send to the correct serving page for their specific local issues. This means that the user, placing the trust into the users to not misuse the toolkit, must provide a location.

Coordination and moderation of the system is going to be one of the key technical challenges for the system, it may be that each region has a regional Unity coordinator to approve and monitor communications. The moderator will need to adjust the permissions of issues in case it the development of the issue becomes too sensitive to keep public. Therefore, vigilance will be a key requirement on the human side of this project.

Naming of the toolkit: Research has found that if an application has the words “police” or similar, it is often perceived very badly. The challenge is instead of Community policing, the focus should be on the community, helping the community with support of the police.

6. INSTEAD OF CONCLUSIONS

There are plenty of definitions of Community Policing, many of which are from different points of view. All the definitions have two things in common: they include the terms "community" and "police". The approach taken by the person providing the definition is the key: the focus can be on "police", "community" or both.

The Unity approach is community-centred (citizen-focused) meaning that people are at the heart of identifying policing priorities and they participate at creating sustainable CP solutions. Unity aims at creating a flexible citizen-centred CP model, which strengthens the cooperation between the police and the communities they serve to maximise the safety and security of all citizens.

Unity conceptualises CP in terms of "collaboration and coordination, whilst facilitating shared ownership, responsibility and building trust and community confidence". Unity will create a new and sustainable citizen centred CP model, built around community trust and confidence and providing two-way flows of information and communication. "By working with citizens and community stakeholders to arrive at full understanding of their concerns, targeted interventions and solutions can be agreed which not only address any immediate symptoms but also tackle any possible long term implications". With regard to the concept of police work and the organization of the police in a given society, the model of community policing is interpreted differently, with different programs, approaches and technology but with the same goal in various European nations. The *Unity* project aims to unify the European member states with an effective community policing methodology, which is underpinned by the technological advance in modern society.

REFERENCES

Bayerl, P. S., Van der Giessen, M., & Jacobs, G. (October 2015). Unity Deliverable 3.1 – Report on Existing Approaches and Best/Effective Practices to Community Policing. Centre of Excellence in Public Safety Management/Rotterdam School of Management, Erasmus University Rotterdam.

Bayerl, P. S., Van der Giessen, M., & Jacobs, G. (January 2016). Unity Deliverable 3.2 – 1st Stakeholder Analysis – Shared Themes and Concepts. Centre of Excellence in Public Safety Management/Rotterdam School of Management, Erasmus University Rotterdam.

Bayerl, P. S., Jacobs, G., & Van der Giessen, M. (October 2015). Unity Deliverable 7.1 – Report on Evaluation Criteria. Centre of Excellence in Public Safety Management/Rotterdam School of Management, Erasmus University Rotterdam.

Bennett, R. H. (1999). The relative effects of situational practices and culturally influenced values/beliefs on work attitudes. *International Journal of Commerce and Management, 9* (1&2), 84-102.

Berry, J. W. (1989). Imposed etics-emics-derived etics: The operationalization of a compelling idea. *International Journal of Psychology, 24*(6), 721-735.

Berry, J. W. (1997). An ecocultural approach to the study of cross-cultural industrial/organizational psychology. In P.C. Early, M. Erez (eds.), *New Perspectives in*

International Industrial Organizational Psychology (pp. 130-147). San Francisco: New Lexington.
Committee of Experts on Police Ethics and Problems of Policing. (2002). *The European Code of Police Ethics.* Strasbourg: Council of Europe Publishing.
Craig, C. S., & Douglas, S. P. (2005). *International Marketing Research.* John Wiley & Sons, Chichester.
Cuncliff, A. L. (2011). Crafting qualitative research: Morgan and Smircich 30 years on. *Organizational Methods Research, 14* (4), 647-673.
Friedmann, R. R. (1992). Community Policing: Comparative Perspectives and Prospects. New York: St. Martin's Press.
Henfridsson, O., & Lindgren, R. (2005). Multi-contextuality in ubiquitous computing: Investigating the car case through action research. *Information and Organization, 15*(2), 95–124.
Hofstede, G. (1980). Culture's Consequences: International Differences in Work-Related Values. London: Sage.
Joyce, P. (2013). Policing, Development &Contemporara Practice. London: Sage publications Ltd.
Lindgren, R., Andersson, M., & Henfridsson, O. (2008). Multi-contextuality in boundary-spanning practices. *Information Systems Journal, 18* (6), 641-661.
Malhotra, N. K., & McCort, J. D. (2001). A cross-cultural comparison of behavioral intention models-Theoretical consideration and an empirical investigation. *International Marketing Review, 18*(3), 235-269.
OFCOM. (2015, August 06). *The UK is now a smartphone society.* Retrieved from OFCOM: http://media.ofcom.org.uk/news/2015/cmr-uk-2015/
O'Neill, M., Hail, Y., Wooff, A., & James, D. (October 2015). Unity Deliverable 2.1 – Legal and Ethical Framework. University of Dundee.
Pike, K. L. (1971). Language in Relation to a Unified Theory of the Structure of Human Behavior. The Hague: Mouton & Co.
Ponsaers, P. (2001). Reading about «community (oriented) policing» and police models. Policing: An International Journal of Police Strategies & Management, 24(4): 470-496.
Poortinga, Y. H. (1997). Towards convergence? In: J. W. Berry, Y. H. Poortinga, J. Pandey (eds.), *Handbook of Cross-Cultural Psychology 1* (2nd ed., pp. 347-387). Boston: Ally and Bacon.
Poppinga, B., Heuten, W., & Boll, S. (2014). Sensor-based identification of opportune moments for triggering notifications. Pervasive Computing, IEEE .
Trojanowicz, R., C., & Bonnie, B. (1990). *Community Policing: A Contemporary Perspective*. Cincinnati, OH: Anderson.
Unity Consortium. (2014). *Unity.* European Union Horizon 2020 Programme (No 653729)
Weisburd, D., & Eck., J. (2004). What can police do to reduce crime, disorder and fear? The Annals of the Amecican Academy of Political and Social Science.
Yeganeh, H., & Su, Z. (2006). Conceptual foundations of cultural management research. *International Journal of Cross Cultural Management, 6* (3), 361-376.

STRUČNI RAD

Nikolina Grbić Pavlović[12]

SPECIFIČNOSTI SASLUŠANJA DJECE I MALOLJETNIKA OŠTEĆENIH KRIVIČNIM DJELOM

Sažetak

Pored toga što se danas djeca i maloljetnici sve češće pojavljuju kao izvršioci krivičnih djela i prekršaja, veoma često se pojavljuju i kao žrtve negativnih uticaja i događaja u sredini u kojoj žive. Novija viktimološka saznanja ukazuju da djeca veoma lako postaju žrtve određenih krivičnih djela koja čine (najčešće) odrasla lica na njihovu štetu. Iz tog razloga mnoga zakonodavstva sve češće unapređuju postupke u kojima se djeca i maloljetnici pojavljuju kao žrtve krivičnih djela. Upravo je tako i novim Zakonom o zaštiti i postupanju sa maloljetnicima u krivičnom postupku Republike Srpske naglašen karakter specifične zaštite djece i maloljetnika prilikom njihovog saslušanja kao oštećenih krivičnim djelom. Naročito je naglašen adekvatan pristup ovlašćenih lica prilikom saslušanja djece i maloljetnika, kao i upotreba tehničkih uređaja za prenos slike i zvuka. Upravo ovakav način saslušanja djece i maloljetnika biće glavni predmet ovog rada. U radu će se, takođe, prikazati podaci o korišćenju posebno opremljenih prostorija za ispitivanje maloljetnika u praksi Ministarstva unutrašnjih poslova Republike Srpske.

Ključne riječi: *djeca i maloljetnici, žrtve, saslušanje, pristup i način ispitivanja, tehnički uređaji za prenos slike i zvuka.*

1. UVOD

"Djeca su nam poslana kao kiša koja dolazi iz duše, kao bogatstvo i obećanje koje se uvijek može ispuniti; naša je dužnost da se pobrinemo i da pripomognemo da se sve to zaista i ispuni. Nemojte misliti da je dijete slabić; dijete je ono što će izgraditi ličnost čovjeka."
Maria Montessori

Zlostavljanje djece nije nov problem. Surova kažnjavanja, usmrćivanja i zlostavljanja djece poznata su bila i u najranijim kulturama. Žrtvovanja i ubijanja djece te nasilna odgajanja bila su rezultat hronične materijalne oskudice u ranim ljudskim zajednicama, ali i posljedica ekstremnih nejednakosti i eksploatacije (Šućur, 2005, 23). Sve do modernih vremena fizičko i psihičko nasilje nad djecom smatralo se sastavnim dijelom roditeljskog prava. Danas, nasilje nad djecom predstavlja globalni fenomen i svakodnevni događaj (Hyder, Mac Veigh, 2007). Svakoga dana su milioni djece u svijetu žrtve nasilja, psihičkog i fizičkog zlostavljanja i

[12] Doc. dr. Nikolina Grbić Pavlović, Visoka škola unutrašnjih poslova Banja Luka, e-mail: nikolinagrbic@blic.net

seksualnog iskorištavanja. Zločini se događaju u porodici, školi ili u sredini u kojoj se dijete kreće, a izvršioci su često oni kojima djeca najviše vjeruju.

O problemu definisanja nasilja nad djecom raspravlja se već nekoliko desetina godina. Unatoč žustrim raspravama, još uvijek postoje znatne poteškoće u definisanju pojma zlostavljanja djece. Ipak, definisanje i identifikovanje ove pojave je nužno radi mjerenja ove pojave, te radi prevencije i tretmana zlostavljanja.

Prema preporukama konferencije koju je 1989. godine sazvao *National Institute of Child Health and Human Development* iz Sjedinjenih Američkih Država, zlostavljanje ili maltretiranje obuhvata ponašanja usmjerena prema drugim osobama koja krše važeće norme i predstavljaju znatan rizik za pojavu fizičke ili emocionalne štete na osobama. Takva ponašanja uključuju akcije i propuste koji su namjerni i nenamjerni. Prema tome, pojam „zlostavljanja djece" odnosio bi se na široki skup ponašanja koja su rizična sa stajališta djece i adolescenata (maltretiranje, nasilje, zapuštanje i slično), a koja manifestuju, prije svega, roditelji, članovi porodice i drugi staratelji (Šućur, 2005, 23).

"Nasilje nad djecom svih oblika,…realnost današnjice i ozbiljan kriminalni fenomen, galopirajući teror bez granica. Ono je danas globalni problem i izrazito sigurnosno pitanje vezano uz budućnost čovječanstva, jer djeca su naša budućnost. Društvena opasnost i štetnost nasilja nad djecom je vrlo velika i rezultira dalekosežnim posljedicama (Modly, 2004, 71)."

Postoje tri glavna oblika zlostavljanja (koja se i u literaturi najčešće navode), iako je moguće da dijete bude tokom života zlostavljano na više načina (Đuderija i drugi, 2006, 7):

- emocionalno (ili psihološko) zlostavljanje,
- fizičko zlostavljanje i
- seksualno zlostavljanje.

Uz navedene kategorije mnogi autori često dodaju i kategoriju zanemarivanja, odnosno zapostavljanja djece. Naravno, uvijek moramo imati u vidu da se sve navedene forme nasilja prema djetetu međusobno mogu kombinovati. To se naročito odnosi na seksualno nasilje, koje po svojoj sadržini predstavlja poseban oblik nasilja prema djeci, ali je po svojim posljedicama uvijek kombinovanog tipa (Clark, 1989).

2. KRIVIČNOPRAVNI POLOŽAJ DJECE I MALOLJETNIKA ŽRTAVA KRIVIČNOG DJELA

Dječija prava, kao posebna kategorija ljudskih prava, prvi put su uspostavljena Deklaracijom o pravima djeteta iz 1959. godine. Danas jedan od najvažnijih dokumenata svakako je Konvencija o pravima djeteta (1989) sa dva prateća protokola, i to: Fakultativni protokol uz Konvenciju o pravima djeteta o prodaji djece, dječijoj prostituciji i pornografiji (2000) i Fakultativni protokol uz Konvenciju o pravima djeteta o zabrani učešća djece u oružanim sukobima (2000). Na regionalnom planu od posebne su važnosti aktivnosti Savjeta Evrope povodom afirmisanja prava djece i maloljetnika i njihove zaštite. Tako je Savjet zauzeo jasan stav o problemu seksualnog zlostavljanja i iskorišćavanja djece u dvije preporuke, i to:

Preporuka R (91) 11 o seksualnom iskorišćavanju, prostituciji i trgovini djecom i mladima i Preporuka Rec (2001) 16 o zaštiti djece od seksualnog iskorišćavanja.
Zaštita interesa žrtve jedan je od imperativa savremenih krivičnih zakonodavstava, uključujući i maloljetnička krivična zakonodavstva (Radulović, 2010, 74). U našem domaćem zakonodavstu, u Republici Srpskoj, donesen je poseban Zakon o zaštiti i postupanju sa maloljetnicima u krivičnom postupku Republike Srpske[13]. Iako je u najvećem dijelu Zakona regulisan krivičnopravni položaj maloljetnih učinilaca krivičnih djela, ipak šesti dio ovog Zakona[14], predstavlja posebnu cjelinu i bavi se djecom i maloljetnicima kao žrtvama, odnosno oštećenim krivičnim djelom. Tako je predviđeno da sudija za maloljetnike, odnosno vijeće kojim predsjedava sudija za maloljetnike ili sudija koji ima posebna znanja sudi i punoljetnim učiniocima za krivična djela propisana Krivičnim zakonom, kada se u krivičnom postupku kao oštećeni pojavljuje dijete i maloljetno lice.[15]

Sljedeća karakteristika ovih odredaba odnosi se na krivična djela iz Krivičnog zakona[16] kod kojih se dijete, odnosno maloljetno lice najčešće nalazi u ulozi oštećenog. To su ona krivična djela koja se, s obzirom na posljedicu izvršenog djela, smatraju naročito teškim u odnosu na djecu i maloljetnike. Kod ovih krivičnih djela prema stavu zakonodavca uloga maloljetnog oštećenog lica posebno je izražena, a krivični postupak hitan.[17]

Radi se o sljedećim krivičnim djelima[18], i to:

- Ubistvo;
- Teško ubistvo;
- Ubistvo djeteta pri porođaju;
- Navođenje na samoubistvo i pomaganje u samoubistvu;
- Teška tjelesna povreda;
- Otmica;
- Protivpravno lišenje slobode;
- Zlostavljanje;
- Silovanje;
- Obljuba nad nemoćnim licem;
- Polno nasilje nad djetetom;
- Obljuba zloupotrebom položaja;
- Zadovoljavanje polnih strasti pred drugim;
- Trgovina ljudima radi vršenja prostitucije;
- Iskorišćavanje djece i maloljetnih lica za pornografiju;
- Proizvodnja i prikazivanje dječije pornografije;

[13] Zakon o zaštiti i postupanju sa maloljetnicima u krivičnom postupku Republike Srpske (Službeni glasnik Republike Srpske, br. 13/10, 61/13).
[14] Odredbe članova od 184. do 190.
[15] Član 184.
[16] Krivični zakon Republike Srpske (Službeni glasnik Republike Srpske, br. 49/03, 108/104, 37/06, 73/10, 1/12).
[17] Član 190.
[18] Članovi Krivičnog zakona, kako slijedi po navedenim krivičnim djelima: 148, 149, 151, 153, 156, 165, 166, 167, 193, 194, 195, 196, 197, 198, 199, 200, 201, 204, 205, 207, 208, 209, 210, 225, 233, 234.

- Rodoskrnavljenje;
- Vanbračna zajednica sa maloljetnim licem;
- Oduzimanje maloljetnog lica;
- Zapuštanje i zlostavljanje maloljetnog lica;
- Nasilje u porodici ili porodičnoj zajednici;
- Kršenje porodičnih obaveza;
- Izbjegavanje davanja izdržavanja;
- Omogućavanje uživanja opojnih droga;
- Razbojništvo;
- Razbojnička krađa.

Osim navedenih krivičnih djela navedenih, postoji i niz drugih krivičnih djela kod kojih dijete ili maloljetnik može da bude žrtva, iako to iz opisa djela nije vidljivo (Klajn-Tatić, 2009). Iako takva djela nisu na popisu krivičnih djela ostavlja se mogućnost sudiji za maloljetnike da sudi odraslom učiniocu tog krivičnog djela kad je ono učinjeno na štetu djeteta, odnosno maloljetnog lica. Isto tako, tužilac za maloljetnike ima diskreciono pravo da pokrene krivični postupak protiv punoljetnih učinilaca i drugih krivičnih djela (pored pobrojanih) propisanih Krivičnim zakonom, ukoliko ocijeni da je to potrebno radi posebne zaštite ličnosti djece i maloljetnika koja kao oštećeni učestvuju u krivičnom postupku.[19]

Takav postupak prema punoljetnim licima se odvija prema pravilima Zakona o krivičnom postupku Republike Srpske[20] osim u dijelu koji se odnosi na kazneni nalog.

Prema Zakonu postoje i dvije naročite karakteristike ovog krivičnog postupka, a koje se tiču posebnih znanja koja moraju posjedovati najvažniji učesnici ovog postupka (Nikolić-Ristanović, 2003, 6). Tako istragu u ovakvom postupku može da vodi isključivo tužilac koji je stekao posebna znanja iz oblasti prava djeteta i krivičnopravne zaštite maloljetnih lica, a u istražnim radnjama mogu da učestvuju samo policijski službenici koji su prošli edukaciju iz oblasti prava djece i maloljetnika.

3. SASLUŠANJE DJECE I MALOLJETNIKA ŽRTAVA KRIVIČNIH DJELA

Oduvijek se, naročito prema kriminalističkim pravilima, pravila razlika prilikom saslušavanja pojedinih kategorija svjedoka. Tako se razlikuju svjedoci po osnovu: tipičnih karakteristika svjedoka, starosti, polne pripadnosti, zdravstvenog stanja, zainteresovanosti, strane predlaganja, istinitosti iskaza i načina saznavanja (Simonović, 2004, 165-166). Najviše pažnje prilikom saslušavanja, u svakom slučaju, imaju svjedoci – žrtve krivičnih djela.
U poređenju sa drugim žrtvama, svijest o potrebi prilagođavanja uobičajenog načina ispitivanja svjedoka specijalnim potrebama i interesima djece je, u poređenju sa drugim posebno ugroženim kategorijama žrtava, najviše razvijena (Nikolić-Ristanović, 2003, 6).

[19] Član 194. stav 2.
[20] Zakon o krivičnom postupku Republike Srpske (Službeni glasnik Republike Srpske, br. 53/12).

Pribavljanje iskaza od djece i maloljetnika ima specifičnosti koje se pri saslušanju moraju uvažavati, a koje su rezultat psihofizičke nerazvijenosti i nezrelosti djeteta, nepostojanje životnog iskustva, ekstremne sugestibilnosti i bogate fantazije (Simonović, 2004, 172).

U većini zemalja Evropske Unije djeca se tretiraju i ispituju sa više obzira i empatije nego druge žrtve (Nikolić-Ristanović, 2003, 6). Najnovija viktimološka dostignuća pokazuju da osim štete koju djeca trpe kao rezultat krivičnog djela (primarna viktimizacija), često je prisutna i dalja šteta koja nastaje kao neadekvatna reakcija njihove socijalne sredine (sekundarna viktimizacija) (Carić, 2004, 187). Da bi se takva šteta spriječila ili bar umanjila Zakon sadrži precizna uputstva za postupanje sa djecom i maloljetnicima kao žrtvama krivičnih djela (Simović i drugi, 2015, 531), koja su slična uputstvima drugih zemalja. Tako se kao najbolja praksa, u smislu svođenja sekundarne viktimizacije na minimum, pokazala praksa onih zemalja čija zakonodavstva omogućavaju sljedeće:

- Ispitivanje od strane specijalno obučenih policijskih službenika;
- Ispitivanje preko stručnjaka, npr. psihologa, ili uz pomoć stručnjaka, npr. socijalnog radnika;
- Ispitivanje u prisustvu lica u koje dijete ima povjerenje;
- Ispitivanje u prostoru u kome se dijete oseća prijatno;
- Ispitivanje preko video linka, pri čemu se dijete nalazi u zasebnoj prostoriji;
- Korišćenje video zapisa kao dokaza na sudu, da bi se izbjeglo davanje iskaza više puta (Nikolić-Ristanović, 2003, 6).

Prilikom saslušanja djece i maloljetnika jedna od osnovnih odredbi svih zakonodavstava u regionu jeste da su svi učesnici u postupku prema djeci i maloljetnicima dužni naročito obazrivo se ponašati prema njima (Singer, 1998, 223). Način ispitivanja djece i maljoljetnih lica već odavno je ustanovljen kriminalističkom praksom, i u tom smislu oduvijek je davao manje – više pozitivne rezultate. Saslušanju ovih lica uvijek treba pristupiti individualno, uvažavajući pri tome tipične uzrasne karakteristike. Svakako da se razlikuje saslušanje djece u preškolskom uzrastu, djece u školskom uzrastu i djece u periodu mladalaštva i puberteta.

Potrebno je uvažavati sljedeća taktička i tehnička pravila kriminalistike u slučaju saslušanja djece i maloljetnika (Simonović, 2004, 174-176):

- Djecu i maloljetnike treba da saslušava specijalizovani radnik za ovu vrtsu saslušanja;
- Izgled prostorije u kojoj se saslušava dijete treba prilagoditi svakodnevnom dječijem iskustvu;
- Detaljno pripremiti saslušanje i prikupiti podatke o ličnosti djeteta ili maloljetnika;
- Dijete treba odvojiti od roditelja i ostalih svjedoka dok se od njega ne pribavi iskaz;
- Po mogućnosti prvo saslušanje djeteta treba da bude i posljednje;
- Nastojati uspostaviti kontakt, povjerenje i oslobađanje od straha djeteta;
- Saslušanje sprovoditi u mirnoj atmosferi;
- Podsticati prisjećanje djeteta i maloljetnika;
- Konsultovati i druge stručnjake;
- Kontrolisati iskaz djeteta i maloljetnika;

- Nastojati video i zvučno obezbjediti iskaz djeteta i maloljetnika.

Tako je i u Republici Srpskoj predviđeno da se saslušanje djeteta ili maloljetnika u pravilu obavlja uz pomoć pedagoga, psihologa ili drugog stručnog lica.[21] Ukoliko se kao svjedok saslušava dijete (do 14 godina) ili mlađi maloljetnik (od 14 do 16 godina) oštećen krivičnim djelom iz člana 184. Zakona, saslušanje se može provesti najviše dva puta.

Kada se saslušanje obavlja u prostorijama Ministarstva unutrašnjih poslova Republike Srpske, ono se saslušava u posebno opremljenim prostorijama (slika 1 i slika 2), gdje tužilac ili ovlašćeno službeno lice saslušava svjedoka putem tehničkih uređaja za prenos slike i zvuka, a bez prisustva tužioca ili ovlašćenog službenog lica u prostoriji gdje se svjedok nalazi. Dijete ili mlađe maloljetno lice može se saslušati u svom stanu ili drugom prostoru u kome boravi ili centru za socijalni rad. Saslušanje djeteta ili maloljetnika se u pravilu obavlja uz pomoć pedagoga, psihologa ili drugog stručnog lica. Angažovanje ovih lica, mnogi autori navode, je neohodno jer se smatra da oni po samoj prirodi svoje profesije bolje razumiju oštećeno lice ove starosne kategorije i na taj način doprinose da se izbjegnu moguće štetne posljedice vođenja krivičnog postupka prema djeci i maloljetnicima (Bejatović, Soković, 2009, 212).

Slika 1. Prostorija za maloljetnike 1

Slika 2. Prostorija za maloljetnike 2

Naime, iako su policijski službenici završili potrebnu edukaciju i postali sertifikovani za rad sa djecom i maloljetnicima, Zakonom im nije dozvoljeno da direktno razgovaraju sa djecom i maloljetnicima oštećenim krivičnim djelom. U praksi to izgleda ovako: pedagog, psiholog ili drugo stručno lice sjede sa djetetom ili maloljetnikom u jednoj prostoriji (slika 1), dok u drugoj prostoriji sjede policijski službenik, tužilac, advokat, roditelj ili staratelj i druga lica koja mogu prisustvovati saslušanju maloljetnika (slika 2). Maloljetniku pitanja postavlja isključivo lice koje se nalazi s njim u prostoriji, dok sa tim licem iz druge prostorije ostali

[21] Član 186. Zakona. Međutim, već pomenutim idejama o promenama postojećeg *lex specialis* zakona u Srbiji relativizuje se prisustvo stručnih lica, prilikom saslušanja maloljetnog oštećenog, u svojstvu svjedoka. Ideja je da se, ubacivanjem prefiksa "po pravilu", stvori normativna podloga za izuzetno odstupanje od obaveze saslušanja maloljetnog oštećenog, u prisustvu stručnih lica odgovarajućeg profila (Knežević, 2010, 326).

učesnici mogu razgovarati putem motorola i bubice koju kod sebe nosi stručno lice. Takav način ispitivanja se snima, a snimak se može koristiti na sudu kako se ne bi dijete ponovo ispitivalo na okolnosti događaja. Ovakav način ispitivanja naišao je mnogobrojne kritike od strane radnika iz prakse (naročito policijskih službenika) koji rade u praksi.

Tabela 1: Saslušanje djece i maloljetnika u specijalizovanim prostorijama u Ministarstvu unutrašnjih poslova Republike Srpske (juli-decembar 2015. godine)

Centar javne bezbjednosti	**Broj ispitanih (po polu)**		**Svojstvo ispitanog lica**			**Snimanje razgovora**	**Stručno osoblje**		
	M	**Ž**	**Svjedok**	**Žrtva**	**Počinilac**		**Inspektor**	**Soc. radnik**	**Psiholog**
Banja Luka	2	6	1	7	0	8	8	8	6
Istočno Sarajevo	11	2	3	3	7	2	13	13	2
Prijedor	18	8	10	6	10	11	5	1	1
Doboj	-	3		3		3	3	3	3
Trebinje	2	-			2	-	1	1	-
Bijeljina	Nije koristio prostorije sa audio i video snimanjem								
Ukupno	33	19	14	19	19	24	30	26	12

U tabeli 1 prikazani su neki od parametara koji se vode u Evidenciji o korišćenju prostorija za maloljetnike u organizacionim jedinicama Ministarstva unutrašnjih poslova Republike Srpske za period od jula do decembra 2015. godine. Navedene prostorije imaju svi centri javne bezbjednosti u Republici Srpskoj, kao i Uprava za policijsko obrazovanje (slika 1 i slika 2). U prostorijama u Upravi za policijsko obrazovanje navedene prostorije se koriste isključivo za održavanje vježbi sa studenatima Visoke škole unutrašnjih poslova, praktične nastave za polaznike Policijske akademije i edukaciju pripadnika Ministarstva unutrašnjih poslova republike Srpske prilikom održavanja specijalizovanih seminara i kurseva.

Prostorije za maloljetnike po centrima javne bezbjednosti koriste se isključivo u operativne svrhe. Iz tabele 1 je vidljivo da se prostorije za maloljetnike koriste na različit način od strane pripadnika policije. Određeni centri navedene prostorije koriste kako za ispitivanja djece i maloljetnika koji su žrtve krivičnih djela, tako i za maloljetne svjedoke i počinioce krivičnih djela. U nekim centrima, prostorije za maloljetnike, koriste se samo za djecu i maloljetnike koji su žrtve krivičnih djela, dok se u nekim centrima (kao što je CJB Bijeljina) prostorije i ne koriste. Takođe, evidentno je da se sva salušanja i ne snimaju audio i

video opremom. Zapravo, snimaju se sva saslušanja maloljetnika žrtava krivičnih djela, dok se saslušanja maloljetnih počinilaca i svjedoka ne snimaju uvijek i u pravilu. Evidentno je da je u većini slučajeva prilikom saslušanja djece i maloljetnika prisutan, pored inspektora za maloljetnike i socijalni radnik i/ili psiholog.

Novi način saslušavanja djece i maloljetnika, audio i video opremom, uz aktivno učešće drugih lica u vođenju postupka (psiholozi, pedagozi, socijalni radnici), pored pozitivnih mišljenja, donijela su i mnoge dileme kod organa istrage. Iako je ovakakav način rada predviđen Zakonom, nalazimo da ovo rješenje i nije najadekvatnije. Prosto je nemoguće da saslušanje lica (bilo da se radi o osumnjičenom licu, bilo da se radi o žrtvama krivičnog djela) obavlja bilo ko osim ovlašćenih službenih lica, odnosno policijskih službenika ili tužilaca. Psiholozi, pedagozi ili druga stručna lica nemaju dovoljno znanja iz oblasti kriminalistike i prava, a što je u pravilu osnovno za obavljanje bilo kakvog razgovora na okolnosti krivičnog djela. Često se dešava da inspektor mnogo više izgubi vremena „upoznajući“ stručna lica sa obilježjem krivičnog djela, dokazima, uviđajem i slično, nego što bi trajalo samo ispitivanje djeteta ili maloljetnika. Stručna lica bi trebalo da budu servis i podrška policijskim službenicima i tužiocu prilikom pripreme samog razgovora sa djecom i maloljetnicima, te da prate njihovo saslušavanje iz druge prostorije i u svakom trenutku reaguju ukoliko procijene da ovlašćeno lice ne vodi saslušanje na adekvatan način. Jer, ipak, policijskom službeniku čiji je osnovni opis poslova da upravo vodi ovakve razgovore, sa dodatnim znanjima iz oblasti prava djece i maloljetnika i sklonošću sa rad sa ovom kategorijom učinilaca krivičnih djela ili žrtava krivičnog djela, u potpunosti pristaje da direktno vrši saslušanje djece i maloljetnika. A što je, možda i najvažnije u ovom slučaju, potrebno je naglasiti da stručna lica (pedagozi, psiholozi i drugi) nisu ovlašćeni da vode krivični postupak (Perić, 2007, 263).

Ukoliko se dijete ili maloljetnik ponovo saslušava i na sudu, saslušanje se obavlja na način da sud, stranke u postupku i branilac mogu postavljati pitanja, a da ne budu prisutni u istoj prostoriji sa svjedokom. Saslušanje djeteta ili maloljetnika se obavlja tako da se pitanja postavljaju posredstvom suda, a po potrebi uz pomoć pedagoga, psihologa ili drugog stručnog lica. Na isti način se saslušavaju djeca ili maloljetnici koji su svjedoci - očevidci učinjenog krivičnog djela iz člana 184. ovog zakona.

Takođe, propisana je zabrana suočenja djece i maloljetnika sa osumnjičenim ukoliko se saslušava dijete ili maloljetnik koji je ozbiljno fizički ili psihički traumatizovan okolnostima pod kojima je izvršeno krivično djelo ili pati od ozbiljnih psihičkih poremećaja koji ga čine posebno osjetljivim.[22]

Nadalje, ukoliko prepoznavanje osumnjičenog, odnosno optuženog vrši maloljetnik oštećen krivičnim djelom, ili je očevidac učinjenog krivičnog djela, takvo prepoznavanje u

[22] Član 187.

svim fazama postupka vrši se na način koji u potpunosti onemogućava da osumnjičeni, odnosno optuženi, vidi maloljetno lice.[23]

4. ZAKLJUČAK

S obzirom na to da je problem nasilja nad djecom, a posebno seksualna zlostavljanja djece i ozbiljan i složen, u njegovom rješavanju neophodna je saradnja stručnjaka različitih profila. Nažalost, u praksi, teret ovog problema nosi izuzetno mali broj stručnjaka.

Kako se ne bi stvarale dodatne traume kod djeteta usljed osjećaja straha i krivice i pod sjećanjem na kriminalni događaj prilikom saslušanja djece i maloljetnika žrtava krivičnih djela potrebno je uključiti stručna lica u pripremu ovih razgovora. Svakako da je jako važno da tužioci i policijski službenici, kao i sudije, budu adekvatno edukovani za rad sa ovom kategorijom žrtava. Ponekad i sama edukacija nije dovoljna, te je potrebno za takav rad angažovati ona lica koja imaju naročitu sklonost sa rad sa djecom i maloljetnicima. U tom smislu potrebno je raditi na stalnom osposobljavanju socijalnih službi, stalnu edukaciju socijalnih radnika i policije, uključivanje zdravstvenih ustanova, škola, posebno centara za mentalno zdravlje, uspostavljanje i definisanje koordinacije između institucija koje se bave ovim problemom.

Kada je u pitanju saslušavanje djece i maloljetnika žrtava krivičnih djela, potrebno je dataljnije pravno regulisati sam način saslušavanja ove kategorije žrtava krivičnih djela. Ovo je naročito važno kako bi se na teritoriji cijele Republike Srpske uspostavila jednaka praksa u postupanju. U tom smislu predlaže se korišćenje audio i video opreme u svakom slučaju gdje su djeca i maloljetnici oštećeni krivičnim djelom, svjedoci, ali i učinioci krivičnog djela. Takođe, odredbu o stručnim licima gdje se navodi da se djeca i maloljetnici ispituju isključivo posredstvom ovih lica potrebno je mijenjati. Naime, ova lica trebalo bi da budu servis i podrška policijskim službenicima i tužiocu prilikom pripreme samog razgovora sa djecom i maloljetnicima, te da prate njihovo saslušavanje iz druge prostorije i u svakom trenutku reaguju ukoliko procijene da ovlašćeno lice ne vodi saslušanje na adekvatan način. Kada su u pitanju policijski službenici i tužioci ovdje je potrebno voditi računa da, pored obavezne edukacije iz oblasti prava djece i maloljetnika koju trebaju imati, ova lica moraju imati i naročitu sklonost za rad sa djecom i maloljetnicima.

Pri tome je neizostavna i medijska kampanja u cilju edukacije stanovništa. Veoma važno je da nadležne institucije u svom radu sa djecom-žrtvama nasilja imaju pravovremenu i kvalitetnu komunikaciju, kako u dijelu preventivnog rada, tako i u dijelu „obrade slučaja“, ali i po okončanju predmeta pred nadležnim organom. Edukacija, kampanje i različiti načini saradnje sa djecom u vezi sa problemom nasilja su metode koje je potrebno dalje sistemski razvijati.

[23] Član 188.

LITERATURA

Bejatović, S., Soković, S. (2009). *Maloletničko krivično pravo*. Kragujevac: Pravni fakultet Univerzitet u Kragujevcu.

Carić, A. (2004). *Zakon o sudovima za mlade. Zagreb*: Narodne novine.

Clark, L. M.G. (1989). *Feminist Perspectives on Violence Against Women and Children: Psychological, Social Service, and Criminal Justice Concerns.* Canadian Journal of Women&the Law, Vol. 3 Issue 2, 420-431.

Đuderija, S., Milosavljević, M., Malešić, S., Jerković, A., Smajić, Z. (2006). *Inicijalni izvještaj o nasilju nad djecom u Bosni i Hercegovini*. Sarajevo: Vijeće za djecu Bosne i Hercegovine.

Hyder, T., Mac Veigh, J. (2007). Gender-based violence against children in emergencies: Save the children UK's response. *Gender & Development*, Vol 15, Issue 1, 81-93.

Knežević, S. (2010). *Maloletničko krivično pravo – materijalno, procesno i izvršno.* Niš: Pravni Fakultet u Nišu.

Modly, D. (2004). Prevencija nasilja nad djecom (kriminalistički aspekt). *Kriminalističke teme*, godište 3, broj 3-4.

Nikolić Ristanović, V. (2003). Podrška žrtvama i sprečavanje sekundarne viktimizacije: savremena zakonska rešenja i praksa. *Temida,* broj 1.

Perić, O. (2007). *Komentar Zakona o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica,* 2. dopunjeno izdanje. Beograd: Službeni glasnik.

Radulović, Lj. (2010). *Maloletničko krivično pravo*. Beograd: Pravni Fakultet Univerziteta u Beogradu.

Simonović, B. (2004). *Kriminalistika.* Kragujevac: Pravni Fakultet u Kragujevcu, Institut za pravne i društvene nauke.

Simović, M., Jovašević, D., Mitrović, Lj., Simović, M. (2015). *Maloljetničko krivično pravo*, 2. izdanje. Banja Luka: Međunarodno udruženje naučnih radnika – AIS.

Singer, M. (1998). *Kaznenopravna odgovornost i zaštita mladeži.* Zagreb: Nakladni zavod Globus.

Šućur, Z. (2005). *Nasilje nad djecom. Kriminologija delikata nasilja*. Zagreb: Globus, Zagreb.

Klajn Tatić, V. (2009). Djeca kao subjekti biomedicinskih istraživanja ili ogleda u svjetlu medicinskih, etičkih i pravnih razmatranja. *Pravni život*, 9, 837-853.

Zakon o zaštiti i postupanju sa maloljetnicima u krivičnom postupku Republike Srpske (Službeni glasnik Republike Srpske, br. 13/10, 61/13)

Krivični zakon Republike Srpske (Službeni glasnik Republike Srpske, br. 49/03, 108/104, 37/06, 73/10, 1/12)

Zakon o krivičnom postupku Republike Srpske (Službeni glasnik Republike Srpske, br. 53/12).

Nikolina Grbić Pavlović

THE SPECIFICS OF HEARING CHILDREN AND MINORS AS PARTIES DAMAGED BY CRIMINAL OFFENCE

Summary

In addition to the fact that children and minors nowadays appear more often to be perpetrators of criminal and minor offences, it is evident that they also often appear as victims of the negative impacts and events occurring in their communities. Newer victimological findings indicate that children easily become victims of certain criminal offences committed (mostly) by adults at children's expense. This is the main reason why many types of legislation are increasingly improving the processes related to children and minors as crime victims. That is the case with the new Law on Protection and Treatment of Minors in Criminal Procedure of the Republic of Srpska, which emphasizes the nature of the specific protection of children and minors during their hearing as damaged parties in criminal offences. The particular focus is given to the adequate approach by authorized persons during children and minors' hearing, as well as to the use of technical devices for transferring image and sound. It is this type of children and minors' hearing that is the main subject of this paper. The paper will also present information on the use of specially-equipped facilities for hearing minors, used in the work by the Ministry of Internal Affairs of the Republic of Srpska.

Key words: *children and minors, victims, hearing, approach to and manner of hearing, technical devices for transferring image and sound.*

STRUČNI RAD

Josip Medved[24]
Ante Orlović[25]
Jure Tadić[26]

SIGURNOST CESTOVNOG PROMETA – PRIMJENA SUVREMENE TEHNOLOGIJE I METODA U PREVENTIVNO-REPRESIVNOM DJELOVANJU PROMETNE POLICIJE

Sažetak

Policija je važan faktor implementacije i razvoja sigurnosti u cestovnom prometu. Uloga policije u ovom kontekstu suštinski je uređena Zakonom o policijskim poslovima i ovlastima te Zakonom o sigurnosti prometa na cestama. Postupanje policijskih službenika u obavljanju poslova nadzora i upravljanja prometom na cestama razumijeva primjenu suvremene tehnologije i metoda. One značajno doprinose profesionalizaciji, standardizaciji i efikasnosti u djelovanju prometne policije. Policijski službenici i vozila opremljeni su brojnim tehničkim uređajima koji značajno pojednostavljuju i unapređuju terensko postupanje policije u preventivnom i represivnom smislu. U svezi s navedenim mogu se izdvojiti: prijenosna računala (tableti) koja omogućavaju bolju komunikaciju, pristup informacijama te obavljanje administrativnih poslova; mobilne kamere koje se koriste u službenim vozilima ili na odorama prilikom postupanja; mobilni uređaji za automatsko očitavanje registarskih pločica koji se montiraju na službena vozila. Osim mobilnih uređaja, važnu ulogu za sigurnost cestovnog prometa imaju i fiksni uređaji (kamere) koji se postavljaju uz prometnice u svrhu nadzora brzine kretanja vozila i automatskog očitavanja registarskih pločica (ANPR). U odvijanju cestovnog prometa neizbježne su i prometne nesreće, a njihova sanacija (pravna, financijska) ima veliku značajnost. Sanacija se temelji na očevidima koje provede policijski službenici koristeći se pri tomu suvremenim tehnologijama i metodama (mjerenja mjesta događaja pomoću geodetskih uređaja, izrada situacijskih planova pomoću računalnih programa) u svrhu preciznosti, objektivnosti i efikasnosti svoga postupanja. Prikaz primjene suvremene tehnologije i metoda u preventivno-represivnom djelovanju prometne policije razmatran je kroz tri aspekta: personalno-postupovni, tehničko-tehnološki i metodološko-računalni. Primjenom suvremenih tehnoloških rješenja i metoda, s jedne strane, povećava se operativna učinkovitost policijskih službenika prometne policije na terenu i u postaji, dok se s druge strane osigurava brže, jednostavnije i preciznije lociranje i procesuiranje onih sudionika u prometu koji svojim ponašanjem krše prometne propise i ugrožavaju sigurnost cestovnog prometa.

Ključne riječi: *sigurnost cestovnog prometa, djelovanje prometne policije, suvremene tehnologije i metode.*

---

[24] Josip Medved, bacc. crim., policijski službenik, MUP RH, PU zagrebačka, I. postaja prometne policije
[25] dr. sc. Ante Orlović, profesor visoke škole, MUP RH, Policijska akademija, Visoka policijska škola
[26] Jure Tadić, struč. spec. crim., MUP RH, Policijska akademija, Policijska škola "Josip Jović

1. UVOD

Osiguranje zaštite i sigurnosti sudionika u cestovnom prometu temeljna je zadaća policijskih službenika prometne policije. Policijski službenici svoje zadaće izvršavaju provođenjem preventivnih i represivnih aktivnosti te na taj način osiguravaju poštovanje prometnih propisa, smanjenje broja prometnih nesreća i njihovih posljedica. Većina sudionika u cestovnom prometu uredni su i odgovorni građani koji postupaju u skladu sa znakovima i naredbama ovlaštenih osoba, propisima o prometnim pravilima te prometnim znakovima postavljenim na cesti.[27] Oni izuzetci koji svojim ponašanjem krše prometne propise i ugrožavaju sigurnost ostalih sudionika u prometu – ciljana su populacija prema kojoj se usmjerava postupanje policijskih službenika prometne policije.

Suvremena tehnologija je u aktualnom vremenu neizostavno uključena u sve segmente života društvene zajednice, u privatnoj i poslovnoj sferi, pa je tako uvelike prisutna i u djelovanju policije uključujući i djelovanje policijskih službenika prometne policije. Raznovrsnu tehnologiju i suvremene metode koriste u radu policijski službenici kako bi što efikasnije i uspješnije osigurali sigurnost svim sudionicima u prometu na cestama. Razlozi korištenja suvremenih tehnika i metoda su različiti. One primarno olakšavaju i pojednostavljuju rad policijskim službenicima, ali istovremeno i povećavaju njihovu učinkovitost. One su važna potpora koja bitno doprinosi da postupanja policijskih službenika budu profesionalna i zakonita, a rezultati njihova postupanja ispravni i uredni. Suvremeni tehnički uređaji omogućavaju da se među velikim brojem sudionika u prometu na cestama precizno lociraju i izdvoje oni koji svojim ponašanjem ozbiljno krše prometne propise i ugrožavaju sigurnost ostalih sudionika u prometu. Uvođenjem suvremenih tehničkih uređaja u opus djelovanja prometne policije, i to onih uređaja za čiji rad nije potrebna prisutnost policijskog službenika – osigurava se brži i ekonomičniji postupak, a policijski službenici mogu se preusmjeriti na druge poslove koje uređajima nije moguće odraditi.

Uvođenje projekta e-policija u sustav djelovanja hrvatske policije, nabavka opreme iz proračunskih sredstava Ministarstva, ali i iz Nacionalnog programa za sigurnost cestovnog prometa[28] – značajno doprinosi tehnološkoj opremljenosti prometne policije koja je, u smislu raspoloživosti suvremenih tehnologija i sredstava za rad, vjerojatno najopremljenija operativna služba unutar MUP-a RH. Prikaz primjene suvremene tehnologije i metoda u preventivno-represivnom djelovanju prometne policije u ovom radu razmatramo kroz tri aspekta: *personalno-postupovni, tehničko-tehnološki i metodološko-računalni.* Naznačeni aspekti upućuju na aktualnu raznovrsnost i izdašnost suvremene tehnologije i metoda u radu prometne policije te na izniman potencijal njihove intenzivne implementacije u perspektivi – s obzirom na kontekst i ekspanziju informatičkog doba u kojem globalizirani svijet egzistira.

---

[27] Zakon o sigurnosti prometa na cestama, čl. 34, NN 67/08., 48/10., 80/13., 158/13., 92/14., 64/15. Zagreb: Narodne novine. (dalje: ZSPC).

[28] Nacionalni program za sigurnost cestovnog prometa dokument je kojeg je donijela Vlada Republike Hrvatske, a cilj mu je podizanje razine sigurnosti cestovnog prometa. Strategijom je definirano da se u periodu od 2011. do 2020. godine mora raditi na promjenama ponašanja sudionika u prometu, boljoj cestovnoj infrastrukturi, sigurnijim vozilima i učinkovitijoj medicinskoj skrbi nakon prometnih nesreća. NN 101/98., 15/00., 117/01., 199/03., 30/04., 77/09. i 145/10. Zagreb: Narodne novine.

2. SUVREMENE TEHNOLOGIJE I METODE DJELOVANJA PROMETNE POLICIJE – PERSONALNO-POSTUPOVNI ASPEKT

• **Prijenosna računala – tableti.** U dvadeset i prvom stoljeću svakodnevni život nezamisliv je bez uporabe mobilnih komunikacijskih uređaja. Mobilne "pametne telefone" i prijenosna računala koriste svi, od tinejdžera do direktora korporacija. Koriste ih za e-mail poruke, plaćanje računa, provjere bankovnih računa, trgovanje na burzama kapitala i za štošta drugo. Unatoč relativno teškom i sporom probijanju novih suvremenih tehnologija i metoda u rad državnih službi, uvođenjem projekta e-policija u Ministarstvo unutarnjih poslova policijski službenici na terenu su zadužili prijenosna računala – tablete i koriste ih prilikom obavljanja službenih zadataka. Prednosti i mogućnosti rada s uređajem su brojne.

Operativno dežurstvo policijskim službenicima na teren šalje radni nalog u digitalnom obliku. Osim naloga prosljeđuje im i dojave o događajima na koje se policijski službenici upućuju. Na ovaj način smanjuje se intenzitet komunikacije na sredstvima veze i ostavlja više prostora u eteru za hitne slučajeve. Olakšava se i rad policijskim službenicima u operativnim dežurstvima koji ne moraju dojave prenositi usmeno radioуređajima, čekati povratne informacije i sve to opet unositi u računalo. Dodjeljivanjem zadataka, odnosno prosljeđivanjem dojava policijskim službenicima putem računala – tableta neposredni rukovoditelji imaju bolji izravan uvid u trenutne zadaće policijskih službenika na terenu te ih mogu kvalitetnije nadzirati, raspoređivati i usmjeravati njihov rad.

Pomoću tableta policijski službenik može na mjestu počinjenja prekršaja provjeriti identitet osobe uvidom u fotografiju koja se nalazi u informacijskom sustavu MUP-a te, primjerice ostvariti uvid u evidencije vozačkih dozvola i vozila i u operativne evidencije prekršaja. Policijski službenik na terenu u tablet će unijeti osnovne podatke o nadziranoj osobi poput OIB-a ili registarske oznake i odmah ostvariti pristup bazi podataka informacijskog sustava. Ova mogućnost ubrzava postupanje policijskih službenika koji u istom trenutku imaju podatke o vozilu i osobi prema kojoj postupaju te u skladu s tim mogu odgovarajuće djelovati. Ne moraju čekati da dođu na red i provjere izvršavaju putem radioуređaja čime se rasterećuje komunikacijski kanal i rad operativnog dežurstva.

S obzirom na to da većina policijskih poslova rezultira pisanjem izvješća, tableti osiguravaju značajno smanjenje "papirologije" koja opterećuje policijske službenike na terenu. Velik broj pismena moći će se sastaviti i pohraniti u tabletu i tako osigurati uštedu u papiru, kopirnim uređajima i skladišnom prostoru. Pismena sastavljena na tabletu su urednija, preciznija i sa svim relevantnim podacima, a policijski službenici manje vremena provode sastavljajući ih te se više posvećuju operativnom radu. Za slučaj potrebe pismeno će se uvijek moći otvoriti i po potrebi isprintati, ako ga je potrebno uputiti nekoj drugoj ustrojstvenoj jedinici ili drugim institucijama. U dosadašnjoj praksi da bi policijski službenik prometne policije mogao izići na teren i obavljati poslove koji se od njega očekuju kod sebe mora imati cijeli niz obrazaca u papirnatom obliku. Tako on kod sebe mora imati obrasce prekršajnih naloga, zapisnike o alkotestiranju, potvrde o privremenom oduzimanju predmeta, naloge o određivanju mjera opreza, naloge za premještanje vozila, obrasce za obavljanje očevida, L1 formulare. Popunjavanje tih pismena zahtijeva dosta vremena, a zbog nečitkog ili nepravilnog ispisivanja dolazi do pogrešaka i propusta u radu. To za posljedicu ima obustavljanje postupaka protiv

počinitelja prekršaja i njihova oslobađanja od odgovornosti za počinjena djela u kasnijim postupcima. Nakon što policijski službenik na terenu ispiše pismena, ona se moraju posebno unositi u informacijski sustav i baze podataka. Prilikom tog procesa osobe koje unose pismena moraju "dešifrirati" rukopise, ispravljati pogreške, a postoji i mogućnost da prilikom prepisivanja dođe do pogrešaka. Ovakav postupak zahtijeva veliki broj službenika, posebno u onim policijskim postajama u kojima se godišnje procesuira nekoliko desetaka tisuća prekršaja. Tableti omogućavaju policijskim službenicima da, ako utvrde da je osoba počinila nekakav prekršaj, unesu u digitalni obrazac neki od osnovnih podataka (poput JMBG-a ili OIB-a), nakon čega uređaj automatski povlači sve ostale osobne podatke i popunjava propisane obrasce koji se počinitelju mogu isprintati i uručiti njegove primjerke. Popunjeni obrasci tako su čitki, pregledni i točni te se odmah nalaze u informacijskom sustavu MUP-a pa ih nije potrebno naknadno unositi, prepisivati niti pohranjivati.

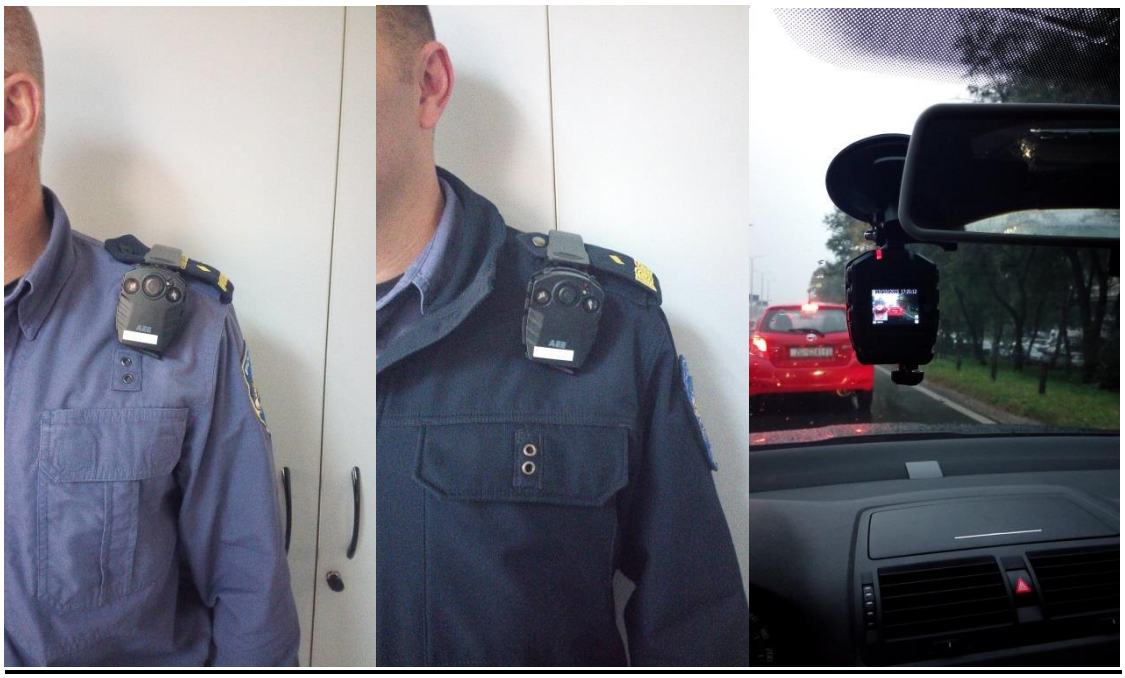
Velika prednost tableta manifestira se i prilikom legitimiranja osoba. Tijekom nadzora osobe odmah se može izvršiti unos legitimiranja u tablet pa su podaci o tome istog trenutka vidljivi u informacijskom sustavu svim policijskim službenicima koji provode kriminalistička istraživanja. To znači da se ne čeka povratak policijskog službenika s terena u policijsku postaju da bi se obrasci legitimiranja unijeli u informacijski sustav, što ponekad u sadašnjoj praksi zna potrajati i nekoliko dana.

Dodatnim usklađivanjem rada uređaja (tableta) i obukom policijskih službenika za rad s njima povećat će se učinkovitost policije i osigurati veća prisutnost policijskih službenika u ophodnjama na terenu.

- **Prijenosne kamere.** Postupanje policijskih službenika prometne policije u pravilu se zasniva na neposrednom kontaktu s građanima. U najvećem broju slučajeva taj kontakt je posljedica nekog oblika neprimjerenog (protuzakonitog) ponašanja građana zbog kojeg policijski službenik postupa kako bi to neprimjereno ponašanje identificirao i sankcionirao. Postupanja policijskih službenika u najvećem broju slučajeva završe bez štetnih i neželjenih posljedica, no ponekad ona rezultiraju napadima na policijske službenike, vrijeđanjima i omalovažavanjima. Predmetna postupanja mogu rezultirati prigovorima i pritužbama građana na rad policijskih službenika – građani često tako žele umanjiti svoju odgovornost za počinjeni prekršaj. Kako bi se takve i slične situacije izbjegle, u okviru pilot-projekta e-sigurnost koji se provodi na području policijskih uprava Zagrebačke, Splitsko-dalmatinske, Osječko-baranjske i Istarske provodi se i pilot-projekt "Sustav za upravljanje policijskim kamerama eKiosk". U okviru ovog projekta osigurana je operativna primjena malih prijenosnih videokamera koje snimaju audiozapise i videozapise (slika 1). Ciljevi pilot-projekta osim navedene zaštite policijskih službenika jesu i zaštita građana prilikom postupanja policijskih službenika, svođenje mogućnosti korupcije na minimum, opremanje policijskih službenika ICT opremom, probitak kriminalističkog istraživanja i automatiziranje radnih procesa u postupanju policijskih službenika.[29] Ovlast za korištenje kamera proizlazi iz Zakona o policijskim poslovima i ovlastima. Zakonom je propisano da je policija ovlaštena, u mjeri u kojoj je to potrebno, te radi nadzora zakonitosti postupanja policijskih službenika,

[29] Uputa Ravnateljstva policije, MUP-a RH za korištenje Sustava za upravljanje policijskim kamerama eKiosk, broj 511-01-50-72786/17-2015. od 10. 2. 2016. godine.

zvučno i vizualno ili na drugi način snimiti obavljanje policijskih poslova i primjenu policijskih ovlasti odgovarajućim tehničkim sredstvima, odnosno snimku na primjeren način objaviti.[30]



Slika 1: Prijenosne kamere postavljene na odoru policijskog službenika i u službeno vozilo

Policijski službenik prilikom otpreme službe zadužuje prijenosnu kameru, koristeći svoj privatni *username* i lozinku te se ona u tom trenutku registrira na njegovo ime. Kamera se uključuje jednostavnim pritiskom na prekidač. Policijski službenik sam procjenjuje i odlučuje u kojem će trenutku uključiti snimanje. Kada uključuje snimanje usmeno će, ako mu to situacija dozvoljava, upozoriti građanina prema kojem postupa da se postupanje snima. Nakon povratka u policijsku postaju kamera se vraća u svoje kućište, a snimljeni podaci se prenose na računalni server. Ako su sva snimljena postupanja bila uobičajena i ni po čemu se nisu isticala ili razlikovala od ostalih i neće se koristiti u postupcima, ona se čuvaju na serveru tri mjeseca nakon čega se automatski brišu. Snimke kamerom policijski službenik nema ovlasti brisati, a spomenutom Uputom o postupanju Ravnateljstva policije propisano je da ovlašteni rukovoditelj može snimke pregledavati, uređivati, presnimavati i propisno označavati te pohranjivati. Ako je snimljeno postupanje po nečemu bilo incidentno ili sporno, policijski službenik ili neposredni rukovoditelj takvu snimku označava kao incidentnu i ona se ne briše kako bi se mogla koristi u nekom od naknadnih postupaka. Uz snimku se može dodati opis snimke tako što se u posebno označen prostor upišu podaci o događaju poput broja predmeta ili unosa u dnevnik događaja. Prilikom nadzora i upravljanja prometom policijski službenici ove kamere koriste u raznim situacijama: snimaju postupanje pri utvrđivanju identiteta vozača; uporabe sredstava prisile; uhićenja; ako utvrde neki od prekršaja fotografiraju taj događaj ili ga snime videom; kod provođenja alkotestiranja sudionika u prometu snimaju postupanje i rezultate ispitivanja; dolaskom na mjesto događaja prometne nesreće kamerom

[30] Zakon o policijskim poslovima i ovlastima, čl. 3.a, NN 76/09., 92/14. Zagreb: Narodne novine.

snimaju zatečeno stanje i osobe prisutne na mjestu događaja, a ti podaci kasnije se mogu koristiti prilikom istraživanja. U pravilu sve što je interesantno za obavljanje policijskih poslova, a naknadno može koristiti policijski službenici snimaju prijenosnim kamerama.

Iako je ovaj projekt tek u začecima, od njega se mnogo očekuje. S obzirom na kratko vrijeme uporabe kamera u Republici Hrvatskoj ne može se u ovom trenutku napraviti kvalitetna evaluacija njihovih učinaka. No u Sjedinjenim Američkim Državama, Kalifornija, u policijskoj upravi Rialto provedeno je istraživanje utjecaja kamera.[31] Tijekom jedne godine policijska uprava rasporedila je prijenosne kamere u 988 smjena. Studija je pokazala impresivne rezultate. Između ostalog, smanjen je broj pritužbi na postupanje policijskih službenika sa 25 na 3 (odnosno 88%), a smanjen je i broj uporaba sredstava prisile policijskih službenika sa 61 na 25 (odnosno 60%). Rezultati istraživanja potvrđuju razloge korištenja prijenosnih kamera. U prvom redu to je zaštita policijskih službenika od zlonamjernih pritužbi na njihov rad. Zatim, afirmativan razlog je i osiguranje zakonitog, profesionalnog i transparentnog postupanja policijskih službenika. Kamere osiguravaju pristojnije ponašanje građana, ali i policijskih službenika. Snimke napravljene kamerama olakšat će provođenje postupaka protiv građana u incidentnim situacijama, ali i ispitivanja zakonitosti postupanja policijskih službenika. Osim za uporabe u formalnim postupcima, snimke kamera moći će se koristiti za edukacije policijskih službenika. Snimke predstavljaju najrealnije situacije s kojim se policijski službenici susreću na terenu. Analizom snimki moći će se policijskim službenicima pokazivati gdje se u postupanju griješi i na koji način se pogreške mogu ispraviti.

3. SUVREMENE TEHNOLOGIJE I METODE DJELOVANJA PROMETNE POLICIJE – TEHNIČKO-TEHNOLOŠKI ASPEKT

- **Fiksne kamere za nadzor brzine kretanja vozila.** Analizom prometnih nesreća u periodu od 2001. do 2010. godine može se zaključiti da je njihov broj u blagom opadanju (blagi silazni trend), a najveći broj nesreća događa se zbog nepropisne i neprilagođene brzine.[32] Otprilike polovina prometnih nesreća s najtežim posljedicama (u kojima su smrtno stradali, teško ili lako tjelesno ozlijeđeni sudionici) tijekom cijelog perioda, izazvane su zbog nepropisne ili neprilagođene brzine.

Budući da je nadzor brzine vozila jedna od temeljnih zadaća prometne policije, Ministarstvo unutarnjih poslova nabavilo je određene količine novih uređaja (kamera) za nadzor i mjerenje brzine. Uređaji se koriste kako bi se represivnim, ali i preventivnim djelovanjem policije osigurala sigurnost cestovnog prometa te kako bi se vozače potaknulo na poštovanje dopuštenog ograničenja brzine kretanja. Nabavkom i stavljanjem u funkciju novih tehničkih

[31]Farrar T. (2013.) The Rialto Police Department's Body-Worn Video Camera Experiment, Operation "Candid Camera", Portal University of Maryland, Department of Criminology and Criminal Justice, preuzeto 11. 2. 2016. godine s web adrese: http://ccjs.umd.edu/sites/ccjs.umd.edu/files/Wearable_Cameras_Capitol_Hill_Final_Presentation_Jerry_Lee_Symposium_2013.pdf

[32] nacionalni program za sigurnost cestovnog prometa, 6.1.1. brzina kretanja, nn 101/98., 15/00., 117/01., 199/03., 30/04., 77/09. i 145/10. zagreb: narodne novine.

uređaja izvršena je zamjena amortiziranih ili dotrajalih uređaja te su pod veći nadzor stavljena ključna mjesta i dionice državnih, županijskih i lokalnih cesta – koja su temeljem raščlambe utvrđena kao potencijalno opasna i rizična. Uređaji su postavljeni na području Policijske uprave osječko-baranjske, Primorsko-goranske i Zagrebačke na deset lokacija u svakoj upravi. Na svakoj lokaciji nalaze se ormari za smještaj radarskih uređaja, a pet uređaja prebacuje se s lokacije na lokaciju, ovisno o procjeni policijskih uprava o potencijalno opasnim lokacijama glede nepoštivanja brzine kretanja vozila.[33]

Fiksni uređaj za nadzor brzine tvrtke Gatsomer RS-GS11[34] sastoji se od kućišta koji je montirano na stupu uz cestu, na visini od nekoliko metara te radarskog uređaja smještenog u kućište. Sastavni dio uređaja je digitalna kamera od 11 milijuna piksela koja snima danju, ali i noću pomoću posebnog blica koji je vozačima nevidljiv i ne ugrožava njihovu sigurnost. Uređaj 24 sata na dan mjeri brzine od 30 do 250 kilometara na sat na temperaturama od -25 do +60 °C. Može snimati vozila u prekršaju u dolasku i odlasku te istodobno pokrivati do četiri prometne trake. Proizvođač garantira sigurnost uređaja u kućištu koje je čak otporno i na pogotke zrna vatrenog oružja.

Osim kamere, uređaji imaju ugrađene i uređaje za automatsko očitanje registarskih oznaka. Oni očitavaju registarske oznake na vozilima i upisuju ih u snimljenu fotografiju. Prednost kamera je što uz njih ne treba biti policijski službenik da ih osigurava i poslužuje. Za pristup snimljenim fotografijama dovoljno je posjedovati računalo s mrežnim pristupom. Iz ureda se policijski službenik spoji na kameru koja ima mogućnost bežičnog prijenosa podataka i sve snimljene fotografije spremi (prenese) na računalo. Fotografije su odlične rezolucije te se iz njih nesporno može utvrditi vozilo i registarska oznaka bilo da je fotografija napravljena po danu ili noći (slika 2). Na snimljenoj fotografiji nalaze se svi podaci važni za procesuiranje prekršaja i ona se koristi kao dokaz u prekršajnom postupku.[35] S obzirom na tehničke mogućnosti koje uređaj ima, u tijeku je izrada dodatnih (softverskih) alata koji će još više olakšati rad i pojednostaviti postupanje policijskim službenicima. Predviđeno je da se kamere povežu s informacijskim sustavom MUP-a te da se podaci o vlasnicima snimljenih vozila automatski koriste za ispis pismena ovisno o težini utvrđenog prekršaja. Na taj način skratit će se uvelike vrijeme potrebno za procesuiranje prekršaja, a i rasteretit će se referade prekršajnih postupaka u policijskim postajama.

[33]predstavljeni fiksni uređaji za mjerenje brzine, vijesti dana 22. srpnja 2015., internet portal ministarstva unutarnjih poslova rh, pruzeto 11. 2. 2016. godine s web adrese: http://www.mup.hr/main.aspx?id=215628

[34] gatso, karakteristike uređaja rsgs11, web stranica gatso, preuzeto 12. 2. 2016. s web adrese: http://www.gatso.com/uploads/downloads/gatso_specsheet_rs-gs11_en_sec.pdf

[35] zspc, čl. 283. nn 67/08., 48/10., 80/13., 158/13., 92/14., 64/15.

Slika 2: Fotografija vozila snimljena fiksnim uređajem za nadzor brzine (lokacija: Zagreb, Slavonska avenija)

Vozila snimljena u prekršaju prekoračenja brzine ne zaustavljaju se i procesuiraju odmah na mjestu već se to radi naknadno na temelju fotografija. Određeni problem predstavljala su vozila stranih registarskih oznaka za koja nije bilo moguće utvrditi vlasnika i procesuirati prekršaj. No taj problem riješen je pristupanjem Republike Hrvatske u Europski informacijski sustav o vozilima i vozačkim dozvolama (Eucaris).[36] To je sustav koji državama članicama omogućava razmjenu njihovih podataka o vozilima i vozačkim dozvolama i/ili drugim podacima vezanim za promet temeljem više pravnih okvira. Pomoću Eucarisa moguće je utvrditi vlasnike vozila iz većine europskih zemalja. Tako se sada obavijesti o počinjenim prekršajima prekoračenja brzine šalju u inozemstvo te se pokreću prekršajni postupci protiv stranih državljana.

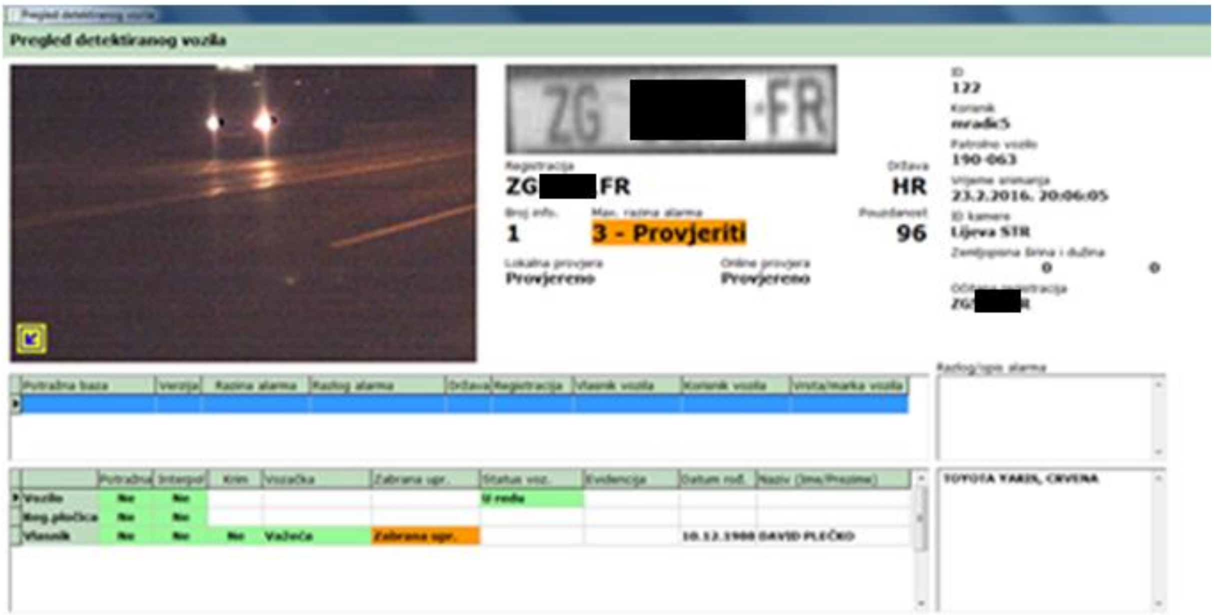
• **Uređaji za automatsko očitavanje registarskih pločica.** ANPR ili *Automatic Number Plate Recognition* je uređaj opremljen kamerama i računalnim softverom koji prepoznaje registarske pločice na vozilima i provjerava ih u bazama datoteka, odnosno u informacijskom sustavu MUP-a. Radi se o prijenosnom uređaju koji se instalira na policijsko vozilo i policijski službenici ga koriste za vrijeme službe. Posjeduje dvije kamere koje se montiraju na vanjske dijelove službenog vozila, prednju i stražnju stranu (slika 3). Uređaj se može koristiti u mirovanju ili u pokretu. Funkcionira tako da uhvaćenu sliku registarske oznake transformira u alfanumeričke znakove koristeći softver, uspoređuje registarsku oznaku s bazom podataka informacijskog sustava MUP-a i automatski alarmira policijskog službenika kada je vozilo

[36]Prijedlozi odluka o pristupanju Republike Hrvatske Eucaris-u sa 226. sjednice Vlade RH, Internet portal Vlade Republike Hrvatske, preuzeto 12. 2. 2016. s web adrese: https://vlada.gov.hr/sjednice/226-sjednica-vlade-republike-hrvatske-16877/16877

interesantno za nadzor.[37] Sustav očitava do deset registarskih pločica u sekundi te ih provjerava u informacijskom sustavu. Nakon što očita registarsku oznaku automatski u informacijskom sustavu izvrši provjeru. Provjerava je li vozilu važeća prometna dozvola, posjeduje li vlasnik vozila vozačku dozvolu te je li vlasniku možda izrečena zaštitna mjera zabrane upravljanja vozilom. Osim za vlasnika obavlja provjere i za ostale korisnike koji su bilo kada evidentirani u vozilu, kao putnici ili vozači. Provjerava imaju li kaznenih djela ili je za njima raspisana potraga. Također provjerava potražuje li se vozilo. Nakon što utvrdi neku od navedenih karakteristika uključuje se signal koji policijske službenike upozorava na nepravilnosti (slika 4). Policijski službenici zaustavljaju vozilo i obavljaju dodatne provjere te poduzimaju propisane radnje ovisno o utvrđenom. Uređaj tijekom osmosatne smjene može izvršiti nekoliko tisuća provjera vozila. Vrhunsko je sredstvo za pronalazak onih sudionika u prometu koji koriste gradske gužve i svakodnevno sudjeluju u prometu iako su im istekle valjanosti prometnih dozvola na vozilima, oduzete vozačke dozvole ili su im izrečene zaštitne mjere zabrane upravljanja.

Slika 3: Kamere uređaja ANPR
(postavljaju se na prednju i stražnju stranu službenog vozila)

[37] david j. roberts and meghann casanova, (2012), automated license plate recognition systems: policy and operational guidance for law enforcement, portal national criminal justice reference service. preuzeto 12. 2. 2016. s web adrese: https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf



Slika 4: Zaslon ANPR uređaja

(očitana je registarska oznaka vozila čiji vlasnik ima na snazi evidentiranu zabranu upravljanja motornim vozilom te kojeg je potrebno zaustaviti i izvršiti dodatne provjere)

S obzirom na mogućnosti i brzinu rada uređaja te kvalitetu i kvantitetu njegovih rezultata očekuje se da će ovakvi uređaji postati sastavni dijelovi svih policijskih vozila. Uređaji će osigurati veću uspješnost u radu policijskih službenika prometne policije u ostvarenju povoljnog stanja sigurnosti cestovnog prometa i smanjenju troškova postupanja.

4. SUVREMENE TEHNOLOGIJE I METODE DJELOVANJA PROMETNE POLICIJE – METODOLOŠKO-RAČUNALNI ASPEKT

Temeljna je zadaća prometne policije da svojim preventivnim i represivnim postupanjem osigura što manji broj prometnih nesreća i njihovih štetnih posljedica. Kako su prometne nesreće neizbježni dio prometa na cestama, prometna policija je ovlaštena služba zadužena za utvrđivanje svih činjenica kada do njih dođe, na temelju kojih će se u kasnijim postupcima dokazati krivnja i odlučivati o odgovornostima sudionika. Da bi pred nadležnim tijelima osigurali procesuiranje krivaca za izazivanje prometnih nesreća (a što je još važnije, da se osigura kako netko nedužan ne bi bio procesuiran za nešto za što nije kriv) te da bi oštećeni sudionici mogli naplatiti nastale štete – očevidi se moraju raditi precizno i ispravno. Iz tog razloga policijski službenici prometne policije koriste razne suvremene metode i računalna sredstva prilikom obavljanja očevida prometnih nesreća.

- **Mjerenje na mjestu događaja geodetskom mjernom stanicom.** Mjerenje položaja tragova i vozila na mjestu događaja jedan su od najvažnijih procesa kod obavljanja očevida prometnih nesreća. Na temelju izmjerenih tragova sastavlja se i zapisnik o očevidu i odlučuje o odgovornosti sudionika za izazivanje prometne nesreće. Prometne nesreće događaju se na

prometnicama i do okončanja očevida u pravilu se zatvara promet u potpunosti ili se odvija otežano. Ako se nesreća dogodi na prometnici na kojoj je gustoća prometa slaba ili postoji alternativni pravac za obilazak – obavljanje očevida ne predstavlja problem. Problem nastaje kada se za promet zatvori važna državna cesta ili autocesta na kojima ne postoje alternativni pravci. Tada su policijski službenici pod velikim pritiskom da očevid završe što prije kako bi se uspostavilo normalno odvijanje prometa. Zbog te žurbe ponekad dolazi do propusta i nepravilnog utvrđivanja činjeničnog stanja. Kako bi što brže i preciznije odradili posao izmjere na mjestu događaja, policijski službenici koriste se geodetskom mjernom stanicom *Sokkia* (slika 5). To je uređaj kojim policijski službenici pomoću GPS-a vrlo precizno mjere mjesto događaja i sve tragove zatečene na njemu. Preciznom i točnom izmjerom mjesta događaja i tragova kasnije se izrađuju objektivni i točni situacijski planovi koji se prilažu zapisnicima o očevidu. Jednom izmjereno mjesto događaja pohranjuje se u bazu podataka i postaje dostupno za budućnost. Tako je većina raskrižja na području grada Zagreba i prometnica na kojima se događaju prometne nesreće izmjerena mjernom stanicom i podaci unijeti u baze podataka. Ako se na tom raskrižju ili dionici ceste dogodi prometna nesreća, policijski službenici ne moraju mjeriti cijelo mjesto događaja već samo tragove i vozila zatečena na mjestu događaja nakon čega se može uspostaviti normalno odvijanje prometa.

Slika 5: Geodetska mjerna stanica Sokkia
(koriste ju policijski službenici za mjerenje mjesta događaja prometnih nesreća)

• **Izrada situacijskih planova mjesta događaja računalnim programom.** Nakon što se završi očevid na mjestu događaja, policijski službenici u postajama izrađuju situacijske planove. Do nedavno su se oni izrađivali ručno pomoću crtaćeg pribora na milimetarskom papiru. To možda i nije problem u postajama u kojima se mjesečno dogodi nekoliko prometnih nesreća, ali u većim gradskim središtima u kojima se svakodnevno događa

nekoliko desetaka prometnih nesreća to je problem. Nakon što policijski službenik izradi situacijski plan on se prilaže zapisniku o očevidu i u kasnijem prekršajnom ili kaznenom postupku služi kao dokaz. Pritisnut nedostatkom vremena policijski službenik kod ručnog crtanja situacijskih planova radi propuste i planove ne radi dovoljno precizno. U aktualnom vremenu policijski službenici na obuci za obavljanje očevida prometnih nesreća obučavaju se za izradu situacijskih planova pomoću računala u posebnom računalnom programu *Easy street draw*. Pomoću programa situacijski planovi se izrađuju u točnim mjerilima i u skladu s utvrđenim stanjem na mjestu događaja. Podaci iz mjerne stanice kojom je mjesto događaja mjereno ili iz ručnih skica policijskih službenika unose se u program i na temelju njih se izrađuje situacijski plan. Konačnom obradom dobiva se precizan, pregledan i uredan situacijski plan koji je realna preslika onoga što je zatečeno na mjestu događaja (slika 6). Policijskim službenicima koji ga izrađuju uvelike je pojednostavljen i olakšan rad. Program u sebi sadrži razne gotove predloške koje policijski službenik samo treba doraditi i uvrstiti ih u situacijski plan. Nema opasnosti da će se nešto krivo nacrtati zbog čega će se morati raditi novi plan kao kod ručnog crtanja. Posljedica rada ovim programom je brže, ali i preciznije rješavanje zaduženih spisa na temelju kojih se pokreću prekršajni i kazneni postupci te se nadoknađuje prouzročena šteta.

Slika 6: Situacijski plan mjesta događaja prometne nesreće – izrađen u programu Easy street draw

5. ZAKLJUČAK

Sijedom predmetnog istraživanja glede primjene suvremenih tehnoloških dostignuća u preventivno-represivnom postupanju prometne policije, proizlazi da se bez korištenja suvremenih tehnologija i metoda u području sankcioniranja prometne delikvencije i preventivnog rada policije ne može građanima pružiti niti odgovarajući stupanj sigurnosti. Porast inovativnih trendova u prometnoj infrastrukturi i sve brži tehnološki napredak vozila podrazumijevaju kontinuirano tehnološko praćenje i sve zahtjevniju ulogu policije kod takvih izazova. Sustavnim korištenjem suvremenih tehničkih dostignuća policija će svoje postupanje moći usmjeriti na najkritičnije sudionike i lokacije u prometu na cestama te na taj način osigurati da se poštuju zakonski propisi – što će za posljedicu imati smanjenje broja prekršitelja, ali i smanjenje broja stradalih sudionika u prometu.

Uvidom u statističke pokazatelje na područjima policijskih postaja koje u potpunosti primjenjuju projekte dostupnih tehnoloških inovacija u preventivno-represivnom postupanju, dolazi se do podataka o bitnom smanjenju pritužbi na rad policijskih službenika, ali i o smanjenju broja prekršaja i kaznenih djela. Iako hrvatska policija još uvijek nema u potpunosti normativnu uređenost korištenja navedenih suvremenih tehnoloških dostignuća kao neke zemlje EU, od velikog je značaja diferencirani i profesionalni pristup u korištenju policijske opreme, poglavito računalnih i videotehnologija koje su navedene u ovom radu. Hrvatska policija ne zaostaje za mnogim zemljama članicama EU čije redarstvene službe imaju puno veću tradiciju i veća proračunska sredstva.

Osobito je važno istaknuti da se spomenutim pitanjima u Hrvatskoj do sada nitko nije bavio na znanstveno-istraživačkoj razini. Imajući u vidu prostornu, demografsku, kulturološku i sociološku raznolikost Republike Hrvatske, hrvatsku policiju tek čeka da na temelju znanstveno-istraživačkih spoznaja i rezultata u korištenju navedene računalno-tehnološke infrastrukture, donese strateški plan razvoja i primjene suvremenih tehnologija koje zasigurno svakim danom sve više doprinose općoj sigurnosti i sudionika u prometu i svih građana. Samo optimalna i usklađena upotreba dostupnih tehnologija u policijskom postupanju jamčiti će građanima potrebitu sigurnost u svakodnevnom životu.

Korištenjem tehničke opreme koja je navedena u ovom radu, značajno se doprinosi unaprjeđivanju sigurnosnog sustava, ali i međusobnoj povezanosti i funkcionalnosti operativnog rada policije. Iako mnogi policajci govore o svojevrsnoj "tehnološkoj revoluciji" koja se u posljednjih nekoliko godina događa u hrvatskoj policiji, sigurno je da takve promjene valja gledati kao proces koji nije moguće vremenski ograničiti jer razvoj i tehnološki napredak podrazumijeva i promjenu razine svijesti i policijskog službenika i policije u cjelini. Potrebno je istaknuti kako se korištenjem suvremene tehničke infrastrukture nikada ne smiju ugroziti pravni standardi zaštite osobnih podataka i dostojanstvo čovjeka, već primjena tehničkih dostignuća mora biti primarno i isključivo u interesu općeg dobra.

Unatoč svim naporima policije da svojim preventivno-represivnim djelovanjem i sve većom primjenom tehničkih dostignuća građanima pruži maksimalnu sigurnost u prometu, nedvojbeno je vozač ključni čimbenik sustava cestovne sigurnosti, koji svojim psihofizičkim značajkama, znanjima, vještinama, osposobljenošću i ponašanjem utječe na sigurnost i

kakvoću odnosa u sustavu. Ako taj sustav sigurnosti u budućnosti ne bude davao željene rezultate, treba poduzeti radikalne promjene koje vode prema uspostavi novih odnosa u sustavu, a rizik dovodi na razinu društveno prihvatljivog, poglavito u broju smrtno stradalih osoba. Jer i jedna smrtno stradala osoba je previše. Rastom broja registriranih vozila koji sudjeluju u prometu raste i odgovornost prometne policije koja se tom izazovu treba suprotstaviti. Povećanje broja policijskih službenika nije adekvatan odgovor na taj izazov. Jedino rješenje koje se nameće u ovoj situaciji je upotreba što više suvremenih metoda i tehnika u radu prometnih policajaca.

LITERATURA

David J. Roberts and Meghann Casanova (2012). *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement.* Portal NATIONAL CRIMINAL JUSTICE REFERENCE SERVICE, https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf

Farrar, T. (2013). *The Rialto Police Department's Body-Worn Video Camera Experiment, Operation "Candid Camera".* Portal University of Maryland, Department of Criminology and Criminal Justice, http://ccjs.umd.edu/sites/ccjs.umd.edu/files/Wearable_Cameras_Capitol_Hill_Final_Presentation_Jerry_Lee_Symposium_2013.pdf

GATSO web stranica, Karakteristike uređaja Gatso RS-GS11, http://www.gatso.com/uploads/downloads/GATSO_Specsheet_RS-GS11_EN_sec.pdf

Nacionalni program za sigurnost cestovnog prometa. NN 101/98., 15/00., 117/01., 199/03., 30/04., 77/09. i 145/10. Zagreb: Narodne novine.

Portal Ministarstva unutarnjih poslova RH – Predstavljeni fiksni uređaji za mjerenje brzine, Vijesti dana 22. srpnja 2015., http://www.mup.hr/main.aspx?id=215628

Portal Vlade Republike Hrvatske – Prijedlozi odluka o pristupanju Republike Hrvatske Eucaris-u sa 226. sjednice Vlade RH. https://vlada.gov.hr/sjednice/226-sjednica-vlade-republike-hrvatske-16877/16877

Uputa Ravnateljstva policije, MUP-a RH za korištenje Sustava za upravljanje policijskim kamerama eKiosk, broj 511-01-50-72786/17-2015. od 10.02.2016. godine.

Zakon o policijskim poslovima i ovlastima. NN 76/09., 92/14. Zagreb: Narodne novine.

Zakon o sigurnosti prometa na cestama. NN 67/08., 48/10., 80/13., 158/13., 92/14., 64/15. Zagreb: Narodne novine.

Josip Medved
Ante Orlović
Jure Tadić

ROAD SAFETY – USING MODERN TECHNOLOGIES AND METHODS IN PREVENTIVE AND REPRESSIVE MEASURES TAKEN BY TRAFFIC POLICE

Summary

The police represent an important factor of implementation and development of road traffic safety. The role of the police in this context is essentially governed by the Act on Police Duties and Powers and the Road Traffic Safety Act. The conduct of police officers in the road traffic control and management implies the application of modern technologies and methods, which significantly contributes to the professionalization, standardization and efficiency in the functioning of the traffic police. Police officers and vehicles are equipped with numerous technical devices that significantly simplify and improve police's field activity in preventive and repressive sense. Regarding this, we single out the following: laptops (tablets), which allow for better communication, access to information and administrative work; mobile cameras used in company vehicles or on uniforms during police conduct; mobile devices for automatic number plate recognition mounted on company cars. In addition to mobile devices, fixed devices (cameras) that are placed along the roads for the purposes of speed control and automatic number plate reading (ANPR) which play an important role in road safety. Traffic accidents are unavoidable in road traffic and the recovery thereof (legal, financial) is of great relevance. The recovery is based on the investigation conducted by police officers using modern technologies and methods (measuring the scene by geodesic tools, making situational plans using computer programmes) for the purpose of accuracy, objectivity and effectiveness of their performance. The presentation of the application of modern technologies and methods in preventive and repressive measures of the traffic police has been observed in three aspects: personal and procedural, technical and technological and methodological and computer-based. Application of modern technology and methods on the one hand, increases the operational efficiency of traffic police officers in the field and stations; and on the other hand it provides faster, easier and more accurate location and prosecution of the road users who violate traffic rules and endanger traffic safety.

Key words: *road safety, operation of the traffic police, modern technology and methods.*

PREGLEDNI ZNANSTVENI RAD

Davor Labaš[38]
Krešimir Filipić[39]

KRIMINALISTIČKA ISTRAŽIVANJA PROVALNIH KRAĐA U DOM - MOGUĆNOSTI PROCESNOG PRISTUPA UPRAVLJANJA RIZIKOM

Sažetak

Upravljanje rizikom jedan je od alata kojim se organizacije koriste za uspješno upravljanje procesima kojima žele ostvariti svoje ciljeve. Strateška opredijeljenost Ministarstva unutarnjih poslova je primjena upravljanja rizicima na svim razinama organizacije. Policijska profesija pod stalnim je utjecajem neizvjesnosti prilikom poduzimanja svojih radnji. Upravljanje rizikom omogućava kvalitetan pogled unaprijed u razvoju pojedinog procesa. Također, pomaže kod donošenja odluka o potrebi poduzimanja mjera i radnji radi eliminacije rizika. U radu su na osnovu analize slučajeva i dosadašnjeg iskustva iz prakse opisane i objašnjene glavne aktivnosti u procesu kriminalističkog istraživanja provala u dom. Kroz prikaz i primjenu neobvezujuće norme za upravljanje rizikom ISO 31000 identificirani su najčešći glavni rizici u procesu i mjere i radnje kojima policijski službenici nastoje kontrolirati ove rizike. Počinitelji provalnih krađa u domove uzimaju u obzir uloženi napor, izloženost riziku i vrijednost koju otuđuju. Oni također nastoje umanjiti svoje rizike i na svoj način njima upravljati. Usmjerenost rada policije na identifikaciju rizika kojima je počinitelj bio izložen prilikom izvršenja kaznenog djela i analizu je li i kako je iste kontrolirao, mogu biti jedan od pristupa policije u cilju otkrivanja počinitelja. Cilj rada je ukazati na mogućnosti i potrebu uvođenja alata upravljanja rizikom kao jedan od pristupa u upravljanju operativnim policijskim procesima.

Ključne riječi: *provale u dom, kriminalističko istraživanje, upravljanje rizikom, operativni policijski procesi.*

1. UVOD

Moderni načini upravljanja i ekonomičnost rada svih vrsta organizacija imperativ su za uspješno djelovanje na bilo kojem području rada. Različite teorije na području organizacijske znanosti stvarale su načela koja se primjenjuju u praksi svih vrsta organizacija. Jedno od temeljnih obilježja organizacijskih teorija jest da pojava nove teorije i njezina primjena u praksi ne znači nestanak dobrih elemenata starijih teorija.

Prema Tayloru, utemeljitelju znanstvene organizacije i predstavniku klasične teorije organizacije, radniku treba pokazati „najbolji put“ za obavljanje svog zadatka i sve uvjete prilagoditi da on tim putem i prođe. Međutim, apstrahirajući od te klasno-teoretske pozadine, „taylorizam“ je jasno istaknuo važnost racionalizacije na načelu ekonomičnosti u samome radnom procesu. Takvo ekonomsko i tehničko promatranje, preneseno na upravu, stavlja težište na ekonomičnost postupanja upravnih organizacija, nastoji pronaći metode za

[38] Davor Labaš, predavač, struč. spec. crim, MUP, Policijska akademija,Visoka policijska škola, Zagreb, e-mail: dlabas@fkz.hr
[39] Krešimir Filipić, student, bacc. crim, MUP, Policijska akademija, Zagreb, e-mail: kfilipic@mup.hr

racionalizaciju toga postupanja i otkriti opće principe koji bi se mogli primijeniti s istim uspjehom na različite upravne organizacije. (Pusić, 2002, 49)
Stoga i policija kao dio državne uprave ima potrebu i mogućnost korištenja i onih alata u području upravljanja koji nisu korisni samo u svijetu profita već i u području nemerkantilnog djelovanja. Jedan od takvih alata je upravljanje rizikom. Upravljanje rizikom danas je strateško opredjeljenje u području djelovanja državne uprave u Republici Hrvatskoj.[40]
Upravljanje rizikom kao alat za uspješno trasiranje budućih aktivnosti može se primijeniti i na procesima koji se odvijaju ne samo na strateškoj i taktičkoj već i operativnoj razini policijske organizacije. Analizom slučajeva iz prakse i dosadašnjih iskustava u procesu kriminalističkog istraživanja provala u domove razmotriti ćemo koji se glavni rizici pojavljuju u takvim procesima. Nastojat ćemo grupirati identificirane rizike i usporediti sa važećom tipologijom rizika u javnom sektoru. Također, identificirat ćemo glavne rizike počinitelja prilikom počinjenja kaznenih djela provala u dom i analizirati može li usmjerenost policije odnosno promišljanje i postupanje istražitelja na provjeru kako je počinitelj kontrolirao svoje rizike, biti jedan od učinkovitih pristupa u cilju otkrivanja počinitelja. Analizom rada policije metodika istraživanja imovinskih delikata dolazi do saznanja o tipičnim operativno-taktičkim i istražnim radnjama i mjerama koje policija primjenjuje u otkrivanju i razjašnjavanju pojedinih oblika imovinskog kriminaliteta. Međutim, moramo naglasiti da metodika istraživanja imovinskih krivičnih djela ne daje "recept" za otkrivanje i razjašnjavanje imovinskih krivičnih djela niti "najbolju" metodu. Bit primjene pravila metodike istraživanja imovinskih delikata jest uzimanje u obzir individualnosti svakog pojedinog krivičnog djela. Zbog toga praktična primjena operativno taktičkih i istražnih mjera i radnji zahtijeva kreativan pristup. (Dujmović, 1992, 239)

2. PROCESNI PRISTUP UPRAVLJANJU RIZIKOM

2.1. Proces upravljanja rizikom prema normi 31000

Upravljanje rizikom zahtijeva da prije svega jasno definiramo čime mi to želimo upravljati. Više autora i izvora nastoje definirati rizik. Rizik je moguće dešavanje nepoželjnog događaja. Događaj je nešto što se može desiti, definirana pojavnost (Broder, 2003, 102, 231). Rizik je mogućnost nastanka događaja koji mogu nepovoljno utjecati na ostvarenje ciljeva.[41] Rizici koji utječu na ostvarenje ciljeva u pojedinoj organizaciji mogu dolaziti izvana i iznutra.

Vanjski rizici su sljedeći:
- prirodne i druge katastrofe
- teroristički napadi
- kriminalni događaji

[40] Ministarstvo financija (rujan 2009., Zagreb), Smjernice za provedbu procesa upravljanja rizicima kod korisnika proračuna, (http://www.mfin.hr-08.02.2016.).
[41] Zakon o sustavu unutarnjih kontrola u javnom sektoru, (NN 78/15.), članak 4.

- promjena geopolitičkog položaja
- makroekonomske promjene, npr. uvođenje eura.

Na ove rizike organizacija ne može potpuno samostalno utjecati i spriječiti ih u njihovu nastajanju već samo ublažiti njihov utjecaj na ostvarenje ciljeva. Unutarnji rizici vezani su uz provođenje naših aktivnosti i ukoliko ih pravovremeno utvrdimo, u značajnoj mjeri ili u potpunosti možemo eliminirati njihovo djelovanje. Prema tipologiji Ministarstva financija rizici koji se pojavljuju u unutarnjem području mogu se sistematizirati u pet glavnih područja:

- Planiranje, procesi i sustavi (strategije, planiranje, operativni procesi, financijski i drugi logistički procesi, IT sustavi)
- Zaposlenici i organizacija rada (sigurnost zaposlenika, objekata i opreme, podjela poslova i odgovornosti, obučenost i kompetentnost zaposlenika, formalne i neformalne organizacijske strukture i sl.)
- Zakonitost i ispravnost (primjena jasnih, prikladnih i usklađenih propisa, druga potencijalna pitanja vezana uz zakonitost i pravilnost)
- Komunikacije i informacije (metode i kanali komunikacije, kvaliteta i pravodobnost informacija[42].

Ovu tipologiju rizika potrebno je prilagoditi specifičnostima svake organizacije. Na osnovi analize slučajeva iz prakse i iskustva nastojat ćemo identificirane rizike u policijskom procesu grupirati u odnosu na ovu tipologiju u javnom sektoru. Ostvarenje zadataka ili ciljeva u različitim aktivnostima u procesima izloženo je rizicima. Upravo zato jasno prepoznavanje procesa ili njihovih dijelova kao skupa međusobno povezanih aktivnosti je preduvjet da možemo uspješno identificirati rizike i njima upravljati. Proces se pojavljuje kao okvir koji je prožet različitim aktivnostima. Sve te aktivnosti povezuje zajednički cilj. Cilj je očekivano ishodište procesa. Ugrožavaju ga različite prijetnje koje iskorištavaju slabosti dijelova sustava koji sudjeluju u procesu i rezultiraju štetnim događajima. Vjerojatnost nastupanja štetnih događaja i njihov učinak želimo svesti na prihvatljivu razinu provođenjem različitih mjera i radnji. Tim mjerama i radnjama kontroliramo odvijanje našeg procesa u smjeru ostvarenja ciljeva i zbog toga ih nazivamo kontrolama. *Kontrola*[43] je svaka mjera ili aktivnost koja se poduzima u svrhu upravljanja rizicima i povećanja vjerojatnosti da će se poslovni ciljevi ostvariti. Rukovoditelji planiraju, organiziraju i usmjeravaju obavljanje aktivnosti u svrhu ostvarenja poslovnih ciljeva. Rezultati našeg upravljanja rizicima trebali bi se odraziti na bolju percepciju javnosti, bolju učinkovitost i povećanu sigurnost. Sigurnost je primjena niza prihvatljivih praksi, postupaka i načela koji, kad se uzmu kao cjelina, imaju učinak kojim mijenjaju omjer nepoželjnih događaja u ukupnim događajima. Cilj sigurnosnog nacrta jest smanjiti udio nepoželjnih događaja u svim događajima (Broder, 2003, 232). Rizici u postupanju policijskih službenika su njihova svakodnevica. Međutim, oni nisu vezani samo za nastupanje opasnosti koja može ugroziti njihove živote i živote građana, već i za druge procesne rizike koji se javljaju u policijskim aktivnostima i koji mogu omesti uspješno ostvarenje cilja.

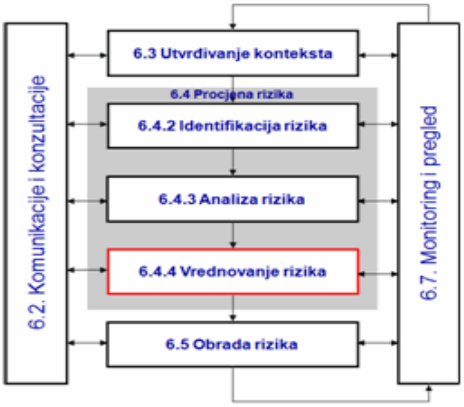
---

[42] Ministarstvo financija , rujan 2009, Zagreb. Smjernice za provedbu procesa upravljanja rizicima kod korisnika proračuna, (http://www.mfin.hr-08.02.2016.).

[43] Zakon o sustavu unutarnjih kontrola u javnom sektoru, NN 78/15, članak 1.

Izgrađivanje pristupa u kojem želimo upravljati našim procesima na dinamičan način i korištenje alata s kojim nastojimo spriječiti, izbjeći ili umanjiti posljedice neželjenih događaja nameće se kao stalni izazov u policijskom radu.
Planirani odgovor na rizike mora nam pružiti zadovoljavajuću razinu povjerenja u naša profesionalna očekivanja da neželjene događaje preveniramo ili eliminiramo njihov utjecaj na prihvatljivu razinu. On nije ograničen isključivo izradom sigurnosnih prosudbi nego se može nadograditi i unaprijediti korištenjem novih alata.
Kao mogućnost za unapređenje rada u području upravljanja policijskim procesima razmotrit ćemo primjenu generičkog univerzalnog pristupa procesu upravljanja rizikom kroz normu ISO 31000. Standard ISO 3100 opisuje generički proces za upravljanje rizicima i pogodan je za sve vrste rizika u svim područjima, što znači i za upravljanje operativnim rizicima[44]. Proces za upravljanje rizicima je definiran normom ISO 31000:2009 i spada u grupu smjernica, odnosno neobveznih normi za primjenu. (Nađ, Relić, 2012).
Detaljni opis procesa:

Slika 1: Komunikacija i konzultacija: Komunikacija i konzultacija kroz proces mora se odvijati kroz svaku fazu upravljanja rizikom i procesom kao cjelinom
Izvor: Adelsberger (2015). Stručni prilozi: ISO 31000 i generički pristup upravljanja rizicima. http://www.kvalis.com (21. 12. 2015.)

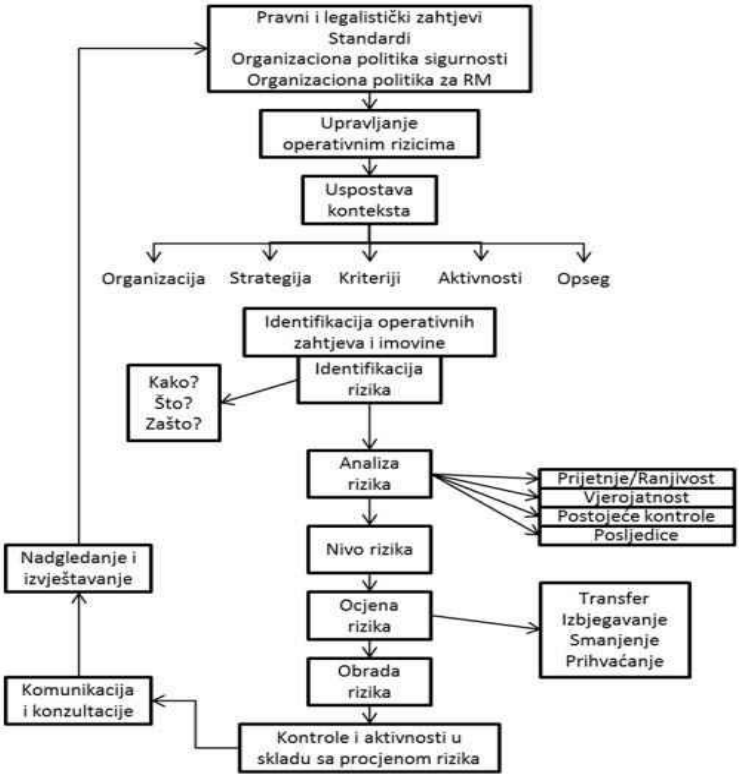


Utvrđivanje konteksta: Utvrđivanje eksternog, internog i konteksta upravljanja rizikom u kojem će se odvijati ostatak procesa. Treba utvrditi kriterije prema kojima će se procjenjivati rizik i definirati struktura analize.
Identifikacija rizika: Identifikacija gdje, kada, zašto i kako bi događaji mogli spriječiti, umanjiti, odložiti ili povećati postizanje ciljeva.
Analiza rizika: Identifikacija i procjena postojećih kontrola. Određivanje posljedica i vjerojatnosti i zatim razine rizika. Ova analiza treba razmotriti područje potencijalnih posljedica i kako bi se one mogle pojaviti.

[44] Alarm, airmic, IRM (2010). A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31 000 https://www.theirm.org/media/886062/ISO3100_doc.pdf (08.02.2016,15,04)

Procjena rizika: Usporedba procijenjenih razina rizika s prethodno utvrđenim kriterijima i razmatranje ravnoteže između potencijalnih koristi i nepovoljnih rezultata. To omogućuje donošenje odluka o opsegu i prirodi potrebnih obrada i o prioritetima.
Obrada rizika: Izrada i primjena specifičnih troškovno učinkovitih strategija i akcijskih planova za povećanje potencijalnih koristi i smanjenje potencijalnih troškova. Praćenje i preispitivanje: neophodno je pratiti učinkovitost svih koraka procesa upravljanja rizikom. To je važno za neprekidno poboljšavanje (Adelsberger, 2015).
Modificirana blok - shema procesa za upravljanje rizicima prema ISO 31000:

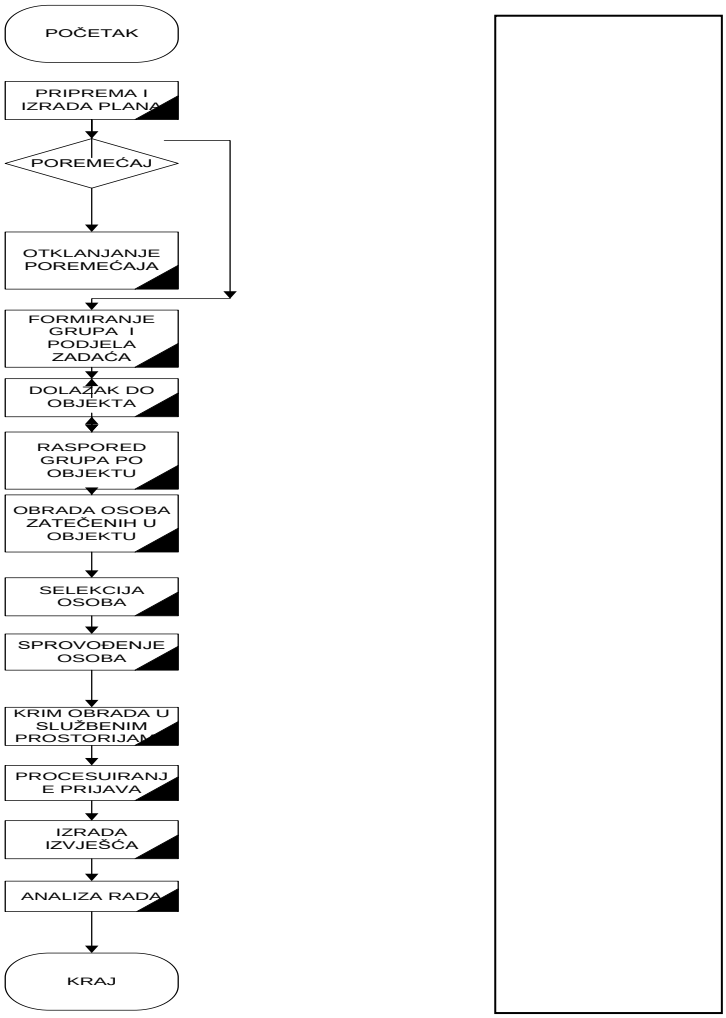
Slika 2: Blok - Shema procesa sa upravljanje rizicima (na temelju ISO 31000:2009)
Izvor: Adelsberger (2015). Operativni rizici kao temelj sustava upravljanja, http://www.kvalis.com (21.12.2015.)



Iz priložene blok - sheme na slici 2 može se vidjeti da je proces upravljanja rizicima relativno složen i da ima niz podprocesa koji se u pojedinim slučajevima područja primjene mogu drugačije realizirati. Npr. identifikacija operativnih zahtjeva i imovine, kao i identifikacija rizika može se razlikovati za područje informacijske sigurnosti (ISMS), procesne rizike, upravljanje zaštitom životne sredine (EMS), operativnih rizika, itd. Međutim, proces je u potpunosti jednak u svakom slučaju i jedinstven za sve vidove rizika u organizaciji.

2.2. Policijski procesi kao okvir procesa upravljanja rizikom

Primjena ove norme u području rada policijske organizacije na operativnoj razini otvara nove mogućnosti kvalitetnog upravljanja procesnim rizicima. Početak primjene procesa upravljanja rizikom nameće potrebu da naše aktivnosti koje se odvijaju u određenom vremenskom slijedu razmotrimo kao operativni proces koji ima svoj početak i kraj. Prikaz tehnologije procesa na primjeru racije jasno prikazuje slijed aktivnosti ili operacija koje se provode i moguće poremećaje



Slika 3: Racija-tehnologija procesa

Izvor: Jurak, F. (1993). Organizacija i funkcioniranje policije, slika 6, str. 20

Svaki proces ima svoj početak i kraj te sljedeće elemente: operacije ili aktivnosti, otklanjanje poremećaja, izrada izvješća, analiza rada, prihvaćanje izvješća. Kada nastane poremećaj nastaje nova situacija koja zahtijeva otklanjanje poremećaja. Ako imamo unaprijed razrađenu tehnologiju otklanjanja poremećaja onda to više nije poremećaj već je to podproces otklanjanja poremećaja (Jurak, 1993, 23). S obzirom na to da je proces upravljanja rizikom po svojoj prirodi usmjeren na otklanjanje mogućih poremećaja, isti se također javlja kao upravljački podproces u kojem je obuhvaćena identifikacija, analiza, procjena, te obrada rizika kao odgovor na moguće poremećaje u procesu. Primjenu upravljanja rizikom razmotrit ćemo na glavnim aktivnostima u dijelu procesa kriminalističkog istraživanja.

3. UPRAVLJANJE RIZICIMA U KRIMINALISTIČKOM ISTRAŽIVANJU PROVALA U DOMOVE

3.1. Upravljanje rizikom u aktivnostima kriminalističkog istraživanja

Kriminalističko istraživanje je ukupnost onih policijskih ovlasti, mjera i radnji koje se prema ovom ili drugim zakonima poduzimaju kada postoji osnova sumnje da se priprema ili je počinjeno kazneno djelo za koje se progoni po službenoj dužnosti ili prekršaj ili postoji sumnja da određena pojava ugrožava ili bi mogla ugroziti živote ljudi, njihova prava, slobodu, sigurnost, nepovredivost ili imovinu te radi otkrivanja kaznenog djela za koje se progoni po službenoj dužnosti ili prekršaja, pronalaženja počinitelja, sprječavanja da se počinitelj sakrije ili pobjegne, da se otkriju ili osiguraju tragovi i predmeti koji mogu poslužiti pri utvrđivanju činjenica i da se prikupe obavijesti koje mogu biti od koristi za uspješno vođenje kaznenog ili prekršajnog postupka.[45]

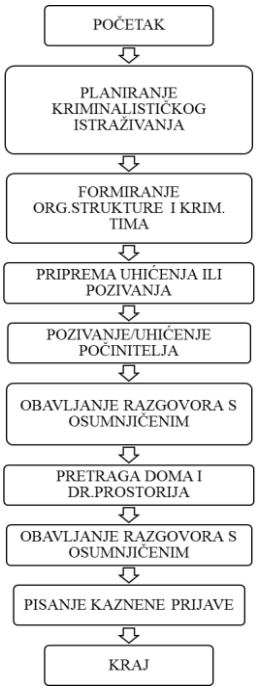
Analizom kriminalističkog istraživanja više slučajeva provalnih krađa na području policijske postaje koja djeluje u urbanoj sredini, prikupljanjem iskustava policijskih službenika u sklopu radionica upravljanja rizikom i vlastitim iskustvom nastojali smo utvrditi najčešće aktivnosti koje se provode u kriminalističkom istraživanju u jednoj ustrojstvenoj jedinici. Proces kriminalističkog istraživanja i glavne rizike razmotrili smo od poduzimanja početnih aktivnosti nakon osnova sumnje da je određena osoba počinitelj do završnih aktivnosti koje se odnose na podnošenje kaznene prijave protiv počinitelja.

Za potrebe ovoga rada ukratko ćemo opisati slučajeve provalnih krađa koji su bili predmet analize.

U prvom slučaju počinitelj je uporabom prikladnog predmeta obio i otvorio ulazna vrata stana, ušao u unutrašnjost, ispremetao stvari kojom prilikom je zatečen od strane vlasnika te zadržan do dolaska policije. U drugom slučaju počinitelj je zavlačenjem prikladnog predmeta između krila prozora i doprozornika kroz prozor ušao u unutrašnjost kuće i otuđio novac i zlatni nakit. Obavljenim očevidom pronađeni su u kući otisci papilarnih linija počinitelja koji je od ranije evidentiran za ovu vrstu kaznenih djela. U trećem slučaju počinitelj je preskočio balkonsku ogradu i prikladnim predmetom razbio staklo na balkonskim vratima i ušao u stan te započeo prekapati po stvarima. Isti je zamijećen zbog stvaranja buke od susjeda, te nakon

[45] Zakon o policijskim poslovima i ovlastima, NN, 76/09., 92/14., članak 2.

što je izašao iz kuće kroz balkonska vrata zatečen je prilikom udaljavanja od susjeda i zadržan do dolaska policije. Snimke video-nadzorne kamere zabilježile su cjelokupni događaj. U četvrtom slučaju počinitelj je zavlačenjem podesnog predmeta između krila prozora i doprozornika u prizemlju kuće ista obio i ušao u unutrašnjost kuće, otuđio predmete koje je ukrcao u kombi vozilo. Na putu su ga zaustavili policijski službenici i nakon provjera lišen je slobode. U petom slučaju počinitelj je svladavanjem visine preko krova garaža došao do balkona stana kojom prilikom je kroz otvorena balkonska vrata ušao u stan i otuđio predmete. Otuđeni predmet pronađen je naknadno kod druge osobe što je omogućilo utvrđivanje počinitelja. Ovakvi i slični slučajevi gotovo su svakodnevnica kojom se bave policijski službenici i kriminalistički istražitelji u nekoj od ustrojstvenih jedinica policije. Kriminalistička istraživanja povodom ovakvih kaznenih djela odvijaju se na najnižoj i srednjoj razini policijske organizacije. Za opisane slučajeve zajedničko je da je policija od trenutka postojanja osnova sumnje za određenu osobu da je počinitelj nekog od opisanih kaznenih djela, kroz završni dio procesa kriminalističkog istraživanja trebala prikupiti sve tragove, obavijesti i predmete koji mogu biti od koristi za uspješno vođenje kaznenog postupka. Time je određen jasan cilj ovog dijela procesa koji se sastoji od više aktivnosti prilagođenih okolnostima navedenih slučajeva.
Za potrebe ovog rada izdvojili smo glavne aktivnosti koje se najčešće odvijaju u navedenom dijelu procesa kriminalističkog istraživanja (slika 4):



Slika 4: Prikaz glavnih aktivnosti u dijelu procesa kriminalističkog istraživanja

Slika 5: Prikaz glavnih aktivnosti u „procesu" provale u dom

Bez obzira na to što možemo reći da je u dva slučaja od navedenih slučajeva počinitelj zatečen na počinjenju kaznenog djela, kao prvu aktivnosti na možemo zaobići planiranje kriminalističkog istraživanja. Najveća prijetnja dobrom planiranju je nedostatak ili netočnost raspoloživih podataka o sumnjivoj osobi, o predmetima kaznenog djela, gdje i na koji način bi se oni trebali pronaći. Kontrole koje su nezaobilazne su prikupljanje podataka kroz raspoložive *evidencije* unutar samog policijskog sustava i dodatne policijske provjere na terenu i prikupljanje obavijesti iz različitih izvora (građana, informatora i dr.). U fazi planiranja kriminalističkog istraživanja potrebno je predvidjeti koje će se sve aktivnosti provoditi od uhićenja ili pozivanja počinitelja do podnošenja kaznene prijave. Kriminalističko planiranje odnosi se na strukturu koja je obilježena 1) brojnošću relevantnih čimbenika, 2) međusobno uvjetovanim odnosima i vezama i 3) sljednim (uglavnom kauzalno povezanim) aktivnostima. (Pavišić, Modly, Veić, 2006, 176).

Sljedeća aktivnost je vezana uz *formiranje odgovarajuće organizacijske strukture* odnosno kriminalističkog tima koji će provesti potrebne zadaće. Rizici koji se najčešće javljaju u ovoj fazi su nejasne uloge i zadaće izvršitelja, nestručnost policijskih službenika kao posljedica neznanja i neiskustva na otkrivanju ove vrste kaznenih djela, nemotiviranost izvršitelja, nedostatak službenika zbog preopterećenosti drugim zadaćama i slično. Kontrole kojima ove rizike možemo smanjiti na prihvatljivu razinu su formiranje takve privremene organizacijske strukture u kojoj će kao prethodna kontrola postojati *jasna podjela poslova i odgovornosti*. Neophodno je uvesti timski rad s formiranjem voditelja tima i voditelja grupa sa stručnim znanjima i iskustvima u skladu s aktivnostima koje slijede u procesu. Svrsishodno može biti dodatno određivanje *jasnih podciljeva* (kontrolnih) pojedine grupe s jasnim zadaćama. Temeljna prednost timske organizacijske strukture jest u tome što se u ustrojstvu organizacije može postići relativno „plitka“ struktura, s minimalnim brojem razina (Jurina, 2008, 49). Kompleksnost organizacijske strukture ne bi trebala imati obilježje previše razina u rukovođenju, a komunikacijsko opterećenje mora pružiti mogućnost pravovremene izmjene informacija i pravovremenih odluka.

U tom cilju potrebno je iskoristiti i *planirane linije komunikacije i suradnje* sa *specijalističkim odjelima* te eventualno uključivanje potrebnog broja službenika specijalističkog odjela u tim. Na motiviranje službenika može pozitivno djelovati uvođenje *jasnih procedura i kriterija* predlaganje djelatnika za nagrade, omogućavanje korištenja slobodnih dana, napredovanja u hijerarhiji i slično. Također, uz formiranje organizacijske strukture koja će podržavati ovaj proces javljaju se rizici vezani uz nedostatak tehničkih i inih sredstava koji preventivnim kontrolama kao što su *periodička provjera ispravnosti* vozila i opreme, inventurni popisi – *evidencije, rashodovanje neispravnih i zastarjelih sredstava, planiranje pričuve* – moraju svesti ove rizike u organiziranju na prihvatljivu razinu. Za navedene aktivnosti možemo reći da pripadaju u pripremnu fazu ovog dijela procesa kriminalističkog istraživanja. U tim aktivnostima rukovoditelj ili drugi policijski službenik koji upravlja procesom trebao bi biti u stanju rizike koji su identificirani kao najčešći, analizirati tako da procijeni jesu li uvedene kontrole dostatne i da li iste eliminiraju identificirane rizike na prihvatljivu razinu. To može biti proces samostalnog promišljanja ali i transparentni proces suradnje sa sudionicima u kojem voditelj procesa i suradnici na osnovi prikupljenih saznanja i iskustava iz ranijih

postupanja analiziraju i procjenjuju rizike i kontrole koje su na raspolaganju, te nastoje pripremiti učinkoviti proces kriminalističkog istraživanja. Situacije ponekad ne zahtijevaju primjenu previše kontrola jer one mogu usporiti proces, već samo onih koje su potrebne u određenoj situaciji.

Nakon ove interne pripremne faze, pristupa se sljedećoj fazi procesa koja je više vezana uz rad na terenu i započinje aktivnostima pozivanja ili uhićenja počinitelja za kojeg raspolažemo osnovom sumnje da je počinitelj kaznenog djela. Glavni rizici su bijeg počinitelja, pružanje otpora i ugrožavanje života policijskih službenika i drugih građana, te eventualno uništenje traženih predmeta kaznenog djela. Postojeći policijski sustav ima već ugrađene „kontrole" kojima nastoji ove rizike svesti na prihvatljivu razinu. Zadaća je voditelja i sudionika procesa da identificiraju rizike u odnosu na konkretan događaj, *prepoznaju* i *analiziraju kontrole* kojima raspolažu i primijene one koje su svrsishodne. Uvid u postojeće *evidencije* o dosadašnjem ponašanju počinitelja i prikupljene obavijesti trebale bi pružiti dovoljno podataka o počinitelju. Ovdje je vrlo bitna procjena o vjerojatnosti i posljedicama pružanja otpora koja se može iskazati kroz izradu posebne sigurnosne prosudbe. U slučaju procjene postojanja realne opasnosti pružanja otpora ova zadaća pristupa objektu i lišavanja slobode može se dodijeliti policijskim službenicima koji su *specijalno obučeni i opremljeni* za oduzimanje slobode. Uvijek trebamo nastojati provesti planirano oduzimanje slobode (Grigolet, Štrk, Wulf, 2005, 194) u kojem ćemo nastojati oduzimanje slobode provesti na mjestu, u vrijeme i na način da rizik opasnosti za tijelo i život službenika i građane ali i samog mogućeg počinitelja, bude sveden na prihvatljivu razinu. U ovoj aktivnosti kao značajni oblik kontrole javljaju se i *slobodni i unaprijed dogovoreni komunikacijski kanali* radi eventualnog angažiranja dodatnih snaga odnosno *pričuve.* Pored organizacijskih rizika značajno mjesto u provedbi uhićenja može zauzeti uporaba sredstava prisile. Kako bi eliminirali rizik nezakonite uporabe sredstava prisile, policijski službenici moraju poštovati kontrole koje su ugrađene kroz *zakonske odredbe i pravila struke* o uvjetima i načinu provođenju ove radnje.

Nezaobilazna aktivnost koja se u analiziranom dijelu procesa obavlja jest obavljanje razgovora s mogućim počiniteljem. U odnosu na procjenu istražne situacije, potrebe za prikupljanjem korisnih izjava od osumnjičenika se ne mogu vezati isključivo uz neki određeni stadij prethodnog postupka već se mogu pojavljivati ovisno o okolnostima pojedinog slučaja. Ako je osumnjičenik otkriven ubrzo nakon počinjenja ili temeljem neke okolnosti koja čvrsto upućuje na povezanost, može biti opravdano prikupljanje njegovih izjava već na početku istraživanja. (Karas, 2015, 111). Informacijski deficit i netočnost podataka o pripremi provale u dom, samom počinjenju i aktivnostima počinitelja nakon počinjenja kaznenog djela može daljnje kriminalističko istraživanje pogrešno usmjeriti, tako da se ne pronađu tragovi i predmeti kaznenog djela, supočinitelji, prikrivači otuđenih predmeta i dr. Glavne prijetnje su nepripremljenost i nestručnost policijskih službenika koji obavljaju razgovor, ograničenost raspoloživog vremena trajanja razgovora, „zatvorenost" počinitelja za razgovor, ali i eventualni napad na službenika, bijeg ili samoozljeđivanje počinitelja. Kontrole kojima raspolažemo *su obučen i iskusan istražitelj, planirano vođenje i trajanje* razgovora, *mjere opreza – zona sigurnosti* prilikom obavljanja razgovora i *angažiranja dodatnih policijskih*

službenika za čuvanje osobe, vođenje razgovora u za *to pripremljenoj i opremljenoj prostoriji,* poštovanje svih *zakonskih odredbi* o obavljanju razgovora s dokaznom snagom.
U cilju ostvarenja cilja procesa i prikupljanja materijalnih dokaza koji mogu biti od koristi za uspješno vođenje kaznenog postupka, sljedeća aktivnost koja se najčešće provodi je pretraga doma i drugih prostorija. Pretraga doma ima kao i oduzimanje slobode jako kontrolno okruženje prožeto nizom zakonskih odredbi, jer se radi o zadiranju u temeljna ljudska prava koje policija može ostvariti jedino pod strogim zakonskim uvjetima. Njihovim poštovanjem eliminiraju se rizici koji su vezani uz nezakonito pribavljene materijalne dokaze. Međutim, da bi eliminirali rizik nedostatka materijalnih dokaza potrebno je eliminirati ugroze procesa kao što su nepoznata stvarna adresa na kojoj bi se mogli nalaziti otuđeni predmeti ili uništenje predmeta prije započinjanja pretrage. I ovom prilikom upućeni smo na *paralelne ili provjere* iz više izvora, korištenje postojećih *evidencija i evidencija o ranijim postupanjima policije* u cilju utvrđivanja potencijalnih lokacija gdje bi se predmeti mogli nalaziti*, prikriveno motrenje* prije započinjanja pretrage radi sprečavanja uništenja predmeta, *korištenje specijalne opreme* i utvrđivanje eventualnih prikrivača predmeta i njihovih adresa koje koriste za prikrivanje otuđenih predmeta. I ovdje je vrlo važna *komunikacija i jasno utvrđene linije izvješćivanja* o situaciji na terenu radi donošenja brzih i dobrih odluka.
Razjašnjavanje prikupljenih saznanja iz dotadašnjih provedenih kriminalističkih mjera i radnji zahtijeva ponovno obavljanje razgovora s osumnjičenom osobom ili mogućim svjedokom. Policijski službenik prije takvog razgovora mora raspolagati svim pojedinostima i podacima koji su prikupljeni tijekom dotadašnjeg kriminalističkog istraživanja. Kroz radni sastanak sa svim izvršiteljima kriminalističkog istraživanja mogu se razmijeniti i analizirati sva nova saznanja do kojih se došlo tijekom kriminalističkog istraživanja. Na taj način osigurat će se *prijenos (sa)znanja* i utvrdit će se potrebne *linije komunikacije* između istražitelja koje se javljaju kao dodatno uspostavljene kontrole.
Iste kontrole možemo koristiti pri pisanju kaznene prijave. Rezultat kriminalističkog istraživanja nastoji se objediniti u kaznenoj prijavi. Pred službenikom koji sastavlja kaznenu prijavu zahtjev je da mu je poznat cjelokupni tijek kriminalističkog istraživanja, svi podaci koji su prikupljeni, te sva pismena koja su nastala tijekom cjelokupnog procesa kriminalističkog istraživanja. Podnoseći prijavu, tijela državne vlasti i pravne osobe navest će dokaze koji su im poznati i poduzeti – sve da bi se sačuvali tragovi kaznenog djela, predmeti na kojima je ili kojima je počinjeno djelo te drugi dokazi.[46] Organiziranje pisanja kaznene prijave i ispunjavanje svih potrebnih elemenata kaznene prijave izloženi su rizicima prekoračenja zakonskog roka za eventualno privođenje počinitelja pritvorskom nadzorniku i unosu netočnih podataka. Točnost i potpunost podataka i svih elemenata kaznene prijave koja se prosljeđuje nadležnom državnom odvjetništvu obuhvaćena je i kontrolom *dvostruke autorizacije,* odnosno supotpisa policijskog službenika na kaznenoj prijavi, a koji sastavlja kaznenu prijavu te njegova rukovoditelja. Svaka kaznena prijava uvodi se posebnu *evidenciju*. Rizik prekoračenja zakonskog roka za podnošenje kaznene prijave i eventualno dovođenje pritvorskom nadzorniku svakako treba procijeniti s obzirom na ostatak vremena s kojim u

[46] Zakon o kaznenom postupku, NN, broj 152/08., 76/09., 80/11., 91/12. - Odluka i Rješenje USRH, 143/12., 56/13., 145/13. i 152/14., članak 204.

konkretnom slučaju raspolažemo. Kako bismo ga umanjili, potrebno je planirati prostor, vrijeme, tehnička sredstva i policijskog službenika koji će sastaviti kvalitetnu kaznenu prijavu.

Upravljanje rizikom u operativnim procesima zahtijeva brzu izmjenu identifikacije, analize, procjene i obrade rizika. Iskustvo u vođenju procesa nezamjenjiv je izvor za uspješno upravljanje rizikom. Tijekom kriminalističkog istraživanja često se ne može izbjeći ograničenje temeljnih ljudskih prava koje policija može provesti samo uz ispunjene zakonskih uvjeta. Kontrolno okruženje kao rezultat zakonskih i inih propisa je izuzetno snažno. Naime, svako razvijeno demokratsko društvo se opredijelilo da ovakvi procesi budu prožeti zakonskim pravilima i ona su jamstvo, odnosno kontrola da će se proces odvijati na prihvatljiv način. Međutim, pri analizi očekivanih kontrola i načina njihovog funkcioniranja, treba uzeti u obzir i mjere i radnje koje su rezultat organizacijskih pravila i pravila struke. Potrebno je analizirati *kontrole* kao što su npr. raspodjela ovlasti i odgovornosti, odnosno jasna dodjela uloga svakom izvršitelju, stručno ekipiranje, jasne linije izvješćivanja, procedure, fizičke zapreke, načela stručnog postupanja, evidencije, obrasci, ček-liste, propisana osnovna i specijalna oprema, razvrstavanje i dupliciranje sredstava odnosno pričuva, prijenos znanja, periodične provjere, posebna stručna znanja i specijalizacije, obuka i stjecanje posebnih vještina, autorizacija, lozinke, sigurnosne zone, usmjeravanje kretanja ili druge taktičke mjere opreza i ostale interne kontrole koje policijski sustav može koristiti.

Ukoliko želimo grupirati prijetnje i rizike kojima je proces bio izložen, razvidno je da se oni javljaju u području planiranja, organiziranja sredstava i upravljanja ljudskim potencijalima, zatim rizici koji su vezani uz izlaganje opasnosti službenika, rizici koji su povezani sa zahtjevom za poštovanje zakonskih odredbi, te rizici vezani uz unutarnju i vanjsku komunikaciju i dostupnost podataka. Uspoređujući ovakvo grupiranje rizika u promatranom procesu s prihvaćenom tipologijom rizika u javnom sektoru razvidno je da se podudaraju. Osiguranje ostvarenja cilja aktivnosti, operacije ili cjelokupnog procesa trebao bi biti rezultat logične povezanosti internih kontrola na osnovi dostignuća najbolje prakse. Ovaj zahtjev ne može se ostvariti bez faze monitoringa i pregleda koja posebno dolazi do izražaja na kraju procesa kojim nastojimo upravljati. Naime, svaki voditelj procesa trebao bi odvojiti vrijeme za analizu provedenog. Pregled i analiza procesa treba odgovoriti na pitanja jesu li rizici bili pravovremeno identificirani, procijenjeni i jesu li odluke u svezi obrade rizika bile odgovarajuće. Takav pristup može dovesti do poboljšanja u upravljanju budućim procesima. Zbog toga treba osigurati organizacijsku klimu u kojoj će se moći slobodno analizirati učinjeno, bez straha od neopravdane kritike i sankcioniranja.

3.2. Usmjerenost rada policije na rizike počinitelja

Provalnici vjeruju da kod provalnih krađa postoji razmjer između napora koji je potrebno uložiti u počinjenu provale, rizika i koristi. (Pavišić, Modly, Veić, 2012, 215). Možemo li onda znanja i iskustva u upravljanja rizikom, odnosno identificiranja, analize i obrade rizika koristiti kao pristup u provjeri jesu li počinitelji kaznenih djela uspješno upravljali rizicima u

„vlastitom“ procesu počinjenja kaznenog djela? Ovakvo promišljanje u kriminalističkom istraživanju provala u dom zahtijeva poznavanje uobičajenog načina ponašanja odnosno aktivnosti počinitelja kod takvih kaznenih djela. Najčešće aktivnosti u procesu provalnih krađa u domove prema procesnom pristupu kako smo ga prethodno prikazali na primjeru procesa racije na slici broj 3, možemo prikazati kao slijed aktivnosti počinitelja na slici broj 5. Cilj počiniteljeva procesa možemo opisati: počinjenja kaznenog djela na način da se sakriju tragovi i predmeti kaznenog djela i ne utvrdi njegov identitet.

Kako bi ostvario svoj cilj, počinitelj provodi više aktivnosti koje najčešće imaju slijed kroz faze pripreme, te aktivnosti za vrijeme i nakon počinjenja kaznenog djela. Sve te njegove aktivnosti rezultiraju rizicima koji mogu naštetiti ostvarenju njegova cilja. Rizike nastoji eliminirati ili svesti na prihvatljivu razinu mjerama i radnjama koje poduzima. On njima želi nadzirati odnosno kontrolirati svoje aktivnosti. Zato je poželjno da policijski službenici znaju prepoznati kontrole (radnje) koje počinitelj najčešće poduzima kako bi zaštitio svoje aktivnosti, odnosno svoj protuzakoniti proces i da se usmjere na provjeru je li počinitelj bio uspješan u nadzoru svojih rizika.

U fazi pripreme počinjenja kaznenog djela, jedna od prvih aktivnosti jest da počinitelj prikuplja detaljne informacije o mjestu počinjenja kaznenog djela, predmetima odnosno vrijednostima koje može otuđiti i pogodnom vremenu počinjenja kaznenog djela. Glavni rizici koji se u njegovim aktivnostima javljaju su da njegova „znatiželja“ za potrebnim podacima ne izazove sumnju kod oštećenog ili drugih osoba koje raspolažu takvim podacima. On ove rizike obrađuje i pokušava ih kontrolirati tako da potrebne informacije prikuplja naizgled nezainteresirano, uzgred ili dolazi do informacija i putem posrednika, a ne samog vlasnika. Iz tog razloga radnje policije mogu se usmjeriti na provjeru je li počinitelj uspješno kontrolirao rizike već na samom početku svog procesa.

Praksa i iskustvo istraživanja nam zbog toga nameću potrebu da tijekom razgovora s oštećenim ili prijaviteljem utvrdimo a) vrijeme počinjenja djela, b) što je počinitelj morao poduzeti da počini djelo baš na taj način, c) na koji način i od koga je počinitelj mogao doći do informacije koje su mu bile potrebne za počinjenje kaznenog djela, d) podatke o nastaloj šteti, odnesenim predmetima i njihovu identitetu e) podatke o sumnjivim osobama (njihov identitet, spol, osobni opis, posebni osobni znaci, način odijevanja, ponašanje, eventualni govor) (Pavišić, Modly, Veić, 2012, 202).

Razvidno je da odgovor na pitanje c) na koji način i od koga je počinitelj mogao doći do informacije koje su mu bile potrebne za počinjenje kaznenog djela je podatak koji bi mogao pojasniti početak procesa počinitelja u pripremi i planiranju počinjenja kaznenog djela.

Ukoliko se u razgovoru s oštećenim ili prikupljanjem obavijesti od drugih osoba, dođe do podataka o osobi koja je prikupljala takve podatke, otvara se „put“ pronalaženju počinitelja. Zbog toga razgovor s oštećenim, ali i drugim ukućanima treba biti detaljan. Ponekad ga je dobro i ponoviti. Tijekom razgovora poželjno je doći do podataka koji bi pomogli utvrditi krug osoba kojima su bili dostupni podaci o vrijednostima otuđenih predmeta. „Oštećena lica su sklona pretjerivanju, nesvjesnom izvrtanju činjenica, neosnovanom sumnjičenju iz različitih razloga, ovisno tome kakvo djelo se dogodilo, radi li se o materijalnoj ili moralnoj šteti, o odnosu sa učiniocem, o njegovoj vlastitoj ličnosti itd. Dobro zaprimljena i

dokumentirana kaznena prijava je osnovni dokument i orijentacija u traganju za učiniocem. Zbog toga ne treba postupati birokratski već treba biti u češćem kontaktu s oštećenim radi eventualne dopune kaznene prijave novim podacima i indicijama“ (Roso, 1988, 183)

Sljedeću od aktivnosti koju možemo izdvojiti u pripremi počinjenja kaznenog djela je „snimanje“ navika ukućana i promatranje objekta (doma) provala. Cilj počinitelja je planiranje pogodnog vremena počinjenja, pronalaska najboljeg pristupa objektu i svladavanje prepreke nabavom odgovarajućeg provalničkog alata i dr. Glavni rizici kojima je počinitelj ovdje izložen su ostavljeni tragovi na mjestu motrenja koji mogu pomoći njegovoj identifikaciji, zapažanje njegova promatranja i moguća identifikacija od strane oštećenog ili susjeda, povezivanje njegova identiteta s nabavom provalničkog alata i sl. Stoga počinitelj poduzima mjere opreza, maskira se, odnosno nosi kapu, šal, dolazi na mjesto motrenja pješice, ne nosi ili ne komunicira s mobitelom, ne baca opuške, izbjegava objekte u svom susjedstvu. Zadaća policije je provjeriti je li počinitelj poduzeo sve ove kontrolne *mjere opreza.*

U praksi se zato pribjegava izlasku na mjesto događaja. Pod izlaskom na mjesto događaja ne misli se na očevid već na operativni zahvat koji u svom početnom dijelu ima za cilj samo neposredno sagledavanje opće situacije, na osnovi kojeg će se odlučiti o usmjeravanju izvida odnosno poduzimanja izvidnih mjera i radnji i pojedinačnih dokaznih radnji. (Pavišić, Modly, Veić, 2012, 202). Izlaskom na mjesto događaja policijski službenici mogu biti usmjereni na provjeru kako je počinitelj kontrolirao „prijetnje“ svom procesu.

U samoj fazi počinjenja kaznenog djela, kako bi zaštitio svoj identitet, prvi rizik koji mora eliminirati je zatjecanje na mjestu počinjenja kaznenog djela. Iz tog razloga počinitelj odabire povoljan objekt za provalu iz kojeg će moći lako „odstupiti“, zatim mjesto prodiranja u objekt koje je zaštićeno od pogleda susjeda ili slučajnih prolaznika, planira vrijeme počinjenja djela kada je najmanja mogućnost dolaska ukućana, obilaska policije ili čuvara i slično. Također, profesionalan počinitelj ostavlja odstupnicu u slučaju iznenadnog dolaska osoba odnosno planira „izlaz za nuždu“, ostavljajući otvorena vrata balkona ili prozora i sl. Nastoji se kretati u zaštićenim dijelovima objekta od pogleda izvana, kako se ne bi primijetio njegov boravak u stanu, od susjeda ili drugih osoba. Provjera policije kako je počinitelj kontrolirao ove rizike može biti usmjerena na intenzivno traženje tragova u pretpostavljenim prostorima kretanja počinitelja unutar objekta. Ovakav heuristički pristup[47] znatno može ubrzati istraživanje i dovesti do otkrivanja počinitelja.

Sljedeća skupina rizika su tragovi koji izravno omogućuju identifikaciju počinitelja. Naime, aktivacijom ovog rizika posljedice za počinitelja su „katastrofalne“. One najčešće dovode do uhićenja i mogu biti od velikog značaja u kaznenom postupku. Ovaj rizik počinitelji nastoje eliminirati ili smanjiti na prihvatljivu razinu tako da nose rukavice, ne ostavljaju eventualne tragove krvi ili druge nositelje tragova koji bi mogli dovesti do njihove izravne identifikacije. Stoga je policija usmjerena na pronalazak upravo takvih tragova prilikom obavljanja očevida.

[47] Karas, Ž.(2012), prema Grrasberger, Martin; Schmid, Harald, Todesermittlung: Befundaufnahme und Spurensicherung, Springer, Wien, 2009. „Pitanje heurističkog pristupa se može promatrati ne samo na razini cijelog kriminalističkog istraživanja, nego i na razini provedbe pojedinih kriminalističkih radnji. Primjer je traženje tragova na mjestu događaja. Ako se pokušava neodređeno tražiti, radi se heurističkoj metodi, koju se smatra subjektivnom jer ovisi o *iskustvu, nagađanjima* ili *očekivanjima* pojedinačne osobe.“

Počinitelj se u fazi počinjenja može susresti i s drugim rizicima kao što su nepodoban provalnički alat, nedostatak znanja za nečujno svladavanje prepreke, zatjecanje neposredno nakon počinjenja kaznenog djela, i drugi.
Nakon samog počinjenja kaznenog djela, za počinitelja i dalje postoji opasnost da ga netko vidi kako se udaljava, da ga policija zaustavi i legitimira, te bira odlazne putove koji su najmanje naseljeni, na kojima nema nadzornih kamera ispred objekata kao što su banke, pošte i slične institucije. Stoga policija provjerava moguće odlazne putove počinitelja, obavlja provjeru legitimiranih osoba u kritično vrijeme počinjenja u bližoj i široj okolini mjesta počinjenja kaznenog djela i poduzima druge mjere i radnje koje nam se ukažu potrebnima.
Značajni rizici za utvrđivanje identiteta počinitelja javljaju se prilikom prodaje predmeta kaznenog djela koji su otuđeni. Prijetnje koje mogu povezati otuđene predmete s identitetom počinitelja mogu se nalaziti u jedinstvenim obilježjima predmeta odnosno njegovim identifikacijskim oznakama kao što su npr. tvornički broj. Značajan rizik koji počinitelji žele eliminirati jest mogućnost njegove identifikacije putem osobe kojoj prodaje ukradeni predmet. Zbog toga počinitelj poduzima mjere kao što su uništenje identifikacijskih oznaka na predmetu ili se rješava predmeta putem posredne prodaje. Također, počinitelj procjenjuje hoće li se predmeta riješiti odmah ili nakon proteka određenog vremena. Naime, procjenjuje je li manja vjerojatnost i nepovoljni učinak za njegovu identifikaciju ukoliko predmet prodaje nakon proteka određenog vremena, a za to vrijeme predmet drži npr. u skloništu, kod osobe od povjerenja i sl. Nedovoljno „stručno“ i „profesionalno“ postupanje počinitelja je iskazivanje njegove slabosti (ranjivosti) prilikom počinjenja kaznenog dijela. Na taj način njegov proces postaje ranjiv i aktiviraju se glavni rizici koji se očituju u njegovoj identifikaciji i pronalasku materijalnih tragova i drugih dokaza što u pravilu rezultira kaznenim postupkom i osudom počinitelja kao posljedicom.

4. ZAKLJUČAK

Proces upravljanja rizikom ne uvodi nove mjere i radnje, niti nova pravila o načinu izvođenja pojedinih policijskih stručnih poslova ili dokaznih radnji. Proces se, uz uvažavanje posebnosti policijskog rada, može koristiti na operativnoj razini policijske organizacije kao jedan od pristupa u predviđanju odnosno pogled unaprijed u proceduri kriminalističkog istraživanja. Upravljanje rizikom pruža novu mogućnost u promišljanju i pristupu rukovoditelja i kriminalističkih istražitelja koje radnje su prioritet kako bi se eliminirali štetni događaji koji mogu omesti ostvarenje cilja u procesu kriminalističkog istraživanja provala u dom. Također, i pristup u kojem istražitelji promišljaju o rizicima kojima je počiniteljev protuzakoniti „proces„ provale u dom najviše bio izložen, omogućuje lakše rekonstruirati njegovo ponašanje prilikom počinjenja kaznenog djela i odrediti prioritete u poduzimanju odgovarajućih mjera i radnji na njegovu otkrivanju.
Policijski procesi na neposrednoj razini policijske organizacije, kao što je i proces kriminalističkog istraživanja provala u dom, zahtijevaju sustavno prikupljanje praktičnih iskustava što se kvalitetno može ostvariti kroz fazu monitoringa i pregleda u procesu upravljanja rizikom. Prihvaćena opća tipologija rizika javnog sektora, uz prihvaćanje

posebnosti policijskog sustava i rada, može nam pomoći za grupiranje i profiliranje rizika u policijskim procesima.

LITERATURA

Knjige i članci

Broder, F., J. (2003). Analiza rizika i ispitivanje sigurnosti. *Izbor članaka iz stranih časopisa*, Zagreb: MUP (1-2), 3-4.

Dujmović, Z. (1992). Osnovne karakteristike imovinskog kriminaliteta u RH. *Defektologija*, 28(1-2), 213-243.

Grigoliet, B., Štrk, D., Wulf, P. S. (2005). Taktika policijskog postupanja. Zagreb: MUP RH.

Jurak, F. (1993). Organizacija i funkcioniranje policije Zagreb: MUP RH.

Jurina, M. (2008). Organizacija i menadžment. Zaprešić: Visoka škola za poslovanje i upravljanje s pravom javnosti „Baltazar Adam Krčelić".

Karas, Ž. (2012). Uvod u kriminalistiku (odabrana poglavlja), Zagreb: MUP RH.

Karas, Ž. (2015). Kriminalistički značaj pribavljanja osumnjičenikovog iskaza. *Policija i sigurnost*, 2, Zagreb: MUP RH.

Nađ, I., Relić, D. (2012). Procjena rizika kod nasilnog ulaska u dom ili druge zatvorene prostorije (http://www.kvalis.com/o-portalu/item/710 (09.02.2016).

Pavišić, B., Modly, D., Veić, P. (2006). Kriminalistika 1. Rijeka: Sveučilište u Rijeci.

Pavišić, B., Modly, D., Veić, P. (2012). Kriminalistika 2. Rijeka: Sveučilište u Rijeci.

Pusić, E. (2002). Nauka o upravi. Zagreb: Školska knjiga.

Roso, Z. (1988). Informativni razgovor i intervju. Zagreb: MUP RH.

Internetski izvori

Alarm, airmic, IRM (2010) A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31 000, https://www.theirm.org/media/886062/ISO3100_doc.pdf (08. 02. 2016.).

Adelsberger, Z.: Stručni prilozi: ISO 31000 i generički pristup upravljanja rizicima. http://www.kvalis.com (21. 12. 2015.).

Adelsberger, Z.: Operativni rizici kao temelj sustava upravljanja, http://www.kvalis.com (21. 12. 2015.).

Izvor: Adelsberger, Z, ISO 31000 - Upravljanje rizicima. http://www.kvalis.com (21. 12. 2015.).

Ministarstvo financija (rujan 2009, Zagreb), Smjernice za provedbu procesa upravljanja rizicima kod korisnika proračuna, (http://www.mfin.hr- 08. 02. 2016.).

Ministarstvo unutarnjih poslova (studeni 2015.)., Strategija upravljanja rizicima za razdjel MUP-a (http://www.mup.hr/112629.aspx - 09. 02. 2016.).

Nađ, I., Relić, D. (2012). Procjena rizika kod nasilnog ulaska u dom ili druge zatvorene prostorije (http://www.kvalis.com/o-portalu/item/710 - 09. 02. 2016.).

Propisi

Zakon o policijskim poslovima i ovlastima. NN 76/09.,92/14. Zagreb: Narodne novine.

Zakon o sustavu unutarnjih kontrola u javnom sektoru. NN 78/15. Zagreb: Narodne novine.
Zakon o kaznenom postupku. NN, 152/08., 76/09., 80/11., 91/12. - Odluka i Rješenje USRH, 143/12., 56/13., 145/13. i 152/14. Zagreb: Narodne novine.

Davor Labaš
Krešimir Filipić

CRIMINAL INVESTIGATION OF BURGLARY - POSSIBILITIES OF RISK MANAGMENT APPROACH

Summary

Risk managment is one of the tools organisations use for succesfully managing organisation processes in achieving their goals. Strategic commitment of Ministry of Internal Affairs is an application of risk managment on every organisation level. Police proffesion is constantly in incertitude while taking corresponding actions. Risk managment can give quality future perspective in individual proces development. It also helps when decisions about measures and actions for risk elimination are to be made. The work is based on case analysis and previous practical experience, and it describes and clarifies main activities in burglary criminalistic research process. Representing and using optional norm ISO 31000 for risk managment, it identifies main risks in criminalistic research process, as well as most common measures and actions used by police officers in risk managment.
Burglary offenders estimate effort required, possible risks and the value of the object they are about to steal. They tend to lower and then take control of the risks. Nne oft he keys in proces of offender identification is focusing police work on risk recognition to which offender was exposed by commiting a criminal offence, as well as analysing if and how he controled them. The purpose of this article is to point out possibilities and need for risk managment introduction as approaches in police process managment.

Key words: *burglary**,** criminal investigation, risk managment, operative police processes.*

STRUČNI RAD

Tanja Kaurin[48]
Zdravko Skakavac[49]

ZNAČAJ DIGITALNE FORENZIKE MOBILNIH UREĐAJA U OTKRIVANJU I DOKAZIVANJU KRIVIČNIH DELA ORGANIZOVANOG KRIMINALITETA

Sažetak

Digitalno doba je radikalno promenilo svaki aspekt naše svakodnevnice donoseći sa sobom nove globalne pretnje. Premošćavajući fizičke granice internet je ponudio neprocenjive mogućnosti za države i pojedince uz neminovne ranjivosti. Eksploatišući brzinu, praktičnost i anonimnost interneta kriminalne mreže su olakšale koordinaciju između svojih članova bez obzira na njihovu fizičku lokaciju. Otvorio se prostor za izvršenje širokog spektra zločina koji ne poznaje granice, bilo fizičke ili virtuelne, dramatično smanjujući vreme potrebno za organizovanje i izvršenje složenih kriminalnih aktivnosti. Sajber okruženje je zapravo pogodovalo organizovanom kriminalitetu koji je odavno poprimio ozbiljne razmere, kako po fenomenološkim aspektima, tako i po pitanju posledica koje ostavlja, a mobilnost je samo dodatno usložila bezbednosnu situaciju.
Cilj rada je da ukaže na značaj primene digitalne forenzike u otkrivanju krivičnih dela organizovanog kriminaliteta bez obzira da li su u pitanju klasične kriminalne aktivnosti ili one koje spadaju u domen sajber kriminala. Iz tog razloga akcenat je stavljen na digitalnu forenziku mobilnih uređaja, pre svega zbog njihove sveprisutnosti ali i zbog individualnosti u upotrebi. Pored objašnjenja digitalnih dokaza do kojih možemo doći forenzikom mobilnih uređaja dat je praktičan primer akvizicije podataka primenom Cellebrite UFED Analyzer-a.

Ključne riječi: *digitalna forenzika, sajber kriminal, forenzika mobilnih uređaja, organizovani kriminalitet.*

1. UVOD

Teško da postoji uređaj koji po brojnosti i frekventnosti upotrebe može nadmašiti mobilne telefone. Podatak da je broj mobilnih korisnika prevazišao broj ljudske populacije govori u prilog činjenici da postojanje i analiza digitalnih dokaza na mobilnim uređajima postaje sve značajnija u istrazi i krivičnom gonjenju različitih vrsta zločina jer može da razotkrije sklonosti, kretanje osumnjičenih, komunikaciju, poveže sa određenim ljudima/kriminalnim gurpama i pruži potencijalno ključne informacije o zločinu. Činjenica da moderni mobilni

[48] Tanja Kaurin, Fakultet za pravne i poslovne studije dr. Lazar Vrkatic, Novi Sad, Srbija, e-mail: tanja.kaurin@useens.net
[49] Zdravko Skakavac, Fakultet za pravne i poslovne studije dr. Lazar Vrkatic, Novi Sad, Srbija, e-mail: zskakavac@useens.net

telefoni imaju karaktersitike koje su dugi niz godina bile rezervisane isključivo za desktop računare dodatno govori u prilog njihove primenljivosti.

Teroristički napad u Mumbaju novembra 2008. godine je samo jedan u nizu primera koji pokazuju do koje mere se mobilni telefoni mogu koristiti kao oružje. Teroristi su koristili satelitske telephone i GPS da napadnu nekoliko ciljeva sa smrtonosnom preciznošću. Najneobičniji deo ovog napada je zapravo do koje mere su koristili mobilne telefone jer su bili povezani tokom svake faze od početka do kraja. GPS im je pomagao i da se efikasno kreću gradom a ciljeve kao i direktne puteve do njih su prepoznavali delimično i zbog toga što su proučavali satelitske fotografije sa Google Earth-a. Napad u Mumbaju svakako nije prvi u kome su teroristi koristili mobilne telefone ali način na koji su to radili je značajan za otkrivanje i jedinstven. U ovom slučaju korišćeni mobilni telefoni su bili nosioci velike količine podataka koje su mogle da se iskoriste kao digitalni dokazi.

Organizovane kriminalne grupe širom sveta oslanjaju se na internet i mobilnu komunikaciju prilikom organizovanja, kontaktiranja i upoznavanja sa potencijalnim ciljem. Terorističke organizacije koriste internet za regrutovanje, pranje novca, krađu kreditnih kartica i širenje propagande. Najveće organizovane pljačke se sprovode upravo putem računarskih mreža.
Sve navedeno ukazuje na mnoštvo digitalnih podataka, potencijalnih dokaza, koji se nalaze svuda oko nas i ne smeju biti zanemareni u istragama. Vrste podataka koji se nalaze u okviru mobilnih uređaja i način na koji se koriste stalno se razvijaju te se prikupljanjem podataka može zaključiti mnogo više od istorije poziva, razmene tekstualnih poruka ili stavki u kalendaru. Pored velike raznovrsnosti mobilnih uređaja koji su komercijalno dostupni, prisutni su i različiti operativni sistemi, sistemski fajlovi, aplikacije, servisi i periferije. Sve to pruža mnogo mogućnosti ali i velike izazove za digitalnu forenziku mobilnih telefona. Svaki od ovih uređaja je hardverski i softverski specifičan te može biti podržan forenzičkim alatima do određenog nivoa, ali se može desiti i da nije podržan uopšte.

U radu je obrađen pojam organizovanog kriminaliteta sa akcentom na promene koje je doneo dramatičan tehnološki razvoj. Zbog ogromnog uticaja mobilnih uređaja i u organizovanim kriminalnim grupama upotrebe mobilnih komunikacija akcenat je dat na digitalnoj forenzici mobilnih uređaja kao dobrom rešenju za ubrzanje i povećanje uspešnosti istrage. U trećem poglavlju je objašnjen pojam digitalne forenzike, opšta pravila i komponente da bi preko četvrtog poglavlja i pojašnjavanja specifičnosti vezanih za digitalnu forenziku mobilnih telefona došli do petog u kome je na praktičnom primeru – ekstrakcije podataka primenom Cellebrite UFED Touch-a pokazano koje se vrste podataka mogu prikupiti i od kakvog je to značaja za istragu.

2. ORGANIZOVANI KRIMINALITET

Organizovani kriminalitet, kao univerzalna i istorijska pojava je savremeni društveni fenomen koji ozbiljno ugrožava čovečanstvo. U suštini, organizovani kriminalitet je specifični oblik savremenih vidova profesionalnog kriminaliteta koji se po mnogim osobinama razlikuje i od tradicionalnih vidova zločinačkog udruživanja, kao i od klasičnih oblika kriminaliteta kako

nacionalnih tako i međunarodnih razmera. Danas se sa sigurnošću može tvrditi da ni jedan kontinent a ni država nisu pošteđene ove pojave. Pitanje je samo razmera i obima pojednih fenomenoloških aspekata ove pojave. Skoro sve države u svetu, bez obzira na politički sistem i stepen razvoja, suočene su sa problemom da se suprotstave raznim oblicima savremenog kriminaliteta (Skakavac, 2007).

Rob Wainwright direktor Europol-a je istakao: „Organizovani kriminalitet je dinamičan i prilagodljiv i predstavlja izazov za organe sprovođenja zakona širom EU kako bi održale korak sa promenljivom prirodom ove ozbiljne pretnje“.

Suočene sa izazovima organizovanog kriminala, sa njegovom ogromnom društvenom opasnošću i specifičnostima u odnosu na „obični“ kriminal, savremene države i međunarodna zajednica u poslednje vreme donose posebne materijalnopravne, organizacione i procesne propise za njegovo sprečavanje, otkrivanje i suzbijanje. Tim se propisima ustanovljavaju posebni organi za borbu protiv organizovanog kriminala, sa širim ovlašćenjima pre krivičnog postupka i u krivičnom postupku nego što ih inače imaju organi krivičnog gonjenja. To pretpostavlja bitna odstupanja od ustaljenih i do sada opšteprihvaćenih načela krivičnog materijalnog i procesnog prava i stavova o krivičnoj odgovornosti i kažnjivosti učinilaca krivičnih dela (Grubač, 2002).

Korišćenje posebnih dokaznih mehanizama u pretkrivičnim i krivičnim postupcima protiv najtežih oblika kriminaliteta, temelji se na zaključku da “klasični”, u praksi uobičajeni dokazni metodi nisu dovoljni, jer zbog same prirode najtežih krivičnih dela i njihovih učinilaca, njima se ne mogu postići zadovoljavajući rezultati u sudskom postupku.

Krajem 20. veka, primena specijalnih istražnih tehnika je stekla i svoje međunarodno utemeljenje, pored onog navedenog u nacionalnim zakonodavstvima. Do tada je bilo neuobičajeno da se međunarodni pravni akti upuštaju u rešavanje određenih konkretnih dokaznih pitanja, vezanih za posebne tehnike prikupljanja i obezbeđivanja dokaza, ali je razvoj i priroda najtežih oblika kriminaliteta uticala da se ova pitanja rešavaju i na međunarodnopravnom nivou, jer je prema problemima u praksi, shvaćeno da se na drugi način ne može voditi uspešna borba protiv najtežih oblika kriminaliteta, a posebno onih koji imaju međunarodni karakter (Milošević, 2003).
Korišćenje posebnih dokaznih radnji ili specijalnih istražnih ovlašćenja ili posebnih tehnika istrage, posebno je značajno kada su u pitanju sofisticirane i složene kriminalne operacije, kao “pranje” novca, kada se deluje u sprezi sa određenim poslovnim subjektima, pre svega bankama i drugim finansijskim organizacijama. U članu 4. stav 2. Konvencije o pranju, traženju, zapleni i konfiskaciji prihoda stečenih kriminalom omogućeno je državi potpisnici da usvoji zakonodavne i druge neophodne mere, koji mogu da obuhvate i naloge za pristupe kompjuterskim sistemima i izradu određenih dokumenata (Škulić, 2003).

2.1. Organizovani kriminalitet u sajber okruženju

Ozbiljne kriminalne grupe maksimalno eksploatišu tehnološki napredak, posebno razvoj Interneta za generisanje novih zločina ali i modifikaciju klasičnih. Očigledne su namere, maštovitost i razvoj sposobnosti da se iskoriste sve potencijalne slabosti informacionih sistema i identifikuju novi načini za izvršavanje kriminalnih dela (SOCA, 2006:10).

U izveštaju "Exploring tomorrow's organised crime" koji je EUROPOL izdao u martu 2015. kao ključni pokretači budućih promena navode se:

- Inovacije u transportu i logistici omogućavaju organizovanim kriminalnim grupama sve veći broj počinjenih zločina anonimno preko interneta, bilo gde i bilo kada, bez fizičkog prisustva.
- Nanotehnologija i robotika otvaraju nova tržišta za organizovani kriminal i nove alate za sofisticirane kriminalne šeme.
- Sve veća eksploatacija Big Data i ličnih podataka omogućava organizovanim kriminalnim grupama da obavljaju složene i sofisticirane krađe identiteta.
- E-otpad se pojavljuje kao ključna nezakonita roba za organizovane kriminalne aktivnosti u Evropi.
- Ekonomske nejednakosti u Evropi čine da organizovani kriminal postaje društveno prihvatljiv jer se organizovane kriminalne grupe infiltriraju u ekonomski oslabljene zajednice predstavljajući se kao provajder rada i usluga.
- Organizovane kriminalne grupe će pokušati da se infiltriraju u industrije koje zavise od prirodnih resursa kao brokeri ili agenti u trgovanju.
- Virtualne valute omogućavaju pojedincima da budu samostalni u kriminalnim aktivnostima koristeći poslovni model kriminal-kao-usluga (crime-as-a-service) bez potrebe za sofisticiranom kriminalnom infrastrukturom za prijem i pranje novca.
- Organizovane kriminalne grupe će se skoncentrisati na sve veći broj starijih osoba koje počinju da koriste mogućnosti interneta nudeći im nezakonite usluge i robu.

  Osnovna podela organizovanih kriminalnih grupa koje koriste informaciono-komunikacione tehnologije (ICT) za izvršavanje kriminalnih aktivnosti (Kim-Kwang, 2008):

- tradicionalno organizovane kriminalne grupe koje ICT koriste samo kao sredstvo za pomoć u izvršavanju klasičnih kriminalnih radnji;
- organizovane sajber kriminalne grupe koje djeluju isključivo online i
- organiziovane grupe ideološki i politički motivisanih pojedinaca koji koriste ICT kako bi olakšali svoje kriminalno ponašanje.

2.2. Tradicionalno organizovane kriminalne grupe

Uključivanjem tradicionalno organizovanih kriminalnih grupa u kriminalne radnje potpomognute informacionim tehnologijama povećava se broj kriminalnih aktivnosti koje rezultuju ogromnim profitom. Primera radi Internet je obezbedio novo i mnogo veće tržište za one koji su uključeni u prodaju falsifikovane i piratske robe. Jedno od područja koje beleži konstantan rast su falsikovani lekovi. Razlozi leže pre svega u visokoj ceni pregleda i recepta, teškoćama do kojih može doći, ili zbog neugodnosti pacijenta da potraži određeni lek u

lokalnoj apoteci. Internet omogućava falsifikatorima da se na jeftin i jednostavan način oglašavaju, pronađu adekvatno tržište i lako distribuiraju svoje proizvode, što značajno olakšava aktivnosti kriminalnih grupa. (UK OCTF, 2007: 34).

Globalizacija i trend migracija takoreći brišu nacionalne granice i ubrzavaju proces transformacije kriminala, brišu izvore i otežavaju detekciju uzroka zločina udaljavajući ga od domaće baze. Masovna migracija iz manje razvijenih zemalja u zapadne zemlje dovela je do je etno-nacionalnih kriminalnih grupa koje su povezane sa svojom otadžbinom što koriste za pljačkanje emigranta posebno ilegalnih. U tome prednjače korejske, vijetnamske, kineske, ruske (misli se na područje bivšeg Sovjetskog Saveza), karipske i Južnoameričke organizacije koje deluju na području SAD-a, Velike Britanije i Evrope. U zemljama zaliva su indijske, pakistanske, Šri Lanke i Bangladeške bande (Singh, 2007: 80).

Uprkos vladinim naporima na razbijanju organizovanih kriminalnih aktivnosti, ove kriminalne grupe su prepoznale ICT kao dragocen alat koji olakšava ili poboljšava izvršenje zločina. Svoje aktivnosti i znanja prilagođavaju tehnološkim promenama te koriste ICT kako bi unapredili kriminalne aktivnosti kao što su krijumčarenje narkotika, trgovina ljudima, trgovina korporativnim identitetom i tajnim informacijama, izvršenja iznude, prevare i prevare na mreži, pranje novca koji se koriste za onlajn plaćanja, širenje ilegalnih materijala preko interneta, kao i upotreba interneta za prodaju falsifikovane robe (pre svega farmaceutskih proizvoda i lekova) (Skakavac i Kaurin, 2012).

Pored klasičnih kriminalnih radnji koje su jednoznačno profitno orijentisane, tradicionalno organzovane kriminalne grupe sve češće koriste lažne ili ukradene identitete da počine ne-fiskalne prevare. U te tipove prevara spadaju:

- Napad na računarske mreže i neovlašćen pristup zarad pristupa osetljivim informacijama;
- Phishing;
- Spam;
- Projektovanje i širenje zlonamernog softvera;
- Internet prevare koje uključuju Nigerijsku prevaru (poznatu kao šema 419), onlajn aukcijsku prevaru, prevare sa lažnim identitetom i lažnim karticama.

2.3. Organizovane sajber kriminalne grupe

Uprkos sinergiji između tradicionalno organizovanih kriminalnih grupa i cyberspacea, tradicionalne grupe organizovanog kriminala ne treba mešati sa organizovanim sajber kriminalnim grupama koje djeluju isključivo online. Ove sajber grupe, sajber mafija kako ih često nazivaju, funkcionišu u specifičnom okruženju koje nameće posebna pravila i odnose. Virtuelno okruženje i ICT oružje u rukama stručnjaka otežava razotkrivanje njihovih krminalnih aktivnosti. Kao što je Eugene Kaspersky, osnivač i rukovodilac istraživačkog i razvojnog sektora čuvenog anti-virusa Kaspersky Lab, primetio: „IT kriminalci su samo ljudi koji promene svoje mišljenje ili imaju poremećen um. IT kriminalci ne vide svoje žrtve, tako

da im je lakše načiniti kriminalnu radnju jer ne osećaju svoju ruku u tuđem džepu“ (Infosecurity, 2007).

U zavisnosti od kriminalnih aktivnosti kojima se bavi određena organizovana sajber krminalna grupa zavisi i organizaciona struktura grupe i potreba za članovima sa specifičnim znanjima/veštinama. Često se pojedinci angažuju po potrebi i na određeno vreme koje je potrebno za obavljanje konkretnog zadatka. Ovakve grupe su fleksibilnije sklone su manjem broju članova i nisu tradicionalno organizovane. Brenner (Brenner 2002:27) objašnjava: fizička snaga je beznačajana u sajber svetu. Haker probija žrtvinu odbranu koristeći tehnologiju, automatizovane tehnike koje omogućavaju pojedincu da zaobiđe softversku odbranu. U sajber svetu, snaga je u softveru, a ne u snazi pojedinca ili broju članova grupe.
Profil članova organizovane sajber kriminalne grupe:

- Tehnički sofisticirani članovi. Zločini načinjeni upotrebom tehnologija podrazumevaju da izvršioci posjeduju određeni nivo tehničkih znanja i veština rada na računaru. Važno je da poznaju ranjivosti sistema i kako ih mogu iskoristiti. Avi Rubin profesor informatike na Johns Hopkins univerzitetu ističe da su takvi kriminalci skloni korišćenju naučne literature i daleko više tehnički orijentisani nego kalsični kriminalci. Studije Kshetri (2006) i Jen et al. (2006) pokazuju da značajan procenat sajber kriminalca u Rusiji i Tajvanu spadaju u obrazovanu generaciju Y grupe (definisane kao osobe rođene nakon 1982).
- Članovi koji se poznaju isključivo onlajn. Shodno svojim interesovanjima istomišljenici se pronalaze na forumima i chat sobama te uz pomoć Interneta planiraju aktivnosti.
- Isključivo finansijski motivisani članovi.

2.4. Organizovane grupe ideološki i politički motivisanih pojedinaca

Pre 11. septembra 2001, terorizam i organizovani kriminalitet su se obično posmatrali kao zasebne celine, jer se smatralo da nemaju isti motiv (npr. politička odluka vs. dobit). U poslednjih nekoliko godina, došlo je do konvergencija između terorizma i organizovanog kriminala u kojoj "dve strane 'organizovane' debate pronalaze veću utehu, nagrade i operativnu fluidnost kroz kombinaciju njihovih zajedničkih napora". FBI je istakao da "međunarodni organizovani kriminalci pružaju logističku i drugu podršku terorista, stranih obaveštajnih službi, kao i stranim vladama, sa interesima koji su izrazito nepovoljni za američku nacionalnu sigurnost" (FBI, 2008).

3. DIGITALNA FORENZIKA

Stopa razvoja digitalne tehnologije, sa manjim odstupanjima, i dalje prati Murov zakon predstavljen u časopisu “Electronics” aprila 1965. godine koji je glasio „broj tranzistora koji se može smestiti na kvadratni inč silicijuma duplira se svakih 12 meseci (predložen broj meseci je 1975. korigovan na 24)”. Ovaj zakon, se nije odnosio samo na prost broj tranzistora, odnosno na njihovu veličinu, već i na smanjenje troškova izrade samih tranzistora. Razvoj tehnologije pokazao je da je krajnji efekat koji je Mur predvideo bio usmeren na pojavu, sada već sveprisutnih, jeftinih, moćnih tranzistora. Njegovo razmišljanje utemeljilo je pravac razvoja elektronske industrije u ostatku 20. veka i može se reći da su Murove naznake bile ispravno predviđanje pojave ličnog računara i prenosivih digitalnih uređaja. Od početka 21. veka, stopa rasta je malo usporena ali se još uvek udvostručuje u gustini svake dve godine. To znači da moderni mobilni telefoni imaju snažnije procesore i veće kapacitete za skladištenje od kompjutera koji je NASA koristila za slanje čoveka na Mesec. Spakovani u minjaturni hardver, sa mnogo većom pouzdanošću po neuporedivo nižoj ceni i izuzetno laki za upotrebu.
Jednu od najranijih definicija ovog pojma dao je (Pollitt, 1995): "Kompjuterska forenzika je primena nauke i tehnike u pravnoj primeni digitalnih dokaza. To je sinteza nauke i zakona. Na jednom kraju je čista nauka jedinica i nula. Na ovom nivou, poštuju se zakoni fizike i matematike. Na drugom kraju je sudnica". Ova definicija se smatra pionirskim poduhvatom jer obuhvata obe strane, proces i moguće ishode kompjuterske forenzike, povezujući kompjutersku analizu sa ciljem da se dobiju rezultati koji moraju biti zakonski prihvatljivi. U skladu sa navedenom definicijom (Kuchta, 2000) definiše kompjutersku forenziku kao "nauku koja se bavi primenom računara u relaciji sa pravnim pitanjima". Cilj računarske/digitalne forenzike prema (Carrier i Spafford, 2004) je "da se identifikuju digitalni dokazi korisni za istragu". Dalje objašnjavaju "U istrazi se za izvođenje zaključka uz naučne metode koriste i fizički i digitalni dokazi". (Ker, 2009) ukazuje na to da digitalna forenzika kombinuje računarsku nauku uključujući arhitekturu računara, operativne sisteme, sisteme datoteka, softverskog inženjerstva i mrežnu organizaciju, podjednako kao i zakonske procedure koje se primenjuju na krivične i građanske sporove, visokotehnološki kriminal i zakon o dokazima. Primena digitalne forenzike obuhvata identifikaciju aktivnosti zahtevanih u istrazi (uključujući određivanje relevantnih digitalnih izvora), prikupljanje informacija, čuvanje informacija od slučajnih promena, njihovu analizu i izveštavanje o rezultatima istrage (Casey, 2004). Digitalna/kompjuterska forenzika podrazumeva primenu nauke sa ciljem pojašnjenja dokaza na sudu.

Na osnovu navedenih definicija može se doći do zaključka da je digitalna forenzika nauka koja ima za cilj prikupljanje, čuvanje, pronalaženje, analizu i dokumentovanje digitalnih dokaza odnosno podataka koji su skladišteni, obrađivani ili prenošeni u digitalnom obliku. Prilikom prikupljanja digitalnih dokaza neophodno je primenjivati zakonski dozvoljene postupke i alate. Digitalna forenzika stručnjaku omogućava fizičku i logičnu rekonstrukciju dokaza potrebnih u odgovarajućem postupku (civilnom, kaznenom, privrednom…) podrazumeva forenziku svoh digitalnih nosioca podataka i nije ograničena samo na lične računare. Činjenica da se digitalni dokazi ne nalaze isključivo na računarima ukazuje na to da

će potreba za digitalnom forenzikom i digitalnim dokazima neprestano rasti i biti neophodna prilikom istrage širokog spektra kriminalnih radnji (Skakavac i Kaurin, 2012).

Digitalna forenzika ima svoju tehničku komponentu, odnosno alate u obliku odgovarajućeg softvera i hardvera, ali i svoju pravnu komponentu u smislu poštovanja određenih principa, pravila i metodologije. Neophodno je da odgovorna lica koja sprovode istragu dobro poznaju obe komponente kako bi poštujući pravnu i razumejući tehničku stranu mogli da obezbede validan digitalni dokaz, prihvatljiv na sudu. Digitalni sistemi sadrže značajne količine podataka koji se mogu iskoristiti kao dokazni materijal. Ukloniti digitalne dokaze je daleko teže nego što se uobičajeno misli. Metodama digitalne forenzike moguće je pronaći takav dokazni materijal te obrisane ili izgubljene podatke čak, i u slučaju namernog modifikovanja ili brisanja.

Opšte prihvaćena pravila digitalne forenzike definisao je Ken Zatyko (Zatyko, 2007):

- Princip zakonitosti podrazumeva da je u pravnim istragama pravni organ zadužen za pretres i oduzimanje podataka.
- Lanac istrage se odnosi na hronološko dokumentovanje rukovanjem dokazima tokom cele istrage.
- Slika i heš. Heš slike digitalnog dokaza i samog digitalnog dokaza moraju se poklapati što daje garanciju integriteta kopije.
- Validni alati. Ukoliko je moguće treba koristiti alate odobrene od strane suda kako bi se osigurala pouzdanost i tačnost.
- Analiza podrazumeva izvođenje istražnih i analitičkih tehnika za ispitivanje dokaza.
- Ponavljanje i reprodukcija. Ponavljanje procedure mora dovesti do istih zaključaka od strane bilo kog forenzičara i bez obzira kada se procedura ponovi.
- Izvještaj. Forenzičar mora dokumentovati analitički postupak i zaključke.
- Mogućnost ekspertskog svedočenja. Ukoliko je potrebno forenzičar treba da predstavi sudu nalaze i zaključke do kojih je došao.

Primena digitalne forenzike moguća je u dva smera. Prvi je reaktivni, znači nakon određenih nezakonitih događaja, istražitelji kreću u akciju otkrivanja počinica. U ovom slučaju glavni korisnici su „institucije pravne države“. Drugi smer je proaktivni, prvenstveno namenjen svima onima koji imaju vrlo vredne informacione resurse odnosno intelektualno vlasništvo.

Potpuno isti alati za digitalnu forenziku, ali primenjeni na malo drugačiji način se i ovde mogu koristiti sa ciljem preventivnog delovanja sprečavanja curenja informacija, krađe intelektualnog kapitala i sl. Reaktivna komponenta je tradicionalni (ili post-mortem) pristup istrazi digitalnog zločina nakon incidenta (Palmer, 2001). Ovakav pristup uključuje identifikaciju, očuvanje, prikupljanje, analiziranje i generisanje konačnog izveštaja.
Na ovaj način moguće je sakupiti dve vrste dokaza: aktivne i reaktivne.
Aktivni dokazi su oni koji se mogu sakupiti u realnom vremenu (*dynamic*) nakon incidenta. Primer takvog dokaza su aktivni procesi u memoriji.

Drugi tip, reaktivni dokazi, odnose se na prikupljanje svih preostalih statičkih dokaza, kao što je forenzička slika/kopija hard diska. (Alharbi et al, 2011: 59-72). Proaktivna komponenta je sposobnost da se proaktivno sakupljaju informacije koje su inicijatori za pokretanje događaja kao i čuvanje i analiza dokaza kako bi se identifikovao incident čim se pojavi. Pored toga, preliminarni izveštaj se automatska generiše za naknadno ispitivanje od strane reaktivne komponente. Dokazi koji se skupljaju na ovaj način su proaktivni dokazi koji se odnose na konkretni događaj ili incident čim se pojavi (Orebaugh, 2006:37). Za razliku od reaktivne komponente, faza sakupljanja u ovoj komponenti dolazi pre faze čuvanja sve dok incident još uvek nije identifikovan.

4. DIGITALNA FORENZIKA MOBILNIH TELEFONA

Digitalna forenzička zajednica suočena je sa stalnim izazovom-potrebom da ostane u toku sa najnovijim tehnologijama koje se mogu koristiti za izlaganje relevantnih dokaza u istrazi. Mobilni uređaji su uobičajeni u današnjem društvu i koriste se od strane pojedinaca za lične i poslovne svrhe. Razlikuju se u dizajnu i konstantno prolaze kroz promene postojeće tehnologije kao i uvođenje nove.

Shodno navedenim definicijama digitalne forenzike, digitalna forenzika mobilnih telefona se može definisati kao naučna disciplina koja se bavi pribavljanjem digitalnih dokaza iz memorija mobilnih telefona i SIM kartica u forenzičkim uslovima uz korišćenje prihvaćenih metoda (Vuković, 2011). Mobilni telefon predstavlja multifunkcionalni telekomunikacioni uređaj koji je postao deo čovekove svakodnevnice zahvaljujući svojim tehničkim karakteristikama. Upravo njegova funkcionalnost, jednostavno korišćenje i pristupačnost te da ne zahteva posebno tehničko obrazovanje za svakodnevnu upotrebu uslovila su pojavu mobilnih telefona kao sredstva za izvršenje krivičnih dela (snimanje fotografija i video snimaka određenih kriminalnih aktivnosti kao što je dečija pornografija i sl), kao objekt izvršenja krivičnog dela (otuđenje telefona ili izlaganje zlonamernim softverima) a kao najčešća pojava, javljaju se kao izvor dokaza vezanih za određeno krivično delo. Oni se mogu zateći tokom pripreme izvršenja inkriminisane radnje, na mestu izvršenja krivičnog dela kao i prilikom bekstva i skrivanja počinilaca krivičnih radnji. Široka primena mobilnih uređaja dovela je i do potrebe za njihovom forezikom. Treba napomenuti otežavajuće faktore:

- Česta promenljivost operativnih sistema, standardi za proizvodnju uređaja, tehnologija za skladištenje podataka, procedure zaštite podataka i interfejsa uređaja.
- Raznolikost platforme mobilnih uređaja u kontrastu sa standardizacijom u svetu računara.
- Korišćenje bežične tehnologije za komunikaciju (infrared komunikacija dometa od nekoliko metara, Bluetooth komunikacija sa 20 metara u rasponu i bežična komunikacija sa početnih sto metara) itd (Spalević, Bjelajac, Carić, 2012).

Tokom forenzike mobilnih telefona mogu se naći mnogi digitalni dokazi koji mogu biti interesantni kako u prethodnom tako i u glavnom krivičnom postupku. Zadatak koji se stavlja pred stručnjake iz ove naučne oblasti nije nimalo lak i bezazlen. Kako se pred forenziku stavlja veoma težak zadatak (npr. da poveže počinioca ubistva sa žrtvom preko DNK analize tragova na mestu zločina) tako se i pred digitalnu forenziku stavlja zadatak povezivanja

počinioca krivičnog dela sa digitalnim dokazima. Veoma je važno da se poštuje procedura pribavljanja digitalnih dokaza te njihova obrada i pravilna prezentacija tokom krivičnog ili nekog drugog postupka. Takođe, postupak prilikom izuzimanja zatečenih mobilnih telefona, kao mogući izvor dokaza, sa mesta izvršenja krivičnog dela mora biti zasnovan na pravilnom postupanju i zakonski propisanim procedurama.

Čitav proces digitalne forenzike mobilnih telefona sastoji se od sledećih faza: očuvanje, prikupljanje, ispitivanje, analiza i izveštavanje. Faza očuvanja je prva faza u procesu digitalnog povraćaja podataka i podrazumeva oduzimanje i obezbeđivanje imovine osumnjičenog bez menjanja sadržaja podataka na uređajima. Prikupljanje (akvizicija) je druga faza u kojoj se sakupljaju informacije sa digitalnih uređaja. Ispitivanje i analiza podrazumevaju primenu alata za otkrivanje digitalnih dokaza uključujući i one koji su sakriveni ili menjani. Izveštavanje se oslanja na detaljan pregled svih preduzetih koraka i donetih zaključaka tokom istrage. Prezentuju se rezultati testiranja i ispitivanja i daju objašnjenja do kakvih se zaključaka došlo na osnovu prikupljenih dokaza.

Od svih navedenih faza prve dve se smatraju najvažnijim. Očuvanje i prikupljanje mogu da obezbede ključne dokaze i značajne smernice za nastavak istrage. Svaki korak mora biti sproveden sa izuzetnom pažnjom jer naredne faze ispitivanja u potpunosti zavise od toga koliko dobro su obavljene prve dve. Stoga je proces pronalaženja dokaza počinje u očuvanje i sticanju .

4.1. Osnove tehnologije mobilnih telefona

Tipovi mobilnih uređaja nalaze se u širokom opsegu od onih koji obavljaju niz jednostavnijih funkcija do takozvanih pametih telefona sa mogućnostima sličnim kao i personalni računar. Obzirom da im je osnovna uloga mobilnost, projektovani su da budu kompaktnih dimenzija, sa što dugotrajnijim radom baterije i što manjih težina, udobni za nošenje u ruci.

Veliki broj mobilnih uređaja ima osnovni skup sličnih karakteristika i mogućnosti. Sastoje se od mikroprocesora, *read only* memorije (ROM), *random access* memorije (RAM), radio modula, procesora digitalnog signala, mikrofona i zvučnika, raznih hardverskih priključaka interfejsa i ekrana. Operativni sistem (OS) mobilnog uređaja obično je pohranjen u NAND ili NOR memoriji dok se izvršni kodovi obično pojavljuju u RAM.

Različiti mobilni uređaji imaju različite tehničke i fizičke karakteristike (veličina, težina, brzina procesora, kapacitet memorije). Skoro svi noviji uređaji podrazumevaju globalno pozicioniranje sistema (GPS), kamere a takođe mogu da koriste i različite vrste mogućih proširenja za dodatnu funkcionalnost. Generalno, mobilni uređaji se mogu klasifikovati kao mobilni telefoni koji su namenjeni za, pre svega, jednostavne glasovne i komunikacione poruke ili smart telefoni koji nude napredne mogućnosti i usluge slične onima koje imamo na personalnim računarima.

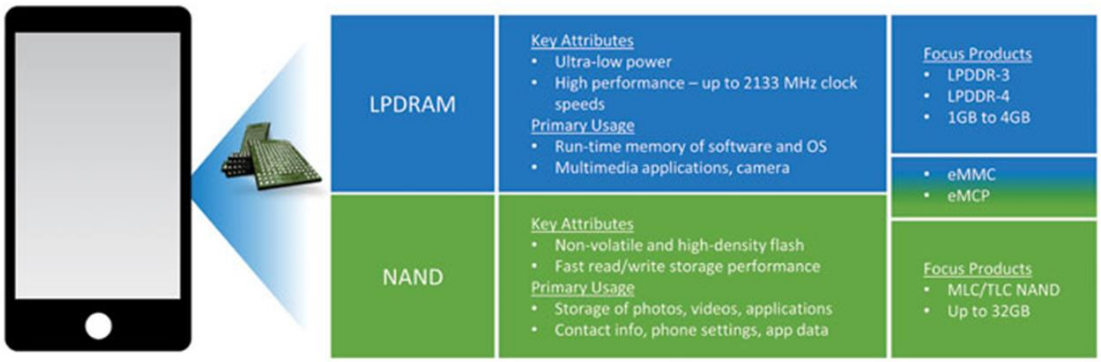
Mobilni uređaji sadrže nepromenljivu i trajnu memoriju. Trajna memorija (t.j. RAM) se koristi za dinamičko skladištenje i njen sadržaj se gubi kada prestane napanje mobilnog

uređaja. Nepromenljiva memorija je konstantnog sadržaja na koji ne utiče prekid napajanja. Mobilni uređaji obično sadrže jednu ili dve vrste nepromenljive fleš memorije. Ovi tipovi su NAND i NOR.

- NAND memorijski čip – pohranjuje podatke ali ne izvršava programe. Karakteriše ga velika brzina rada (često pohranjivanje i povlačenje podataka) i dugotrajnost tako da se upotrebljava u mp3 muzičkim uređajima, digitalnim kamerama i USB „stikovima“ Nudi veći memorijski kapacitet, manje je stabilan, omogućava samo sekvencijalnu pristup i skoro je potpuno otporan na oštećenje datoteka i pokvarene blokove.
- NOR memorijski čip – pohranjuje i izvršava programe. Karakteriše ga brže očitavanje od NAND memorije ali mu treba više vremena za upis i brisanje podataka.

Brzi razvoj mobilnih uređaja pratile su promene memorijskih konfiguracija. Prva generacija mobilnih uređaja sadržala je NOR fleš i RAM memoriju. Sistemski i korisnički podaci su čuvani na NOR i kopirani na RAM zbog bržeg pristupa. Sa pojavom pametnih telefona dodata je NAND fleš memorija. Ova kombinacija NOR, NAND i RAM karakteriše drugu generaciju. Treća generacija, zbog zahteva za većom brzinom transakcije, većom gustinom skladištenja i smanjenja troškova oslanja se samo na NAND i RAM memorije a nedostatak prostora za skladištenje rešava se pomoću Embedded MultiMedia Cards (eMMC) (Ayers, Brothers, Jansen, 2014). Od najnovijih modela pametnih telefona korisnici očekuju mogućnost brzog i udobnog rada sa više aplikacija istovremeno, displeje i multimedijalne sadržaje koje će geldati u Full HD rezoluciji, kamere sa megapikselima, veliki broj aplikacija koje će raditi u pozadini. To postavlja zahteve za izuzetno brzim memorijama, low-power RAM (LPDRAM) ali i za skladištenje u obliku NAND fleš memorije. Na slici 4.1. prikazana je podela memorije pametnih telefona nove generacije sa karaktersitikama.

Pored navedenih, kao vid memorije u mobilnim uređajima može se smatrati i SIM kartica. SIM kartice se sastoje od mikroprocesora, ROM i RAM-a, sa dodeljenim jedinstvenim Integrated Circuit Card Identifier (ICC-ID). ICC-ID sadrži mobilni kod zemlje (MCC), kod mobilne mreže (MNK) i serijski broj kartice. Ove smart kartice se koriste za proveru identiteta korisnika na GSM i UMTS mrežama. SIM kartica sadrži informacije koje se odnose na mrežu i korisnika uključujući i autentikacioni ključ (koji se zove Ki) a potreban je za uspostavljanje veze sa mrežom, jedinstveni matični broj pretplatnika (PIN) za ograničavanje upotrebe SIM kao i telefonski broj pretplatnika Mobile Subscriber ISDN (MSISDN).



Slika 4.1. Memorija pametnih telefona (Williams, 2015)

SIM takođe sadrži identitet međunarodnog mobilnog pretplatnika (IMSI) koji je jedinstveno povezan sa pretplatnikom i sastoji se od koda zemlje, koda mobilne mreže i identifikacionog broj pretplatnika. SIM kartica takođe može sadržati privremeni Mobile Subscriber Identity (TMSI) i Location Area Identity (LAI) uz pomoć koga može da se utvrdi (uz asistenciju operatora) oblast u kojoj se korisnik nalazio u vreme kada je uređaj poslednji put radio (Casey i sur. 2011).

4.2. Rukovanje mobilnim uređajem koji je izvor dokaza

Kao što je već navedeno mobilni telefon kao izvor dokaza, može se pojaviti na više načina: pronađen prilikom vršenja uviđaja mesta izvršenja krivičnog dela, prilikom pretresa lica zatečenih tokom izvršenja krivičnih dela, tokom pretresa prostorija po nalogu istražnog sudije ili na osnovu ovlašćenja policije za pretres. Primera za mogućnost pojave mobilnog telefona kao izvora dokaza je mnogo a samim tim je od velike važnosti da se postupak pronalaženja, pakovanja i obeležavanja, akvizicije podataka i njihovo analiziranje te prezentacija vrše na adekvatan i zakonit način.

Kada je u pitanju mobilni uređaj koji treba analizirati tokom istrage, istražitelj treba pronaći odgovore na važna pitanja:

- Koji je najbolji način da se očuvaju dokazi?
- Kako treba rukovati uređajem?
- Kako pristupiti vrednim ili potencijalno relevantnim podacima koji se nalaze na uređaju? itd.

Uzevši u obzir da su podaci na mobilnim uređajima zapravo potencijalni digitalni dokazi sa svim svojim osobinama (ranjivost, trajnost i sl) i ovde važe opšti principi u rukovanju digitalnim dokazima. To znači da se zapravo forenzički principi koji se odnose na bilo koji digitalni uređaj primenjuju i na mobilne uređaje. Pre svega, svi koraci za prikupljanje podataka trebju biti zabeleženi, moraju podržavati transparentnost i ponavljanja da bi omogućili drugim istražiteljima ponovno prikupljanje podataka koliko god puta bilo potrebno. Treba izračunati i dokumentovati *Hash* dobijenih podataka kako bi se potvrdilo da nije došlo do slučajnih ili namernih izmena. Izuzetno je važno navesti ukoliko je došlo do bilo kakvih

problema, makar i banalnih ili teško objašnjivih. Dokumentacija mora pokazati kontinuitet i kontrolu. Zbog toga je neophodno da se pored zabeleženih detalja o procesu prikupljanja uvek dokumentuju i podaci o transportima, odgovornoj osobi i sl.

Specifičnost mobilnih uređaja je da im je osnovna namena da budu na mreži što može biti izuzetan problem prilikom izuzimanja telefona sa potencijalnim dokazima, stoga je izolacija telefona prvi korak koji je neophodno preduzeti. Mrežna izolacija treba da osigura nepromenljivost sadržaja telefona jer svaki trenutak na mreži otvara prostor za aktivnosti koje mogu dramatično promeniti podatke koji su se nalazili na telefonu. Pored primanja telefonskih poziva i poruka preko aktiviranja daljinskih sistema brisanja do ciljanog menjanja samo pojedinih podataka-prepisivanja postojećih i dodavanja novih.

Postoje tri jednostavna načina za mrežnu izolaciju ali je važno znati da svaki ima određene nedostatke:

- Omogućavanje "Airplane Mode" zahteva interakciju sa mobilnog uređaja koristeći tastaturu, što predstavlja izvestan rizik. Pored toga, može se desiti da na ovaj način sistem nije sprečen da koristi druge usluge, kao što je GPS.
- Isključivanje uređaja može aktivirati neželjene aplikacije, provere identiteta kodova (na primer, UICC PIN i / ili slušalica bezbednosti kod).
- Ostavljajući uključen uređaj ali fizički izolovan skraćuje trajanje baterije a nakon nekog vremena zbog nemogućnosti povezivanja na mrežu može da izazove resetovanje uređaja ili brisanje mrežnih podataka. Faradejevi kontejneri mogu da ublaže radio signal, ali ne nužno da ga u potpunosti eliminišu (Ayers, Brothers, Jansen, 2014).

4.3. Očuvanje dokaza

Očuvanje dokaza uključuje pretragu, detektovanje, dokumentaciju i formiranje baze potencijalnih digitalnih dokaza. Da bi se dokazi mogli uspešno prezentovati na sudu ili bili korišćeni u manje formalnim postupcima moraju biti očuvani. Bilo kakav propust u ovoj fazi mogao bi da ugrozi čitavu istragu i potencijalno izgubi dragocene informacije u vezi konkretnog slučaja. Kako bi očuvanje dokaza bilo uspešno potrebno je voditi računa o:

- proceni i obezbeđenju,
- dokumentovanju,
- izolaciji,
- pakovanju,
- transportu,
- skladištenju i
- trijaži na licu mesta (Ayers, Brothers, Jansen, 2014).

Procena i obezbeđenje se odnosi na pravilno rukovanje uređajem kako se ne bi uništili klasični dokazi tipa otisci prstiju ili tragovi DNK koji bi mogli ukazati na vezu između počinioca i digitalnog dokaza.

Dokumentovanje svih potencijalnih dokaza i komletnog okruženja mora biti detaljno sprovedeno. Svaki podatak iz okruženja može biti izvor vrednih informacija. Dokumentuju se apsolutno svi digitalni uređaji, al i neelektronski materijali (facture, priručnici, kutije…), prostorija/mesto gde se uređaj nalazio. Ukoliko je vidljiva aktivnost na ekranu potrebno je i to dokumentovati.

Izolacija mobilnog uređaja je izuzetno važan korak i neophodno ga je preduzeti što pre. Kao što je već objašnjeno u poglavlju 4.2. pod izolacijom se podrazumeva oneomogućavanje pristupanja sa drugog uređaja ili mreže na uređaj pod istragom. Pored fizičkog odvajanja neophodna je i izolacija od bežičnih merža (WiFi, mobilna, Bluetooth).

Pakovanje, transport i skladištenje. Kada je mobilni uređaj spreman za izuzimanje, forenzički stručnjak treba da zatvori uređaj u odgovarajuću posudu i označi ga na odgovarajući način. Pre transporta i skladištenja treba proveriti i stanje baterije. Svi uređaji trebaju biti u zatvorenim posudama i u sigurnoj zoni sa kontrolisanim pristupom.

Trijaža na licu mesta obuhvata izdvajanje podataka (npr, ručno ili logičko) na licu mesta a odmah zatim i preliminarne analize. Kod uređaja koji podržavaju šifrovanje, ukoliko je moguće, treba uraditi trijažu dok se nalaze u otključanom stanju. Posebno je korisna u identifikaciji medija koji najverovatnije sadrže dokaze i u slučajevima kada je neophodna hitna istraga. Na slici 4.2 dat je algoritam opšteg slučaja. Ovaj algoritam predstavlja polaznu tačku sa smernicama aktivnosti koje su usaglašene sa postojećim pravilima i procedurama.

Slika 4.2. Algoritam trijaže na licu mesta (Ayers, Brothers, Jansen, 2014)

5. EKSTRAKCIJA PODATAKA

Pojam dokaza nije definisan u zakonskim aktima već se koristi kao poznat pojam. Pojam digitalnog dokaza prema National Institue of Justice-NIJ (Electronic Crime Scene Investigation, 2008) definisan je kao informacija i podatak od značaja za istragu, koji je uskladišten, primljen ili poslat preko elektronskog uređaja. Druga definicija predložena od strane Scientific Working Group on Digital Evidence SWGDE (2009) kaže da je digitalni dokaz svaka informacija koja ima dokazujuću vrednost koja je uskladištena ili se prenosi u digitalnom obliku. Zaključak je da digitalni dokaz može biti svaka informacija koja je generisana, obrađivana, uskladištena ili prenesena u digitalnom obliku, koju sud može smatrati merodavnom, tj. Svaka binarna informacija, sastavljena od digitalnih 0 i 1, uskladištena ili prenesena u digitalnoj formi, kao i druge moguće kopije orginalne digitalne informacije koje imaju dokazujuću vrednost i na koje se sud može osloniti, u kontekstu forenzičke akvizicije, analize i prezentacije (Petrović, 2010).

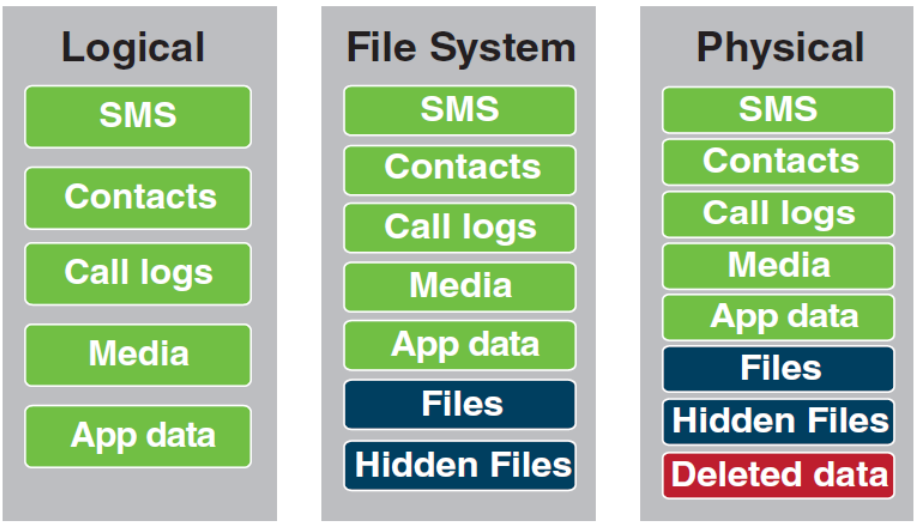
Uopšteno posmatrano postoje tri vrste dokaza (Littlejohn, 2002):

- Fizički dokaz (ponekad se naziva pravi dokaz). Sastoji se od opipljivih objekata koji se mogu videti i dodirnuti.
- Iskaz kao direktni dokaz. Izjava svedoka bazirana na ličnom iskustvu.
- Posredni dokaz. Nije baziran na ličnim zapažanjima već na opservacijama i poznavanju činjenica.
- Prilikom istrage u koju su uključeni i digitalni dokazi prema SWGDE/IOCE standardu postoje naredne tri vrste (Littlejohn, 2002):
- Digitalni dokaz - informacija od značaja za krivični postupak koja se nalazi ili prenosi u digitalnom obliku.
- Fizički dokaz - fizički medijum na koji je uskladištena digitalna informacija ili koji služi za njen prenos.
- Podaci o fizičkom dokazu - informacije od značaja za krivični postupak povezane sa fizičkim dokazom.

Digitalni dokaz je potreban ali ne i dovoljan uslov za građenje slučaja. Ovakvi dokazi su krhke prirode i lako mogu biti modifikovani, uništeni i izgubljeni. Upravo zbog njihove prirode nije dovoljno samo postojanje dokaza koji je rezultat forenzičkog alata i primenjenih forenzičkih tehnika već njhovo prihvatanje na sudu zahteva ispunjavanje određenih uslova. Dokazi se moraju međusobno dopunjavati i ne smeju imati takozvane pukotine za donošenje zaključaka odnosno za utvrđivanje čvrstog digitalnog dokaza. Validni digitalni dokaz treba da potkrepi dokaze iznete u sudnici, da dokaže krivicu ili oslobodi osumnjičenog. Mora biti pouzdan i doprinositi istrazi. Pošto je digitalni dokaz rezultat alata i metoda koje je odabrao i primenio digitalni forenzičar može se tvrditi da upravo od njegove stručnosti i dobrog izbora alata zavisi konačan ishod (Kaurin i Anucojić, 2012).

5.1. Ekstrakcija podataka primenom Cellebrite UFED Touch

Cellebrite ufed touch ultimate je potpuno opremljen mobilni forenzički alat koji omogućava brzu i jednostavnu ekstrakciju podataka sa više od 8.000 mobilnih uređaja. Broj nije konačan jer lista podržanih uređaja konstantno raste (može se naći na sajtu kompanije cellebrite). Uređaj je hardverski nezavistan sa instaliranim ufed softverom na microsfot windows platformi i podržava dva različita metoda ekstrakcije podataka: logički i fizički. Na slici 5.1. Se vidi da je ponuđen i treći tip “file system” ekstrakcija koji zapravo tehnički pripada logičkom. Ukoliko se uređaj koji želimo istražiti nalazi na listi podržanih mogu se dobiti podaci iz navedenih kategorija. Izborom uređaja sa liste podržanih odmah možemo videti koji su tipovi ekstrakcije mogući te, samim tim, koje vrste podataka možemo dobiti.



Slika 5.1. Tipovi ekstrakcije (Cellebrite, n.d)

Telefon nad kojim je izvršena fizička ekstrakcija podataka je alcatel_6033x one touch idol. Pre početka rada važno je proveriti da li je izvršena izolacija od internet pristupa. Ukoliko se podaci pohranjuju na pc takođe je važno da i on bude izolovan. Ne radi se ni bilo kakav update softvera dok su uređaj nad kojim se vrši istraga ili disk na kome se pohranjuju podaci priključeni. Podaci se pohranjuju isključivo na unapred pripremljenom i predviđenom medijumu (flash drive, eksterni hard disk, interni hard disk ili particija na pc itd). Uz ufed touch dolazi komplet potrebnih kablova za priključivanje svih vrsta podržanih telefona a softver je intuitivan i nudi podršku u vidu detaljnih instrukcija za svaki od koraka. U većini slučajeva, mobilni telefoni se na ufed uređaj povezuju preko kabla sa usb priključkom. Nakon uključivanja UFED-a a pre priključivanja mobilnog uređaja treba izabrati koji je proizvođač a zatim i model telefona. Ponuđena je i opcija automatskog detektovanja. Ekran na UFED-u je Touch screen sa mogućnošću podešavanja ugla pozicije ekrana a kretanje kroz aplikaciju moguće je rukom ili stylus-om. Nakon izbora konkretnog modela telefona na ekranu se pojavljuje fotografija modela sa tipovima ekstrakcija koje je moguće pokrenuti. Izborom tipa ekstrakcije dolazimo do ekrana na kome vršimo izbor lokacije na koju ćemo pohraniti podatke. Možemo birati između PC-a ili eksternog hard diska. Naredni korak se može razlikovati u zavisnosti od odabranog tipa ekstrakcije. Ukoliko je logička u pitanju onda sa ponuđene liste podataka koji se mogu ekstrakovati možemo birati koje želimo. Na ovaj način moguće je skratiti verme ekstrakcije ukoliko ciljano suzimo listu. Kod fizičke ekstrakcije ova opcija nije moguća već se izborom na ovaj tip odmah prelazi na korak u kome trebamo prvo priključiti uređaj na USB port sa leve strane (source). S obzirom da uz UFED dobijamo niz različitih kablova, na ekranu dobijamo jasnu instrukciju koji tip kabla koristimo u konkretnom slučaju.

Pre nego priključimo telefon imamo tri važna koraka za koje takođe imamo detaljne instrukcije:

1. Omogućavanje *Developer options*.
2. Omogućavanje *Stay awake* i *USB debugging* moda.

3. Potvrdu *Screen lock* moda.

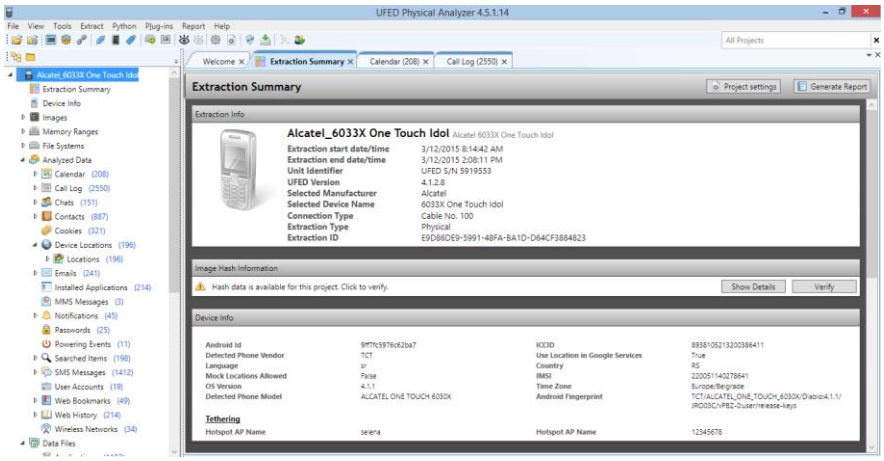
Ulazimo u fazu kada sa desne strane UFED-a na (target) USB priključak konektujemo eksterni hard disk / PC. Pre početka ekstrakcije važno je napomenuti da je potrebno da je baterija 100% puna.
Kao što se vidi i na slici 5.1. fizička ekstrakcija omogućava najobuhvatniju analizu. Prilikom ove ekstrakcije pristupa se i „allocated“[50] i „unallocated“[51] prostoru.
Ovi slojevi uključuju tri različite grupe sadržaja:

- "Logički" sadržaj nedostupan kroz API[52]. (Npr.kod pametnih telefona funkcije i dnevnik poziva).
- Obrisan sadržaj.
- Sadržaj koji telefon prikuplja bez ikakve voljne akcije korisnika ponekad i bez njegovog znanja. (Na primer: WiFi mreže, GPS lokacije, veb istoriju, e-mail zaglavlja, EXIF podatke o slikama kao i podatke o sistemu.

Uobičajeni metod koji se koristi za fizičku ekstrakciju je preko „rescue mode“ ili „download mode“. Radeći u ovom režimu mobilni telefoni omogućavaju umetanje malog dela koda (boot loader) u RAM tokom pokretanja. Tokom početne faze pokretanje uređaja UFED šalje boot loader RAM memoriji telefona. Pokreće se boot loader i vrši čitanje (read only) podataka sa mobilnog telefona bez ostavljanja tragova. Za većinu uređaja, na ovaj način se mogu zaobići svi sigurnosni mehanizmi, čak i ako je uređaj zaključan. Pošto boot loader sadrži samo kod za čitanje različitih memorijskih čipova i ništa ne zapisuje, u bilo kom trenutku tokom, ili nakon, procesa ekstrakcije svi podaci su nepromenjeni i forenzički ispravni. Dešava se da noviji uređaji, nemaju ugrađenu funkcionalnost za upload boot loader-a te se, u tim slučajevima, mora privremeno rutovati telefon. Tokom ovog procesa, Cellebrite klijent se postavlja na uređaj kako bi ga privremeno rutovao i omogućio sakupljanje podataka. Nakon ekstrakcije, klijent se deinstalira i uređaj se vraća u prvobitno stanje.

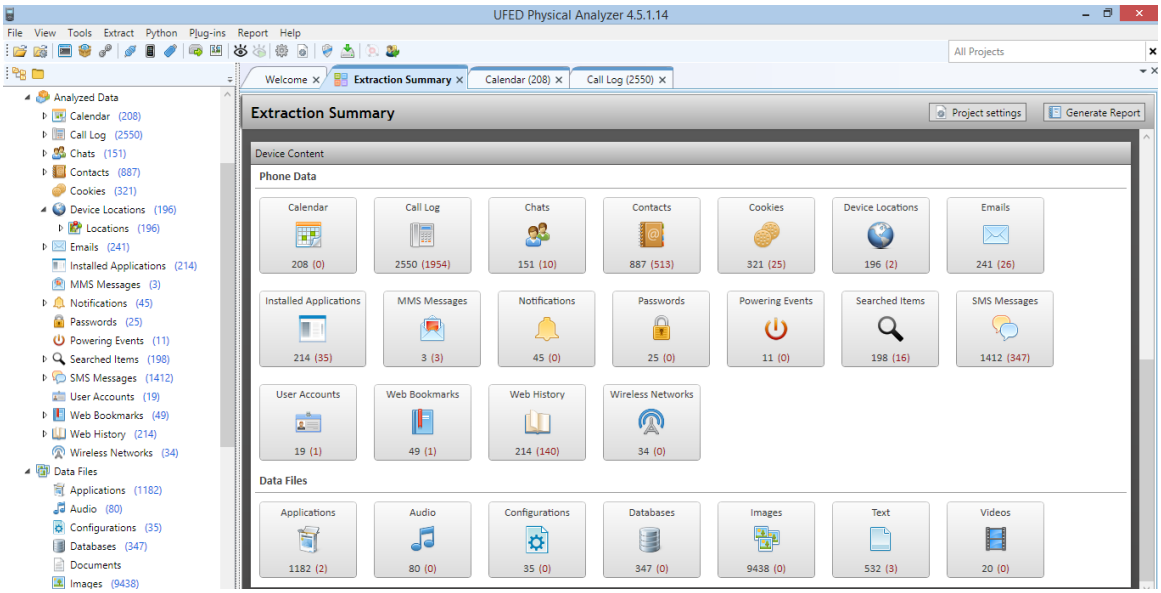
[50] Allocated – deo memorije u koji se organizovano smeštaju podaci. Sadrži OS i korisničke podatke.
[51] Unallocated – deo memorije van definisanog sistema datoteka koji je takođe dostupan za zapisivanje podataka. Tu se mogu nalaziti izbrisani podaci i fragmenti.
[52] API - Interfejs za programiranje aplikacija . Određuje kako aplikacije i firmver na mobilnom uređaju treba da interaguju jedan s drugim.

Na slici 5.2. dat je izgled ekrana odmah nakon iščitavanja podataka. Uočljivo je da je moguće pročitati informacije o ekstrakciji, kao što su: koji je UFED je korišćen (uključujući i serijski broj), vreme početka i završetka, datum i hash informacije.



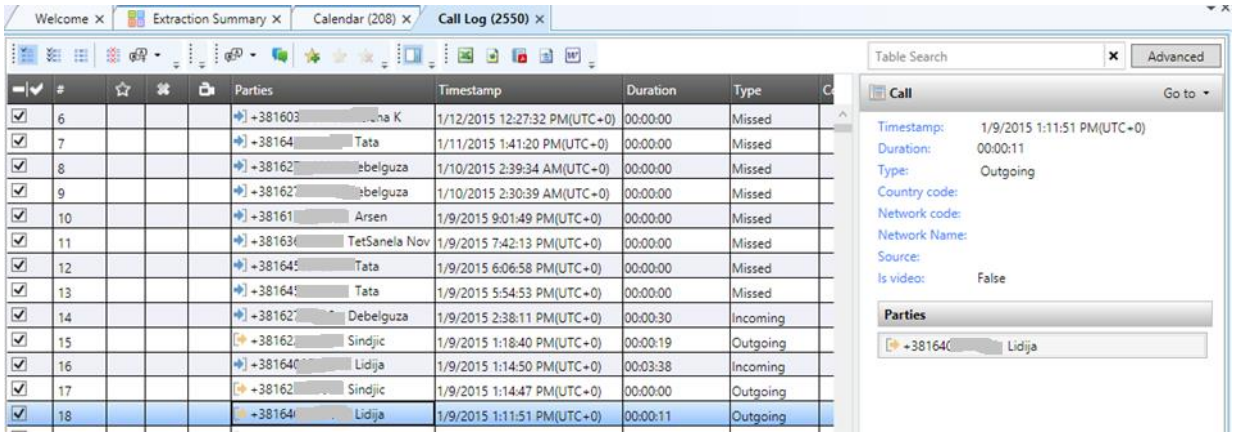
Slika 5.2. Ufd fajl (autorsko delo)

Grananje na levoj strani pokazuje koje vrste podataka i u kojoj količini su sakupljene. Izborom extraction summary (slika 5.3) u desnom prozoru se dobijaju preglednije sređene iščitane grupe podataka sa informacijom koliko izbrisanih podataka po kategoriji je povraćeno što prikazuje crveni broj u zagradi (npr. Memorisano 887 kontakta a obrisanih 513).



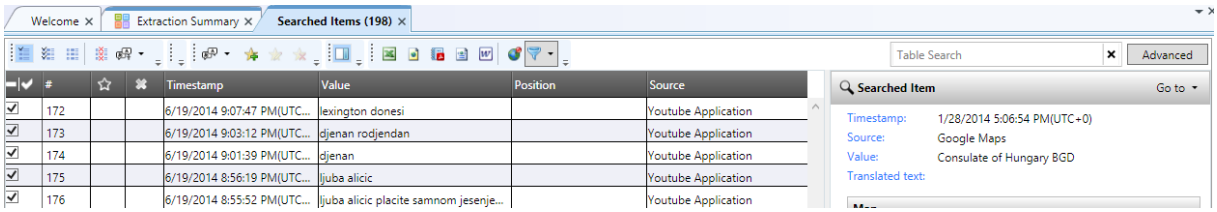
Slika 5.3. Extraction Summary (autorsko delo)

Ukoliko je potrebno pogledati istoriju poziva bira se opcija call log (slika 5.4). Tabelarno sređeni podaci daju sve neophodne informacije o pozivima uključujući i obrisane.



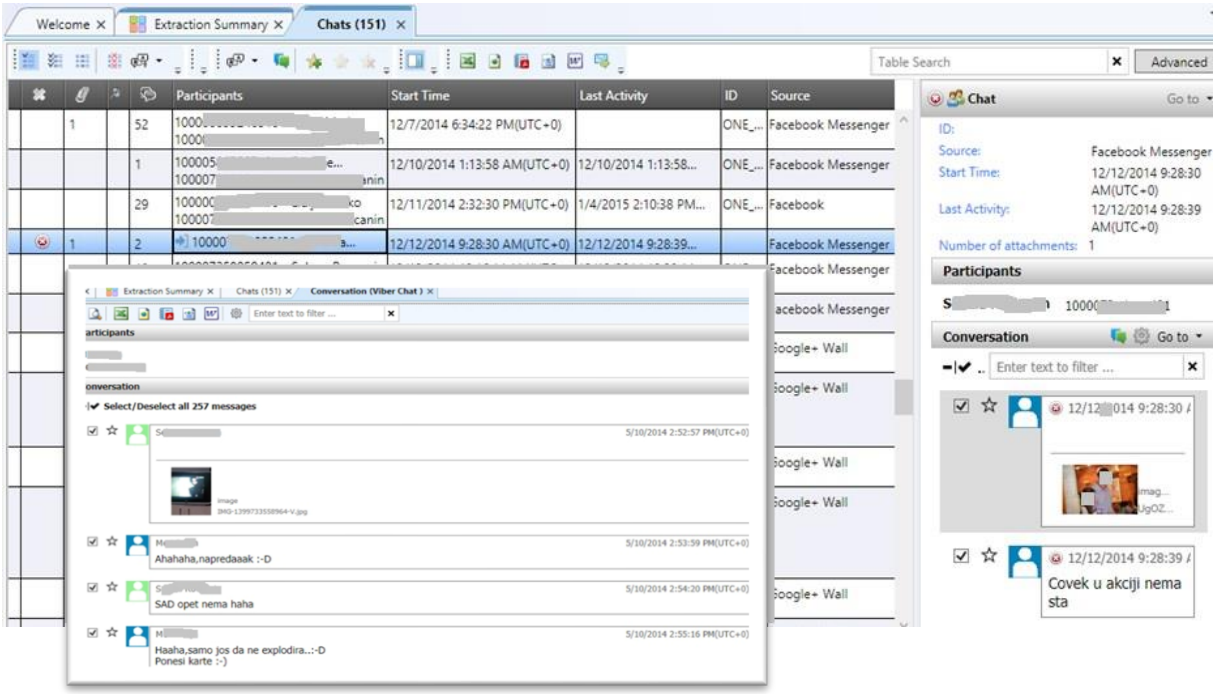
Slika 5.4. Call Log (autorsko delo)

U velikom broju istraga značajni su podaci o pretragama koje su vršene sa izuzetog uređaja. Ključne reči pretrage kao i vremenske odrednice mogu pokazati nameru o izvršenju kao i koliko je dugo planirano i na koji način. Primer ekrana sa iščitanim ineternet pretragama dat je na slici 5.5. Čest je slučaj da ključne reči pretrage pomognu u istrazi ukazujući i na aktivnosti koje još nisu otkrivene (informacije o iznajmljivanju dodatnog prevoznog sredstva, nabavka otrova, planiranje odlaska na neku destinaciju…).



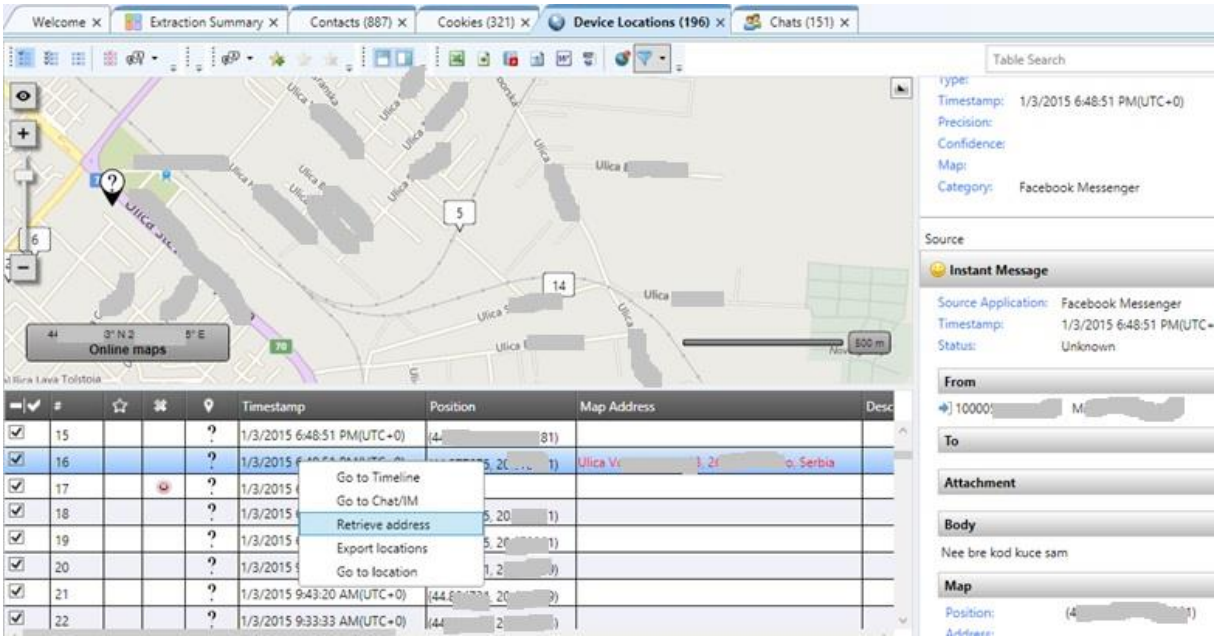
Slika 5.5. Searched Items (autorsko delo)

Tekstualne i chat poruke su generalno važan izvor informacija a od posebnog su značaja kada se prate organiziovane kriminalne grupe. Na slici 5.6. uočljivo je da je moguće hronološki ispratiti komunikaciju između učesnika. Dat je primer iščitane komunikacije koju je vlasnik izbrisao sa telefona i mogu se videti svi podaci: sadržaj, servis koji je korišćen, vremenski parametri, čak i attachment (u ovom slučaju fotografija).



Slika 5.6. Chats (autorsko delo)

Pored ispraćene komunikacije, na slici 5.7. se može videti da postoje tragovi i o lokaciji osoba koje su komunicirale. U padajućem meniju nalaze se opcije koje omogućavaju direktan pregled Timeline aktivnosti učesnika kao i uvid u chat. To znači da ukoliko imamo sumnjive učesnike chata postoji mogućnost da u samom telefonu imamo trag o lokaciji sa koje su razgovarali, možemo hronološki pregledati samu komunikaciju kao i vremenski uređene aktivnosti korisnika. Iz drugog ugla posmatrano, ukoliko imamo lokacije koje su sumnjive možemo preko njih potencijalno doći do učesnika koji su se nalazi tu ili u okolini. Pretraga podataka, relevantna komunikacija ili učesnici, moguća je i ukucavanjem željenog pojma u Watch list (npr. droga, beli prah i sl).



Slika 5.7. Device Locations (autorsko delo)

Prilikom rešavanja slučajeva organizovanog kriminala neophodno je povezati komunikacione kanale kako bi došli do hijerarhijske podele članova grupe. To je proces koji, ukoliko se radi tradicionalnim načinima – bez upotrebe računara, može biti dugotrajan jer uključuje analiziranje velikog broja raznovrsnih podataka. Do ovog tipa rezultata može se doći pokretanjem Link Analysis modula koji može povezati i do 100 ekstrakcija sa različitih mobilnih uređaja. Na ovaj način, analizom i povezivanjem podataka iz aplikacija (FaceBook, Instagram, Twiter…), lokacija, slika, video, audio, poziva, SMS, MMS, e-mail poruka i zajedničkih kontakata dolazi se do identifikacije odnosa između članova grupe i osumnjičenih i žrtava.

Na kraju, u skladu sa specifičnim potrebama moguće je generisati izveštaj u različitim formatima:

- HTML format za pregled rezultata na bilo kom brauzeru.
- PDF format sigurniji jer je složen za menjanje podataka i msword format ukoliko je potrebna editabilnost.
- Microsoft Excel spreadsheet podataka i XML izveštaj, zgodan za otvoranje iz drugih forenzičkih i analitičkih alata. Odličan kada nam je potrebna tabelarna preglednost i upoređivanje podataka.
- EML izveštaj je moguće otvoriti sa klijentima e-pošte.
- KML izveštaj koji se otvara u google maps ili google earth radi lakše vizuelizacije location- based podataka.

6. ZAKLJUČAK

Moderna borba sa organizovanim kriminalnim grupama podrazumeva drugačiji pristup od onog koji je tradicionalan za većinu klasičnih zločina. Evolucija ljudskog ponašanja kao rezultat tehnoloških inovacija stvorila je jedinstvene mogućnosti za kriminal i zloupotrebe. U protekle tri decenije, konstantni porast novih uređaja i aplikacija, za posledicu je imao modifikaciju tradicionalnih oblika kriminalnih aktivnosti ali i formiranje potpuno novih. Ovo se posebno odrazilo na organizovani kriminal jer je rušeći granice i olakšavajući komunikaciju, bez obzira na fizičku lokaciju, internet zapravo omogućio članovima organizovanih krimnalnih grupa virtuelno prisustvo na bilo kom mestu u svetu. Za razliku od off-line sveta gde je potrebno fizički biti prisutan na mestu zločina i gde je moguće počiniti jedan zločin u jednom trenutku sajber prostor je omogućio organizaciju i napade na veliki broj žrtava, istovremeno na velikom broju različitih lokacija i to bez značajnog rizika i napora za skrivanjem identiteta. U radu je, na primeru ekstrakcije podataka Cellebrite UFED Touch forenzičkim alatom, pokazano koliko se značajnih činjenica - potencijalnih dokaza može sakupiti sa jednog mobilnog uređaja. Mobilni uređaji su odabrani za analizu zbog svoje sveprisutnosti i individualnosti u upotrebi te su kao osnovno komunikaciono sredstvo prepoznati kao izuzetno važni organizovanim kriminalnim grupama. Na osnovu ekstrakovanih podataka ukazano je na mogućnost njihove primene u istragama gde se mogu pored direktnih dokaza obezbediti i značajne dodatne informacije koje mogu pomoći u istrazi.

LITERATURA

Alharbi, S. Weber-Jahnke, J., Traore, I. (2011). The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review. *International Journal of Security and Its Applications, Vol. 5 No. 4*, pp. 59-72.

Ayers, R. Brothers, S. Jansen, W. (2014). Guidelines on Mobile Device Forensics, *NIST Special Publication 800-101, Revision 1*.

Casey, E. (2011). *Digital Evidence and Computer Crime. Forensic Science, Computers, and the Internet, third Edition*. Elsevier Academic Press.

Grubač, M. (2002). Krivično procesno pravo, Posebni deo

Kaurin, T. Anucojic, D. (2012). Smernice za izbor alata digitalne forenzike, *Infoteh-Jahorina.* Paper presented at the 2012 Infoteh-Jahorina.

Kim-K. Choo, R. (2008). Organised crime groups in cyberspace: a typology, *Trends in Organized Crime, 11*, pp. 270.

Littlejohn Shinder, D. (2002). *Scene of the Cybercrime:Computer Forensics Handbook*, Waltham: Syngress.

Milošević, M. (2003). Organizovani kriminal, Službeni list SCG. pp. 65.

Orebaugh, A. (2006). Proactive forensics. *Journal of Digital Forensic Practice, vol. 1*, pp. 37.

Palmer, G. (2001). *A road map for digital forensics research-report from the first Digital Forensics Research Workshop (DFRWS).* Utica, New York: DFRWS.

Petrović, L. (2010). Digitalni dokazi. Paper presented at *Ziteh`04*. Retrieved January 25, 2016, from: http://www.singipedia.com/content/986-Digitalni-dokazi

Scientific Working Group on Digital Evidence (SWGDE) International Organization on Digital Evidence (IOCE). (2000). *Digital Evidence: Standards and Principles*, 2000 [Data file]. Available at http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/

Skakavac, Z. (2007). Krivičnoprocesna regulacija posebnih istražnih tehnika u zakonodavstvu Srbije i Makedonije – sličnosti i razlike, *Makedonska revija za kazneno pravo i kriminologiju,* Međunarodni naučni skup – 8. godišnje savetovanje na temu „10 godina primene ZKP Republike Makedonije“, Ohrid 2007. godine;
Skakavac, Z. Kaurin, T. (2012). Digitalna forenzika i digitalni dokazi - protiv organizovanog kriminaliteta, *VI naučni skup Dani bezbjednosti*, Banja Luka.
Spalević, Ž. Bjelajac, Ž. Carić, M. (2012). The importance and the role of forensics of mobil, *Facta Universitatis, 25*, pp. 121 – 136.
Škulić, M. (2003). Organizovani kriminalitet, *Dosije*, 248-250.
Vuković, I. (2013). Digitalna forenzika mobilnih uređaja za potrebe krivičnog postupka, *Telekomunikacije 8*. http://www.telekomunikacije.rs/archive/eighth_issue/mr_ igor_ vukovic:_digitalna_forenzika_mobilnih_telefona_za_potrebe_krivicnog_postupka.428.html (06.02.2016)
Williams, T. (2015). Next Generation of Memory to Emerge from Smartphones, *RTC magazine*, http://rtcmagazine.com/articles/view/120988 (12.02.2016.)
Zatyko, K. (2007). Commentary: Defining Digital Forensics. http://www.forensicmag.com/articles/2007/01/commentary-defining-digital-forensics (30.01.2016.)
Cellebrite touch http://www.cellebrite.com/Pages/mobile-forensics-white-papers (12. 02. 2016.)
Exploring tomorrow's organised crime, https://www.europol.europa.eu/sites/default/ files/edi/EuropolReportDigitalCove.html (10. 02. 2016.)

Tanja Kaurin
Zdravko Skakavac

THE IMPORTANCE OF DIGITAL FORENSICS OF MOBILE DEVICES IN DETECTING AND INVESTIGATING CRIMINAL ACTS OF ORGANIZED CRIME

Summary

The digital age has radically changed every aspect of our everyday lives, bringing with it new global threats. Surmounting physical limits, the Internet has offered invaluable opportunities to the state as well as individuals, but also its inevitable vulnerabilities. Exploiting the speed, convenience and anonymity of the Internet, criminal networks have facilitated coordination among its members, regardless of their physical location. This has created an opportunity for the execution of a wide range of crimes that know no boundaries, whether physical or virtual, thus dramatically reducing the time required for the organization and execution of complex criminal activities. Organized crime favours the cyber environment, which assumed serious proportions long ago, both in phenomenological aspects and in terms of serious consequences; however, mobility brought the complexity of security situation to the new level. The aim of this essay is to point out the significance of digital forensics in detecting criminal acts of organized crime regardless of whether they belong to the classical criminal activity or those within the scope of cyber crime. For this reason, the emphasis is placed on digital forensics, mobile devices, primarily due to their omnipresence but also due to the individuality of their use. In addition to clarification of digital forensic evidences collected by using mobile devices forensic methods and tools, the essay also presents a practical example of data acquisition using the Cellebrite UFED Analyzer.

Key words: *digital forensics, cyber crime, mobile forensics, organized crime.*

PREGLEDNI ZNANSTVENI RAD

Ksenija Butorac[53]
Irena Cajner Mraović[54]
Hrvoje Filipović[55]

UČINKOVITOST VIDEONADZORA U SMANJENJU KRIMINALITETA – PREGLED ISTRAŽIVANJA

Sažetak

Policija se u svakodnevnom radu koristi brojnim metodama, alatima i strategijama ovisno o specifičnom području svog djelovanja. Neki od primjera tehnološkog aspekta rada policije odnose se na korištenje biciklističke ophodnje, vodenih topova, nadzornih kamera, mobilnih alarma u slučaju obiteljskog nasilja, prisluškivanje sumnjivih kriminalnih skupina i drugo. Stoga su policijska istraživanja usmjerena na proučavanje utjecaja društvenih i tehnoloških promjena, odnosno procesa modernizacije na policijsko djelovanje. Neka od njih bave se implementacijom novih vrsta informacija i komunikacijske tehnologije na svim ustrojstvenim razinama te načinom na koji utječu na policijsku kulturu i praksu. Druga se fokusiraju na tehnologije kontrole poput uporabe nadzornih kamera i drugih sustava nadziranja. U tom smislu fokus istraživanja odnosi se na ispitivanje učestalosti i premještanja kriminaliteta, uspješnost otkrivanja kaznenih djela te na druge pozitivne ili negativne efekte proizašle iz korištenja sustava videonadzora. Većina studija upućuje na činjenicu kako videonadzor ovisi o tome gdje je lociran i o vrsti kaznenih djela. Učinci su najizraženiji kad je riječ o kaznenim djelima koja se prethodno planiraju i pripremaju te u područjima gdje se uz videonadzor koriste i dopunske preventivne mjere (npr. pojačana javna rasvjeta). Međutim, kod kaznenih djela s elementima nasilja ne bilježi se njihovo smanjenje, a u malom broju pozitivnih primjera nije ustanovljena statistička značajnost.

Ključne riječi: *videonadzor, kontrola, kriminalitet, istraživanje, učinkovitost.*

1. UVOD

Zamisao o "svepromatrajućem" mehanizmu kao izumu nastala je još u 18. stoljeću kad je britanski filozof i društveni teoretičar Jeremy Bentham (1746.-1832.) osmislio penalnu instituciju (*panopticon*) koja je čuvarima u središnjem tornju kaznionice omogućavala promatranje zatvorenika bez mogućnosti da saznaju tko ih i kada nadzire (prema: Leman-Langlois, 2002). Glavni učinak tzv. panoptizma očituje se u činjenici da se kod ljudi stvara svjesno i realno stanje vidljivosti pojedinca kojom se osigurava automatsko funkcioniranje

[53] Izv.prof.dr.sc. Ksenija Butorac, Visoka policijska škola, MUP RH, e-mail: kbutorac@fkz.hr
[54] Izv.prof.dr.sc. Irena Cajner Mraović, Hrvatski studiji Sveučilišta u Zagrebu, e-mail: icajner@hrstud.hr
[55] Hrvoje Filipović, viši predavač, Visoka policijska škola, MUP RH, e-mail: hfilipovic@fkz.hr

moći koja je u rukama nekog drugog subjekta. U prošlosti je panopticon bio polivalentan u svojoj primjeni. Služio je prilikom izdržavanja kazne zatvorenika, u ustanovama za liječenje duševnih bolesnika i obrazovanje učenika, za nadgledanje radnika i drugo. U svojoj knjizi Nadzor i kazna Foucault (1975; prema Norris, 2003) navodi kako je arhitektonska izvedba stoljećima bila u funkciji moći. Objašnjava kako je posrijedi mikrofizika moći koju u život uvode aparati i institucije. Autor, zapravo, objašnjava odnos socijalnih struktura, institucija i pojedinaca, a u tom kontekstu analizira provođenje državne ili društvene moći. Ona se prakticira kroz discipliniranje građana korištenjem sveobuhvatnog režima nadzora i provođenjem zakona, što potanko analizira Vijver (1998, 6-17). U suvremeno doba panoptizacija predstavlja načelo nove "političke anatomije" koja nastoji kontrolirati volju tijela pojedinca. U tom pogledu danas se koristi suvremena tehnologija nadzora građana zbog rizičnog društva u kojem živimo (Gold, 2004; Coleman, 2004; Ericson i Haggerty, 1997).

Trend politike suzbijanja kriminaliteta i suvremeni koncept nadzora nad građanima utemeljen je na generalnoj pretpostavci da će se ljudi ponašati poštenije i društveno poželjno, ako ih netko promatra (Cvitanović, 2010, 2). Radi se o složenim i manje vidljivim oblicima nadzora koji nadmašuju funkciju preventivnog utjecaja i normalizirajućeg modela društvene kontrole, a očituju se u aktivnim tehnikama nadzora koje nadilaze standardnu "fizičku moć" provođenja zakona. Nekadašnji oblici panoptizacije u suvremenom dobu provode se virtualnim tehnologijama i tehnikama koje na pojedinca utječu prisilno, ustrajno i opetovano s nakanom da mu na taj način usade društveno poželjni stav, ideju ili ponašanje. U ovom kontekstu najbolji se rezultati postižu kad objekt nadzora toga nije svjestan ili kad se autonomno ponašanje uvjetuje ili regulira videotehnikama ili audiotehnikama.

Funkcionalna snaga situacijske prevencije kriminaliteta podrazumijeva upravljanje situacijom, tek potom ima funkciju kažnjavanja. Retributivni element kazne je u pozadini s obzirom na to da su sustavu nadziranja, izvanjski i površno gledano, svojstvene atribucije humanog odnosa, suzdržanosti i nevidljivosti. Ovako ponuđeni model kao novi oblik moći djeluje prirodno, a adresat ga ne osjeća nametnutim, štoviše čini se kao njegov slobodan izbor. Moć discipliniranja pomoću sustava nadzora pojedinca ili mase razvija se i postaje integrirani sustav upravljanja koji u realnosti može pokriti željeno područje i funkcionirati u tajnosti.

Trend globalizacije sveprisutnog nadzora, zahvaljujući tehnološkom razvoju u suvremenom svijetu, utemeljen je uglavnom na globalizaciji sustava vrijednosti. Širenje ove tehnologije osigurava se postupnim, neinvazivnim psihološkim pripremama i osvještavanjem građana najčešće medijskim putem, i to promicanjem važnih društvenih pravila i sustava poželjnog, odnosno prihvatljivog ponašanja. U tom smislu potrebno je uvjeriti ljude da nadzor služi ostvarivanju njihove slobode, sigurnosti i, konačno, njihove egzistencije ("sloboda u zamjenu za sigurnost"). S tehničkog i ekonomskog gledišta može se zaključiti da je današnja tehnologija nadzora postala isplativ i socijalno prihvatljiv instrument socijalnog inženjeringa kao globalnog instrumenta prevencije.

Slijedom navedenog cilj je ovog rada da se na temelju rezultata znanstveno relevantnih istraživanja u posljednja dva desetljeća analiziraju i problematiziraju neka od najvažnijih pitanja tehnologija videonadzora:

- Pridonosi li videonadzor i u kojoj mjeri situacijskoj prevenciji kriminaliteta?

- Smanjuju li sustavi videonadzora razinu kriminaliteta i drugih antisocijalnih ponašanja?
- Postoji li premještanje kriminaliteta u druga područja koja nisu pokrivena videonadzorom?
- Pomaže li videonadzor u otkrivanju i razjašnjavanju kaznenih djela?
- Postoje li pozitivni i/ili negativni (neželjeni) efekti videonadzora?

2. MOGUĆNOSTI, PREDNOSTI I SLABOSTI VIDEONADZORA

Videonadzor je tehnika nadziranja usmjerena na prevenciju kažnjivih ponašanja s ciljem povećanja percipiranog rizika za počinjenje kaznenog djela kod potencijalnog počinitelja (Usher, 2003a). Glavna je svrha videonadzora odvraćanje potencijalnih počinitelja od činjenja kažnjivih radnji na određenom prostoru pod uvjetom da su svjesni postojanja tog nadzora. U slučajevima kad se postojanje kamera javno obznani, potencijalni počinitelji, u pravilu, percipiraju i procjenjuju situacije u kojima povećani rizik uhićenja nadmašuje moguću korist od kaznenog djela te najčešće odustaju od svoje prvotne nakane. Stoga se važna dimenzija kriminalističke prevencije ogleda upravo u percepciji počinitelja koja potiče ili producira samodisciplinu, odnosno kontrolu vlastitog ponašanja u zadanim okolnostima. Videonadzor omogućuje svojevrsnu trijažu koja rezultira efikasnim planiranjem i, ovisno o procjeni, svrhovitim angažiranjem i rasporedom policijskih snaga na temelju praćenja događaja u realnom vremenu.

Videonadzor čini televizija zatvorenog kruga kao generički pojam (eng. CCTV), a riječ je o uporabi videokamera za prenošenje videosignala na središnje kontrolno računalo kako bi se dobivene snimke pratile u realnom vremenu ili pohranile za naknadni pregled i analizu (Gold, 2004, 12). Videosnimke se mogu izdvojiti s odabrane kamere, mogu se rotirati ili izmjenjivati s više kamera istodobno, a korištenjem digitalne tehnologije one se mogu istodobno prikazati omogućujući šire vidno polje (smanjujući slijepe točke) u sustavu videonadzora i značajno bolju čistoću slike u odnosu na konvencionalne kamere (Ratcliffe, 2006). S obzirom na uključenost ljudskog faktora u videonadzor, ovi sustavi mogu biti *pasivni* (pretraživanje snimaka *post festum*) i *aktivni* (praćenje prikaza i fokusiranje zaposlenika u realnom vremenu na određene slike). Prema tome, pohrana snimaka omogućuje kasniju analizu kriminalnog događaja što predstavlja dodanu vrijednost i olakšava konvencionalno kriminalističko istraživanje te na stanoviti način inhibira kriminalnu volju počinitelja za daljnjom kriminalnom aktivnošću počinitelja na istoj lokaciji. S druge strane, identifikacijom i uhićenjem počinitelja te njegovim kažnjavanjem postiže se specijalna prevencija kriminaliteta (zatvorska kazna, uvjetna osuda sa zaštitnim nadzorom i sl.) i na taj način onemogućava kontinuitet i ustrajnost u njegovom kriminalnom djelovanju.

U praksi su sustavi videonadzora najčešće hibridni. Koriste se vidljive i skrivene kamere koje se postavljaju u zaštitne školjke ili kupole. Prisutnost potonjih je teže otkriti ili je nemoguće utvrditi smjer pokrivanja određenog područja sa svrhom odvraćanja potencijalnih počinitelja od kažnjivih radnji u zadanom prostoru (Leman-Langlois, 2002). Važno je napomenuti kako je, u svakom slučaju, neizostavan rad operatera koji nadzire stanje u

prostoru, obavlja pregled snimaka, reagira na uočene informacije izvještavajući policiju te, u konačnici, priprema videozapis počinjenih prekršaja i kaznenih djela kao dokaz na sudu. Operater je najčešće policijski službenik ili zaštitar. Danas postoje napredni sustavi koji omogućuju aktiviranje kamera pomoću senzora za pokret, infracrveno svjetlo koje povećava kvalitetu snimke noću, mogućnost manipulacije smjera i fokusa kamere, procjenu lokacije incidenta izazvanog vatrenim oružjem, tehnologiju prepoznavanja lica sumnjive osobe, ako je program povezan s policijskom računalnom bazom fotografija otprije poznatih počinitelja i drugo (Surette, 2005).

Ova se tehnologija često koristi za nadgledanje javnih prostora (granični prijelazi, promet i prometna čvorišta, središta grada, pješačke zone, parkirališta, kvartovi, parkovi i sl.), polujavnih objekata (banke, tvrtke, kazina) i trgovačkih centara. Za potrebe ovog rada evaluacija učinkovitosti videonadzora odnosit će se na problemski orijentiranu kriminalističku prevenciju na javnim mjestima.

Sustav videonadzora nije fizička barijera za činjenje kaznenih djela, ali je iznimno koristan za situacijsku prevenciju kriminaliteta. Njegova prednost sastoji se u tome što može biti okidač perceptivnog mehanizma kod potencijalnih počinitelja usmjeren na njegovu svijest o tome da može biti uhićen, ako odluči ući u kažnjivu zonu. S obzirom na to da se doživljena opasnost povećava kod racionalnih počinitelja, ovaj faktor ih, u pravilu, obeshrabruje u toj nakani (Clarke, Cornish, 1985). Međutim, da bi ovaj psihološki proces ostvario uspjeh, moraju biti zadovoljena dva elementa:

1. Počinitelj mora biti svjestan prisutnosti kamera i znati da je nadziran.
2. Počinitelj mora vjerovati da kamere predstavljaju dovoljan rizik uhićenja koji anulira korist pribavljenu kaznenim djelom.

Nalazi istraživanja Dittona i sur. (1999, 24) te Honessa i Charmana (1992, 6) upućuju na činjenicu da, unatoč javnoj kampanji i označavanju mjesta videonadzora, relativno je mali udio stanovnika svjestan ili zna da nadzor postoji (30-40%). Koncept videonadzora podrazumijeva počiniteljevu demonstraciju racionalne prosudbe svog ponašanja, što često nije slučaj. Naime, postoje dokazi da su neki potencijalni počinitelji pod utjecajem alkohola ili droga, zbog čega im je sposobnost rasuđivanja i samokontrole smanjena u odnosu na percepciju videonadzora. Ovo je jedan od faktora koji uvjetuje bolju učinkovitost prisutnosti videonadzora tijekom dokazivanja imovinskog u odnosu na nasilnički kriminalitet (Short, Ditton, 1998).

Pored navedenog, videonadzor ima potencijal za smanjenje kriminaliteta kao pomoćni alat policiji u otkrivanju i uhićenju počinitelja. Evaluacije pokazuju da se taj odgovor mora dogoditi u što kraćem vremenu i biti vezan za značajne incidente koje snimaju operateri. Jednako tako, pravosuđe mora odgovoriti brzom sankcijom. Naime, delinkventi pozorno prate koje vrste kažnjivih ponašanja potiču policijsku intervenciju *in flagranti* i kolika je brzina intervencije. Stoga je iznimno važna dostupnost navedenih lokalnih resursa. U prilog ovoj konstataciji govore i nalazi eksperimentalne studije u New Orleansu (Usher, 2003b) koja je pokazala da se učestalost kaznenih djela smanjuje otkrivanjem kaznenih djela i uhićenjem počinitelja *post delictum*, a ne prevencijom, što se procjenjuje relativno slabim učinkom rada policije. Slično istraživanje Makkai i sur. (2004) u Australiji pokazuje kako povećanje

uhićenja ima kratkotrajnu korist koja, dugoročno gledano, nestaje bez uvođenja preventivnih mjera policije.

Važno je razmotriti i učinkovitost tehnologije nadzora u odnosu na vrstu kaznenog djela s obzirom na sposobnost prilagodbe delinkvenata situaciji. Evaluacije upućuju na smanjenu vjerojatnost činjenja provalnih krađa u trgovačkim centrima unutar dosega videonadzora. Nasuprot tome, evidentirano je da se preprodavači droga susreću i dogovaraju u prisutnosti kamera, a transakcije zaključuju na drugom mjestu (Edmunds, Hough, Urquia, 1996).

Općenito uzevši, ova vrsta nadzornog mehanizma može reducirati stopu kriminaliteta kroz povećanje kolektivne učinkovitosti. U tom smislu Welsh i Farrington (2004) smatraju kako uočljiva prisutnost videonadzora lokalnom stanovništvu daje osjećaj sigurnosti i teritorijalnosti (pripadnosti) njihovom stambenom području, što dovodi do povećanja razine neformalne socijalne kontrole. S druge strane, držimo da vidljive kamere mogu izazvati neželjene posljedice. Na svojevrstan način mogu pridonijeti osjećaju stanovnika o stigmatiziranosti njihovog lokalnog područja visokom stopom kriminaliteta što može ubrzati proces njegove društvene dezorganizacije.

2.1. Ostale prednosti videonadzora

Prednosti videonadzora su višedimenzionalne i očituju se u smanjenju straha od kriminaliteta u lokalnoj zajednici, pružanju hitne medicinske skrbi, upravljanju mjestom događaja, prikupljanju informacija, dodanoj vrijednosti ovog nadzora i kao pomoć u kriminalističkom istraživanju.

Provedene studije su intervjuiranjem kupaca u trgovačkim centrima upozorile na povećanje ukupnog broja ljudi koji se osjećaju zaštićenima postojanjem videonadzora, što istodobno povećava i prirodni nadzor u situaciji visoke koncentracije ljudi na određenom području (Ratcliffe, 2006). Jačanje osjećaja sigurnosti ohrabruje građane da češće prebivaju u nadziranom prostoru. Jednako tako, potencijalne žrtve najvjerojatnije mijenjaju svoje ponašanje pod budnim okom kamera. Ipak, kako Ratcliffe (2006) ističe, riječ je manjem udjelu kupaca (oko 40%) koji znaju za područje pokriveno kamerama. Naime, osjećaj sigurnosti građana posljedično pozitivno utječe i na veću ekonomsku dobit ove gospodarske grane.

Za sigurnost zajednice važno je istaknuti da u slučaju ozljeda proisteklih iz počinjenog kaznenog djela ili zbog iznenadnih bolesnih stanja građana koji se događaju na javnim mjestima, operateri žurno izvještavaju hitnu medicinsku službu i policiju, što je izravna korist za javnu sigurnost. Tako Squires (2000) navodi da je tijekom 700 sati promatranja i nadgledanja zabilježeno 20 takvih poziva policiji.

Upravljanje nadziranim prostorom je od neizmjerne važnosti u slučajevima nestanka djece, nadzora prometa, javnog okupljanja ili prosvjeda što iziskuje dodatne policijske snage i resurse. U tom pogledu Brown (1995, 7) navodi da je korištenje videonadzora uvelike smanjilo napade na policiju te je dodatno pomoglo u donošenju procjene za upućivanje prikladnih policijskih snaga na poprište događaja.

Videokamere se koriste i za prikupljanje relevantnih podataka i nadgledanje ponašanja otprije poznatih počinitelja na javnim prostorima (npr. počinitelji krađe u trgovinama ili preprodavači ukradenih predmeta) (Brown, 1995, 7). U pravilu je riječ o pravodobnom prepoznavanju lokalnih počinitelja čije se kretanje prati nenametljivo i s udaljenosti, bez ulaska u fizički prostor počinitelja.

Dodana vrijednost videonadzora očituje se u mogućnosti zahvaćanja šireg područja javnog prostora od zadanog o dosegu kojeg delinkventi nisu svjesni. U kriminološkoj istraživačkoj literaturi ova ekstenzivna vrijednost videonadzora poznata je pod nazivom "širenje koristi" od videonadzora u okolna, nadzorom nepokrivena područja (eng. *diffusion of benefits*) (Harris i sur., 1998, 19).

2.2. Neželjene posljedice videonadzora

Istraživanja upozoravaju na određene slabosti i manjkavosti videonadzora koje uključuju premještanje kriminaliteta, jačanje sumnje ili strah od kriminala i povećani broj kaznenih prijava.

Nerijetko se događa da se umjesto smanjenja, kriminalitet premješta u druge dijelove grada koji su izvan dosega videonadzora. Međutim, provedene evaluacije (Ratcliffe, 2002) sugeriraju da se prostorno premještanje kriminaliteta događa povremeno te da je, s obzirom na omjer, veća korist za kriminalističku prevenciju koja se očituje u redukciji kriminaliteta. Više studija je dokazalo da *nema potpunog premještanja kriminaliteta* iz područja pokrivenog kamerama u susjedno područje. Štoviše, u tom pogledu radi se o relativno malom udjelu kriminaliteta. Primjerice, studija provedena u Londonu (Edmunds i sur., 1996, 16-17) pokazala je maštovitost i inventivnost preprodavača droga koji su zbog sveprisutnih kamera razvili sustav narudžbi putem mobilnih telefona, zbog čega su isporuku morali značajno ubrzati. U ovom slučaju je riječ o taktičkom premještanju pri kojem delinkventi mijenjaju *modus operandi* kako bi osigurali kontinuitet svojih kriminalnih aktivnosti. Navedeno upućuje na činjenicu kako videonadzor može izravno utjecati na modifikaciju ponašanja počinitelja koja u konačnici može imati pozitivni predznak. Naime, ova skupina počinitelja je bila prisiljena odabrati za njih manje učinkovit način organiziranja primopredaje droga što, ukupno gledajući, pridonosi redukciji kriminaliteta.

Sljedeći problem može biti negativna reakcija javnosti na prisutnost videonadzora. Tako su Honess i Charman (1992, 17) u ispitivanju građana utvrdili kako trećina njih smatra da je videonadzor namijenjen "špijuniranju ljudi", zbog čega za to odgovorni gradski službenici nerado oglašavaju i postavljaju vidljive kamere, smatrajući kako će time izazvati nepotrebno negodovanje i strah kod trgovaca i kupaca. Prema tome, iako većina građana vjeruje i osjeća se sigurnije uz videonadzor, za određene skupine ljudi kamere izazivaju suprotan efekt. U tom kontekstu valja naglasiti da videonadzor kao mehanizam primarne prevencije kriminaliteta u psihološkom smislu utječe na povećanu percepciju rizika za počinitelje pa se skrivanjem kamera može nehotice umanjiti njihova učinkovitost.

Posljednja neželjena posljedica je mogući porast zabilježenog kriminaliteta ili određenih vrsta kaznenih djela. Istraživanja Winge i Knutssona (2003) u Oslu pokazala su da se videonadzorom povećava otkrivanje nasilničkog ponašanja, grafita, a osobito preprodaja

droga. Potrebno je napomenuti da ovdje nije riječ o stvarnom kriminalitetu, nego isključivo o registriranom (snimljenom) kriminalitetu. U svakom slučaju kamere omogućuju sekundarnu prevenciju kriminaliteta koja vodi u smanjivanje tamne brojke kriminaliteta.

3. ODABRANA ZNANSTVENA ISTRAŽIVANJA UČINKOVITOSTI VIDEONADZORA U SMANJENJU KRIMINALITETA

Respektabilan broj istraživanja odnosi se na ispitivanje percepcije odgovornih osoba i javnosti u odnosu na ishode i koristi od uporabe kamera u kriminalističkoj prevenciji. Njihovi stavovi su uobičajeno pozitivni iako su dokazi o smanjenju stvarno postojećeg kriminaliteta teže dostupni (Honess i Charman, 1992; Ratcliffe, 2006). Pouzdanost nekih istraživanja je metodološki upitna jer autori ne uzimaju u obzir i ispitivanje kontrolnog područja, neovisnost istraživača i pojednostavljeno pristupaju vremenskim sekvencama (obrascima) kriminaliteta. Stoga su za potrebe ovoga rada ciljano odabrana opsežna istraživanja učinkovitosti videonadzora u Velikoj Britaniji, SAD-u i Kanadi u kojima je korištena i opisana znanstvena metodologija.

Velika Britanija

Stalno unapređenje tehnologije videonadzora, široka dostupnost i ekonomičnost sveukupne opreme doprinijeli su kontinuiranom povećanju lokacija na javnim površinama na kojima se ugrađuje videonadzor u situacijskoj prevenciji kriminaliteta. U tom pogledu zabilježen je ogroman porast lociranja kamera u Velikoj Britaniji (Fussey, 2007), osobito u Londonu (Davenport, 2007). Nešto je manjeg opsega njihovo korištenje od strane policije u Kanadi i SAD-u iako se bilježi porast saveznog financiranja lokalnih policija u borbi protiv terorizma nakon terorističkih napada u rujnu 2001. godine (Cameron i sur., 2008).

Za potrebe ovog rada načinjen je pregled važnijih studija uzimajući u obzir pouzdanost korištene metodologije istraživanja u procjeni učinkovitosti videonadzora u smanjenju kriminaliteta. Prvu meta-analizu[56] kodiranjem ključnih obilježja veličina efekata 46 studija glede učinaka u prevenciji kriminaliteta proveli su Welsh i Farrington (2002). Procjenjujući njihovu metodološku kvalitetu za donošenje zaključka, autori su odabrali 22 studije prema strogim kriterijima mjerenja kriminaliteta prije i poslije praćenja videonadzora u eksperimentalnim i kontrolnim područjima (Sherman i sur., 2002). Istraživači su zaključili da je željeni efekt pokazala samo polovica promatranih studija. Kad je riječ o specifičnim lokacijama, mali pozitivan učinak zabilježen je u strogim središtima gradova te u još manjoj mjeri u stambenim četvrtima (za samo 2% postignut je bolji efekt na eksperimentalnim lokacijama). Kamere u javnom prijevozu utjecale su na smanjenje delinkventnog ponašanja, ali ne značajno. Jedino kod nadzora parkirališta, uz istodobno ulično osvjetljenje, videonadzor

[56] "Meta-analiza je sustavni pregled istraživanja u kojemu se uspoređuju, kombiniraju i sintetiziraju različite, međusobno neovisne studije te integriraju njihovi rezultati u zajednički jedinstveni rezultat" (Bartolucci, 2009, 127).

je pokazao statistički značajnu valjanost koja se očitovala u smanjenju krađa vozila za 41%. Gill i Springs (2005) također su proveli opsežni pregled 13 evaluacija projekata videonadzora u različitom fizičkom okruženju poput središta gradova, parkirališta, bolnica i stambenih četvrti. Cilj njihove meta-analize bio je izmjeriti učinak kamera na učestalost kaznenih djela i na strah od kriminaliteta građana. Koristili su kvazieksperimentalni model – 3. razinu Maryland skale (*Maryland Scientific Methods Scale*) (Sherman i sur., 2002) koja mjeri promjenu u incidenciji kriminaliteta prije i nakon ugradnje videokamera u ciljanom i kontrolnom području. Autori su se oslonili na policijske evidencije kriminaliteta u mjerenju razina kriminaliteta u eksperimentalnom i usporedivom kontrolnom području. Istodobno su praćene i promjene u vrstama kaznenih djela na širem području od onog koje pokriva videonadzor s ciljem mjerenja premještanja učinka tzv. širenja koristi od postojećeg videonadzora (eng. *diffusion of benefits*). Od 13 evaluiranih sustava videonadzora, manje od polovice (Welsh, Farrington, 2002) pokazalo je relativno značajno smanjenje kriminaliteta u ciljnim područjima u usporedbi s kontrolnima, a samo dva sustava pokazala su statistički značajnu redukciju kriminala. Kriminalitet je porastao u 7 eksperimentalnih područja s videonadzorom zato što se dogodio stjecaj drugih zavisnih varijabli poput nacionalnih, sezonskih i drugih izdvojenih karakterističnih trendova u pojavnosti kaznenih djela zbog kojih, inače, dolazi do fluktuacije u stopama kriminaliteta. Najbolji rezultati očitovali su se u miješanoj kategoriji područja koja su se sastojala od parkirališta, bolnica i stambenih četvrti koje je pokrivao jedinstveni sustav kamera. Rezultati su varirali u kriminalnim trendovima u zasebno nadziranim središtima gradova, odnosno stambenim područjima. Naime, bolji rezultati su bili postignuti u odnosu na prethodno pripremana kaznena djela (krađe motornih vozila) od tzv. nepromišljenog ili impulzivnog kriminaliteta (npr. pod djelovanjem alkohola ili droga). U tom smislu zabilježena je značajna prevalencija kaznenih djela protiv života i tijela. Pritom je važno istaknuti kako su određene karakteristike sustava nadzora pokazale svoju prednost: opseg prostora koji pokriva, gustoća kamera (broj kamera koji je ugrađen po jedinici područja) te lokacija koja ima ograničene i kontrolirane pristupne točke popu ulaza i izlaza iz nadziranog područja.

Ispitivanja javnog mnijenja provedena su prije i nakon ugradnje videonadzora na 12 različitih područja, od toga 9 u stambenim četvrtima i 3 u središtu gradova. Ispitivanja građana su pokazala da su oni uglavnom svjesni nadzora kad su u pitanju manje stambene četvrti. U samo tri intervencijska područja građani su (statistički značajno) očitovali manji strah od viktimizacije pri čemu vrsta nadziranog područja nije bila od važnosti. Međutim, ispitanici koji su znali za postojanje kamera, iskazali su veću zabrinutost za svoju sigurnost od ostalih kojima ta činjenica nije bila poznata. Autori su zaključili kako spoznaja o prisutnosti videonadzora ne stvara neizostavno i osjećaj sigurnosti kod građana.

Nakon postavljanja videokamera smanjio se broj žrtava kaznenih djela u 8 eksperimentalnih područja, što je bilo u skladu sa slučajevima koje je registrirala policija. Viktimizacija nije bila povezana s navedenim vrstama područja pokrivenih videonadzorom. Bojazan od viktimizacije se smanjivala upravo razmjerno s redukcijom prijavljenih kaznenih djela od strane žrtava. Stoga proizlazi kako je zabrinutost građana izravno povezana s razinom realno prijavljenog kriminaliteta, a ne s postojanjem videonadzora.

Utvrđeno je, također, kako unatoč prisutnosti kamera, ispitanici gotovo uopće nisu mijenjali svoje ponašanje – samo 2-7% njih posjećivalo je mjesta koja su prethodno izbjegavali iako je 15% ispitivanih građana prije uvođenja kamera smatralo da će ih postojanje nadzora ohrabriti.

Kad je riječ o razini potpore građana uvođenju videonadzora, gotovo dvije trećine (70%) građana se izjasnilo dajući mu snažnu potporu. U tom pogledu autori smatraju kako će uz videonadzor građani češće prijavljivati kaznena djela policiji koja će, opet, brže reagirati na prijave takvih incidenata. U konačnici, smatraju da će se takvom sinergijom učinkovito smanjiti i kriminalitet. Gill i Spriggs (2005) analizirali su i tehničke karakteristike, dizajn, postupak provedbe i ugradnje kamera, upravljanje videonadzorom iz kontrolne sobe i suradnju s policijom. Zaključno naglašavaju da svaki videonadzor treba biti poduprt strateškim planom s jasnim ciljevima ovog sustava, uzimajući u obzir lokalne probleme i već otprije postojeće preventivne mjere.

SAD

Nekoliko evaluacija učinkovitosti videonadzora provedeno je u SAD-u. Welsh i Farrington (2004) proveli su *follow-up* studiju 5 evaluacija i zaključili da ni jedna od njih nije dokazala statistički značajno smanjenje kriminaliteta. Međutim, nekoliko neovisnih studija manjeg opsega provedenih u Philadelphiji, Berkeleyu i Los Angelesu donekle su dale optimistične rezultate. Ratcliffe i Taniguchi (2008) hijerarhijskim su linearnim modeliranjem dokazali tek 13 postotno smanjenje kriminaliteta u Philadelphiji, uzimajući u obzir sezonske promjene stopa kaznenih djela i opće trendove kriminaliteta u promatranim područjima. Jennifer King i sur. (2008) ispitivali su učinkovitost manjeg videosustava u San Franciscu u odnosu na ukupnu statistiku teških kaznenih djela s elementima nasilja i imovinskog kriminaliteta. Rezultati su pokazali statistički značajan pad kaznenih djela protiv imovine, i to za 24% na udaljenosti od 4 m od postavljenih kamera. Videonadzor se pokazao djelotvornijim na javnim u odnosu na privatne lokacije, ali je bio učinkovit i u susjednim područjima bez videonadzora (efekt "širenja koristi"). Ipak, testiranje područja obuhvaćenih videonadzorom upućuje na značajan efekt odvraćanja od počinjenja imovinskog kriminaliteta zahvaljujući videonadzoru. Od kaznenih djela s elementima nasilja značajno smanjenje registrirano je samo kad je riječ o ubojstvu. Jednako tako, autori su istakli ogroman doprinos snimaka u identifikaciji osumnjičenika i svjedoka u kriminalističkom istraživanju i daljnjem sudskom postupku.

Utjecaj videonadzora na kriminalitet istraživali su Cameron i sur. (2008) na jednoj od ključnih prometnica i u stambenoj četvrti u Los Angelesu. Nalazi su pokazali da ne postoji statističko značajno smanjenje ni jedne vrste kaznenih djela te da je ključno lokalno osmišljavanje i provedba kriminalističke prevencije od strane policije, skupina u zajednici i poslovnih ljudi.

Slijedom navedenog zaključili su sljedeće:

- videonadzor je kvalitetan alat za policiju, ali ne i "čudotvorni lijek za sve"
- učinkovit i održiv videonadzor zahtijeva odgovarajuću obuku, vođenje i resurse

- odvraćanje od činjenja kaznenih djela i primjerena intervencija policije moraju biti uzajamno isprepleteni
- potrebna su dodatna istraživanja kako bi se utvrdilo kako operacije ove vrste na lokalnom području mogu utjecati na provedbu šireg programa koji uključuje otkrivanje, uhićenje i progon kriminalaca.

Kanada

U istraživanju učinaka sustava videonadzora u Kanadi sudjelovali su istraživači istraživačkog policijskog centra u Torontu (Verga, 2010). Proveli su randomizirani pokus na pet ciljanih lokacija uspoređujući ih s kontrolnim područjima sa sličnim obilježjima (opća lokacija, fizička obilježja prostora, ista ili slična razina kriminaliteta). Razina kriminaliteta na svim lokacijama je bila relativno stabilna u posljednjem desetljeću pa su tako sezonski varijabilni efekti bili eliminirani. Zabilježili su sve incidente na navedenim područjima prije i nakon uvođenja videonadzora. Usporedili su incidente sa snimaka koji su se dogodili u razdoblju od 6 do 12 mjeseci s policijskim podacima. Utvrđeno je da je razina kriminaliteta smanjena na trima lokacijama, a u preostale dvije lokacije, kontrolnim područjima i u svim zonama okruženja ("širenje koristi") učestalost počinjenja kaznenih djela ostala je uglavnom nepromijenjena. Međutim, ukupni rezultati nisu bili statistički značajni i umnogome se podudaraju s nalazima istraživanja u Velikoj Britaniji i SAD.

4. RASPRAVA

U današnje vrijeme postignuti su svi tehnološki i informacijski preduvjeti korištenja videonadzora kao kriminalistički relevantnoga preventivnog mehanizma u politici suzbijanja kriminaliteta. Pregled prezentiranih istraživanja i njihovih rezultata daje prilično šarenu sliku pa i dvojbene nalaze o djelotvornosti videonadzora u smanjenju incidencije kaznenih djela. Iako postoje stanoviti dokazi u tom smislu, rezultati nisu impresivni, a posebno nisu razmjerni s naglim porastom inicijativa za provođenjem kriminalističke prevencije koja bi se oslonila na videonadzor na javnim mjestima. Najveći broj studija pokazuje kako je učinkovitost ovog sustava ovisna o lokaciji kamera, ali i o vrsti kaznenih djela. Primjerice, prilično konzistentan nalaz provedenih studija upućuje na efekt smanjenja krađa vozila na parkiralištima pokrivenim kamerama. Dosljednima su se pokazali i rezultati u redukciji imovinskog kriminaliteta, osiguranju javnog reda i mira te za počinitelje kaznenih djela koji pažljivo planiraju i pripremaju počinjenje djela u kombinaciji s jakim osvjetljenjem. Nažalost, nalazi istraživanja o kaznenim djelima s elementima nasilja nisu ohrabrujući jer je u svim provedenim studijama krajnji učinak bio neznatan ili nije pokazao statističku značajnost te se posljedično nije dokazao njihov silazni trend. Međutim, nedvojbeni zaključci proizlaze iz korištenoga eksperimentalnog dizajna na temelju kojeg je postignuto suglasje među autorima kako promatrani učinci izravno ovise o specifičnim obilježjima ciljanog područja. Stoga je važno naglasiti da je takva metodologija istraživanja iz navedenog razloga ograničena posljedično činjenicom što je nije moguće u potpunosti replicirati na nekom drugom eksperimentalnom području. Naime, prilikom evaluacije djelotvornosti videonadzora u smanjenju kriminaliteta od velike je važnosti razumjeti i osmisliti izbor ciljane

(eksperimentalne) lokacije videonadzora i njenog fizičkog okruženja. Prije svega, potrebno je razmotriti i analizirati postojanje i raspoloživost mjera za prevenciju i suzbijanje kriminaliteta prije i poslije uvođenja sustava kamera, mogućnost interpolacije videonadzora u postojeće preventivne mjere i prikladnost kontrolnih mjera. Bilo bi idealno da se pri dizajniranju videonadzora identificiraju one lokacije na kojima se ne odvijaju druge vrste izvanjskih intervencija od predviđenih zbog njihova utjecaja na proces i rezultate. Naime, događa se da nepredvidive, iznenadne varijable interferiraju u eksperimentalno praćenje i proučavanje učinkovitosti videonadzora.

Potrebno je obaviti slučajni odabir opisanih lokacija, a ostale koristiti za kontrolno mjerenje. Određuje se i fizičko okruženje predmetnih lokacija, analiziraju dostupni statistički podaci o počinjenim kaznenim djelima u svrhu utvrđivanja mogućeg "širenja koristi" ili efekta premještanja kriminaliteta koji mogu biti u korelaciji s proučavanim sustavom videonadzora. Istodobno se trebaju uzeti u obzir trendovi kriminaliteta, sezonske varijacije i druge relevantne zavisne varijable za odabrane lokacije.

U stvarnim životnim situacijama eksperimentalna istraživanja se provode najčešće radi žurne potrebe za nekom intervencijom na problematičnim lokacijama kada se razmatraju sve dostupne činjenice. Nasuprot tome, idealni uvjeti za provođenje eksperimentalnih istraživanja u realitetu koji nas okružuje su nemogući te je potrebno oprezno tumačiti dobivene rezultate uzimajući u obzir ograničenja prezentirana u ovom radu. Upravo je to razlogom da se o učinkovitosti videonadzora s namjerom smanjenja kriminaliteta ne mogu izvoditi uopćeni ili unisoni zaključci.

U konačnici, buduća istraživanja potrebno je više usmjeriti na funkcioniranje i utjecaj videonadzora u lokalnoj zajednici te percepciju sigurnosti građana u korelaciji s višestrukom funkcijom videonadzora.

5. ZAKLJUČAK

Na temelju pregleda u ovom radu prezentiranih istraživanja i njihovih rezultata može se utvrditi kako su autori skloni oprezno tumačiti složeni obrazac faktora koji utječu na uspjeh ili neuspjeh provedenih studija. Kruti metodološki zahtjevi kad su u pitanju statistički dokazi, uvelike ograničavaju donošenje jednoznačnih ili nedvojbenih zaključaka. Međutim, izvan strogih kriterija svojstvenih kvantitativnim metodama ipak je moguće konstatirati kako postoje dokazi o smanjenju kriminaliteta korištenjem videonadzora. Naime, sve je više nalaza koji upućuju na uspjeh u smanjenju incidencije kaznenih djela. U svakom slučaju, prisutnost kamera neće pogoršati situaciju na nekom području. Od najveće važnosti je razumjeti i procijeniti lokalni kontekst i dostupnost policijskih snaga koje će žurno i primjereno odgovoriti na incident. Istodobno, da bi se postigla što bolja efikasnost, potrebno je koristiti manje sustave videonadzora u strogo definiranim područjima.

Percepcija javnosti o prednostima videonadzora uglavnom je pozitivna (Norris, Armstrong, 1999) budući da se naglašava aktivno sudjelovanje i zaštita građana, a ne nadziranog javnog mjesta, tim više što građani na javnim mjestima ne očekuju zaštitu

privatnosti. Na mjestima gdje se učestalo događaju kaznena djela, videonadzor predstavlja rješenje usmjereno upravo na taj problem.

Kad je riječ o razini utjecaja na smanjenje straha od kriminaliteta kod građana, rezultati istraživanja nisu uvjerljivi jer se uspjeh u tom smislu može postići samo kod nekih skupina u populaciji pod uvjetom da znaju kako su nadzirani. U tom smislu potrebno je provoditi javne kampanje.

Prednosti videonadzora ne treba precjenjivati jer on funkcionira različito u različitim situacijama (Ditton i sur., 1999). Kao što je u radu elaborirano, optimalni rezultati postižu se u kombinaciji s drugim preventivnim mjerama. Na kraju, važno je upozoriti kako stalno rastući videonadzor na nekim javnim mjestima ili u stambenim naseljima može učiniti život građana manje ugodnim mjestom za život.

LITERATURA

Bartolucci, A. A. (2009). *Opis i tumačenje metodoloških i statističkih tehnika u meta-analizama*. *Biochemia Medica,* 19(2), 127-136.

Ulrich, B. (1992). *Risk society: Toward a new modernity*. London: Sage Publishing

Brown, B. (1995). *CCTV in Town Centres: Three Case Studies*. *Crime Detection and Prevention Series,* Paper 68, London: Home Office.

Cameron, A., Kolodinski, E., May, H., Williams, N. (2008*). Measuring the effects of video surveillance on crime in Los Angeles.* Technical Report CRB-08-007, California Research Bureau.

Clarke, R. V., Cornish, D. B. (1985). *Modeling Offenders' Decisions: A Framework for Research and Policy.* U: N. Morris (ed.), Crime and Justice: An Annual Review of Research, 6. Chicago: University of Chicago Press.

Coleman, R. (2004). *Reclaiming the streets. Surveillance, social control and the city.* Cullompton: Willan Publishing.

Cvitanović, L. (2010). *Power of surveillance – implications of technological and information step forward in the 21st century on criminal policy and criminal law.* Godišnjak Akademije pravnih znanosti Hrvatske, 1 (1), 147-160.

Davenport, J. (2007). *Tens of thousands of CCTV cameras, yet 80 percent of crime unsolved.* London: Evening Standard. http://www.standard.co.uk/news/tens-of-thousands-of-cctv-cameras-yet-80-of-crime-unsolved-6684359.html, preuzeto 22. 2. 2016.

Ditton, J., Short, E., Phillips, S., Norris, C., Armstrong, G. (1999). *The Effect of Closed Circuit Television on Recorded Crime Rates and Public Concern about Crime in Glasgow* (Final report). Edinburgh: The Scottish Office.

Edmunds, M., Hough, M., Urquia, N. (1996). *Tackling Local Drug Markets. Crime Detection and Prevention Series,* Paper 80. London: Home Office.

Ericson, R., Haggerty, K. (1997). *Policing the Risk Society*. Toronto: University of Toronto Press.

Foucault, M. (1975). *Discipline and punish: The birth of a prison.* New York.

Fussey, P. (2007). An Uninterrupted Transmission? Processes of CCTV Implementation and the Impact of Human Agency. *Surveillance & Society*, Special Issue on *'Surveillance and Criminal Justice*', 4(3), 229–256.

Gill, M., Spriggs, A., Argomaniz, J., Bryan, J., Waples, S., Allen, J., Kara, D., Kilworth, J.,

Little, R., Smith, P., Swain, D., Jessiman, P. (2005). *Technical Annex: methods used in assessing the impact of CCTV.* Technical Report Home Office Online Report 17/05. London: Home Office.
Goold, B. J. (2004). *CCTV and Policing: Public Area Surveillance and Police Practices in Britain*. Oxford: Oxford University Press.
Harris, C., Jones, P., Hillier, D., Turner, D. (1998). CCTV Surveillance Systems in Town and City Centre Management. *Property Management* 16(3), 160-165.
Honess, T., Charman, E. (1992). *Closed Circuit Television in Public Places*. Police Research Group: Crime Prevention Unit Series, Number 35, London: Home Office.
King, J., Mulligan, D. K., Raphael, S. (2008). CITRIS Report: *The San Francisco Community Safety Camera Program*. Technical Report. Berkley: University of California Center for Information Technology Research in the Interest of Society.
Leman-Langlois, S. (2002). The Myopic Panopticon: The social consequences of policing through the lens. *Policing and Society*, 13(1), 43-58.
Makkai, T., Ratcliffe, J. H., Veraar, K., Collins, L. (2004). ACT recidivist offenders. *Research and Public Policy Series*, 54, 83.
Norris, Clive (2003). From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. U: D. Lyon (ed.) *Surveillance as Social Sorting: Privacy, risk and digital discrimination*. London: Routledge, 249-81.
Norris, C., Armstrong, G. (1999). *The Maximum Surveillance Society*. New York: Berg.
Ratcliffe, J., Taniguchi, T. (2008). *The crime reduction effects of public CCTV cameras in the city of Philadelphia.* Philadelphia: Temple University.
Sherman, L. W., Farrington, D. P., Welsh, B. C., (Eds.), D. L. M. (2002). *Evidence-based crime prevention*. London: Routledge.
Short, E., Ditton, J. (1996). *Does Closed Circuit Television Prevent Crime? An Evaluation of the Use of CCTV Surveillance Cameras in Airdrie Town Centre*. Edinburgh: The Scottish Office Central Research Unit.
Squires, P. (2000). *CCTV and Crime Reduction in Crawley: Follow-up Study 2000*. Brighton, UK: Health and Social Policy Research Centre.
Surette, R. (2005). The Thinking Eye: Pros and Cons of Second Generation CCTV Surveillance Systems. *Policing: An International Journal of Police Strategies and Management* 28(1), 152-173.
Usher, N. (2003a). Video Surveillance Comes to Big Easy. *San Diego Union-Tribune*, 24, 14.
Usher, N. (2003b). Who's Watching You? *Times-Picayune*, 9, 1.
Verga, S. (2010). *Closed-circuit TV surveillance evaluation: Statistical analysis of the effects on rates of crime. Technical Report*. Toronto: Defence R&D Canada-Centre for Security Science.
Vijver, K. (1998). *De Tranen van Foucault.* Enschede: Universiteit Twente.
Welsh, B. C., Farrington, D. P. (2004). Evidence-based Crime Prevention: the Effectiveness of CCTV. *Crime Prevention and Community Safety: An International Journal*, 6(2), 21–33.
Welsh, B. C., Farrington, D. P. (2002). *Crime prevention effects of closed circuit television: a systematic review.* Technical Report Home Office Research Study 252. London: Home Office.

Ksenija Butorac
Irena Cajner Mraović
Hrvoje Filipović

EFFECTIVENESS OF CCTV SURVEILLANCE ON REDUCING CRIME – A RESEARCH REVIEW

Summary

The police have at their disposal a great variety of methods, tools and strategies for different aspects of policing. Some examples have a technological aspect, such as bicycle patrols, the use of CCTV, giving mobile alarms to victims of family violence; use of wire taps in surveillance of suspected criminal groups; water cannons, etc. Police researchers are interested in how social and technological change and modernization processes influence policing. One aspect deals with how the new types of information and communication technology are implemented in various types of police units and the effects they have on police cultures and policing practices. Others focus on technologies of control, such as the use of CCTV and other systems of surveillance. Important questions in research on CCTV are whether these systems reduce the level of crime and order problems in the areas of surveillance; whether there is a displacement of problems to other areas; whether CCTV helps to clear crimes; and whether there are other positive or negative side effects. Most of the studies had found that the effectiveness of CCTV surveillance was dependant on the location of cameras, as well as the type of crime. Generally, the effects were most pronounced in the types of crimes that imply premeditation, and in areas where the CCTV implementation was supplemented with other interventions (e.g., improved street lighting). The results reported were more inconclusive for violent crime offences. Most studies reviewed have not found declines in violent crime; and those that did found that the effect was small and, in most cases, statistically insignificant.

Key words: *video-surveillance, control, crime, research, effectiveness.*

PREGLEDNI ZNANSTVENI RAD

Vladica Babić[57]
Zdravko Skakavac[58]

SUSTAVI NADZORA SUVREMENIH TEHNIČKIH SREDSTAVA I NJIHOVA UČINKOVITOST

Sažetak

I pored ogromnih nastojanja i uspostava sistema nadzora te mogućnosti da se broj naizgled beskrajnih izbora različitih metoda i načina kojima se cyber kriminalci koriste pri infiltriranju u kompjutorske mreže, vlade, međunarodnih organizacija i privatne industrije, jasno je da se pod hitno moraju poduzeti niz od nekoliko koraka u godinama koje dolaze u području prava, politike i tehnologije za zaštitu podataka i suzbijanju ovih sve viših pojava u cyber prostoru. U tu svrhu, potrebno je uključiti sve segmente sigurnosti te regulirati zakonodavne okvire, usvojiti međunarodne konvencije i tehnološke standarde. Preporučeni koraci prema međunarodnoj suradnji su obvezni i s njima treba nastaviti i konstantno ih usavršavati, jer niti jedan od tih koraka ne može potpuno osigurati Internet i u cjelini suzbiti cyber kriminal.

Ključne riječi: *Cyber crime, sistemi nadzora cyber prostora*

1. UVOD

Navedeni sustavi pri analizi komunikacija se koriste sustavima umjetne inteligencije kao *Memex* za analizu glasa i pretvaranje poruke u pisani oblik, zatim dekriptiranja šifriranih poruka i dalja analiza. Raspored prislušnih postaja omogućava slušanje cijelog planeta. Za razliku od prisluškivanja i nadzora za vojne svrhe, *Echelon* je isključivo usmjeren na civilne sustave, što znači da se prate i obrađuju informacije civilnih korisnika, poslovnih sustava, pojedinaca, veleposlanstava i vlada.

Zbog sporog i malo učinkovitog sustava u razvijenim zemljama javila se potreba za uspostavljanjem nekoliko novih nadzornih sustava, koji su svoju operativnost iskazali kroz djelovanje i nedavno predstavljanje u javnosti putem *Edwarda Snowdena*. Zvidač *Snowden* je izašao s podacima za velike sustave od strane *NSA*, te ih objelodanio kroz svoje predstavljanje kao zaposlenika u takvom sustavu. Pored sustava koje je prijavio navodno postoje i drugi sustavi za nadzor i presretanje različitih vrsta komunikacija. Neki od njih su u sustavu SAD-a, UK-a, Australije, Kanade, Novog Zelanda, Francuske, itd. Tako imamo, pod različitim imenima savršene nadzorne sustave koje ćemo u kratkim crtama opisati, te ponuditi

[57] Dr. sc. Vladica Babić, Visoka škola LogosCentar Mostar, e-mail: vladica_babic@net.hr
[58] Prof. dr. Zdravko Skakavac, Fakultet za pravne i poslovne studije dr. Lazar Vrkatić Novi Sad, e-mail: zskakavac@useens.edu

pojašnjenje njihove glavne namjene i zadatka koji obavlja. Kodna imena ovih nadzornih sustava su većini poznata:

Slikworth sustav usklađivanja obavještajnih signala kodiranih imena nadzora dugovalnog radiofrekventnog spektra od strane specijalista iz *Menwith Hill*;

Moonpenny je sustav za nadzor satelitskih komunikacija;

Site, Runway i *Steepbush*su projekti koji kontroliraju mrežu špijunskih satelita postavljenih iznad Rusije pod imenom *VORTEX* – prije njega je bio *CHALET* i *Steepbush* kontrolni centar spojen s najnovijim i najvećim prislušnim satelitima, nazvanim *MAGNUM*, u suradnji s američkim obavještajnim izvorima. Također, jedan od satelita je *BIG BIRD*, koji kružeći oko zemlje snima fotografije u niskoj orbiti;

Carnivore je sustav koji je uspostavio FBI, a koji je dizajniran kao nadzorni program za *e-mail* i elektroničke komunikacije.[59] Upotrebljava se kao *packet sniffer* koji može nadzirati sve mete kroz internetske komunikacije. Nasljednik programa *Carnivore* je *NarusInsight* vodeći program koji u realnom vremenu mrežnog prometa pruža usluge istraživanja i analize podataka, zatim situacijske svijesti u *cyber*-okolini;[60]

Dishfire je tajni globalni sustav za nadzor i prikupljanje baze podataka koju vodi *NSA i GCHQ*; sustav prikuplja stotine milijuna *SMS* poruka na dnevnoj bazi iz cijelog svijeta. Sustav u vezi zove se *Prefer*;

MWSN je program vlade SAD-a za nadzor svih komunikacija kako domaćih tako i stranih, u borbi protiv terorizma na Bliskom istoku, kojeg je poslije zamijenio program *TIA*;[61]

StoneGhost je tajno ime za operativnu mrežu za razmjenu podataka između MO SAD-a i UK-a, Kanade, Australije i kasnije Novog Zelanda;[62]

Tempora je kodno ime za bivši tajni Dkompjutorski sustav koji je upotrebljavao *GCHQ* koji se koristi za pohranu podataka iz optičkih kablova tako da oni mogu biti obrađeni kasnije po potrebi;[63]

Frenchelon je preslikan sustav *Echelon* od strane *DGSE*, za istraživanje terorizma u komunikacijskim kanalima zemaljskih i satelitskih stanica od strane Francuske;[64]

---

[59] Izvor: www.fbi.govFederal Bureau of Investigation, Carnivore je nastao 1997. ali je 2005. zamijenjen sa programom NarusInsight. – pristupljeno: 10.12.2014.

[60] Izvor:http://www.marketwired.com/press-release/Narus-Announces-Latest-Product-Upgrade-NarusInsight-8-Traffic-Intelligence-Analytics-1628722.htm – p ristupljeno: 10.12.2014.

[61] Izvor: http://www.palgrave.com/resources/sample-chapters/9781137426215_sample.pdf str.13. – pristupljeno: 10.12.2014.

[62] Izvor: https://bandcamp.com/copyright StoneGhost, Tajno nazvano Five eyes (pet očiju). – pristupljeno: 10.12.2014.

[63] Harding L., *The Snowden files*, The Guardian, London, 2014, str. 63.-70.

[64] Izvor: http://www.zdnet.com/article/frenchelon-france-has-nothing-to-envy-in-echelon/ Frenchelon, Posjeduje desetak stacionarnih stanica na različitim lokacijama po svijetu, neke od njih su: Saint-Barthélemy, Bouar, Djibouti, Camp Lemonnier, Combined Joint Task Force – Horn of Africa, Mayotte,Réunion, Kourou i New Caledonia. – pristupljeno: 10.12.2010.

Fairview je tajni program za masovna nadziranja građana stranih zemalja pokrenut od strane *NSA*, a radi prikupljanja podataka iz telefona, interneta, e-mail podataka i sadržaja poruka u paketu iz kompjutora i mobilnih telefona;[65]

Mystic sustav za cjelokupno snimanje telefonskih razgovora po cijelom svijetu koji pohranjuje podatke u bazu iz koje mogu povući podatke unazad do 30 dana, omogućavajući analitičarima ulazak u sadržaj prošlih razgovora;[66]

PRISM je tajni antiteroristički program za masovni elektronički nadzor. Pokrenut je 2007. godine od strane *NSA*, uz sudjelovanje *GCHQ*. *PRISM* program prikuplja pohranjene internetske komunikacije na temelju zahtjeva koji su napravljeni na kompjutorskim tvrtkama kao što su Google Inc. i slične;[67]

ADVISE je program američke vlade, koja radi na razvoju ogromnog kompjutorskog sustava koji može prikupljati masovne količine podataka i međusobno ih povezivati u potrazi za obrascima terorističkih komunikacija i aktivnosti. Taj sustav je dijelom već operativan, dok je dio još uvijek u razvojnoj fazi. On sam može tragati za korelacijama između blogova i elektroničke pošte, s jedne strane i datoteka raznih vladinih agencija i obavještajnih službi, s druge. Nazvan skraćenicom *ADVISE* – prema *Analysis, Dissemination, Visualiration, Insighti, Semantic, Enhancement*, taj sustav će obavljati masovne pretrage internetskih komunikacija i svoje unakrsno povezane podatke pohranjivati kao "entitete". Tih entiteta, kako procjenjuju stručnjaci, bit će u redu vrijednosti od trilijuna. Svi programi nadzora suočavaju se s jednim velikim problemom, a to je nemogućnost obrade velike količine podataka koji se dnevno pohranjuju od strane ovih monitoring sustava;[68]

U istočnoj hemisferi kod Ruske Federacije imamo projekte kao što je *SORM*. To je ruski tehnički sustav za pretraživanje i nadzor na internetu. Primjenu je ostvario zakonom donesenim 1995. godine, koji omogućuje ruskoj FSB službi nadzor i praćenje telefonskih i internetskih komunikacija;[69]

SORM1 je sustav koji je uspostavljen 1996. za praćenje fiksnih i mobilnih telefonskih komunikacija, izdvojen je iz sustava SORM kao zaseban segment;[70]

SORM2 je odgovoran za presretanje internetskog prometa uključujući i VoIP;[71]

SORM3 prikuplja informacije iz svih komunikacijskih medija, i nudi dugoročnu pohranu (tri godine), pruža pristup svim podacima pretplatnika.[72] Osim toga, omogućava korištenje mobilnih kontrolnih točaka, preko svog uređaja koji može biti priključen izravno na komunikacijskom čvorištu i može odmah presresti i snimiti promet na memorijski prostor.

---

[65] Harding, L., 2014, *The Snowden files*, The Guardian, London, str. 63.-70.
[66] Izvor: https://www.schneier.com/blog/archives/2014/03/mystic_the_nsas.html – pristupljeno: 10.12.2010.
[67] Harding, L., 2014, *The Snowden files*, The Guardian, London, str. 63.-70.
[68] Ibid.
[69] Izvor: http://www.tadviser.ru/index.php, Система Оперативно-Розыскных Мероприятий, – pristupljeno: 10.12.2014.
[70] Harding L., 2014, *The Snowden files*, The Guardian, London, str. 63.-70.
[71] Ibid.
[72] Ibid.

SORM3 može uzeti podatke u bilo kojoj mreži i s njihovih servera, a također se upotrebljava za pohranu podataka s društvenih mreža koje imaju sjedište u Rusiji;

Nadzor telekomunikacija u Rusiji, prema podacima kojima raspolažemo. obavlja operativac *FSB,* koji mora imati nalog za to, ali ga istovremeno ne mora pokazati nikome. *ISP*[73] zakonom su obvezni i moraju platiti za montažu *SORM* opreme preko koje *FSB* ulazi i kontrolira njihov sustav komunikacija i za to ne moraju tražiti nalog suda. Kao što vidimo sustav *SORM* je samostalan sustav za nadzor i *FSB* ne treba kontaktirati osoblje *ISP*. U sjedištu *FSB* koji je zaštićenim vodovima izravno je povezan sa *SORM* uređajima koji su instalirani na svim čvorištima *ISP* širom zemlje. U svakom ruskom gradu postoje zaštićeni podzemni vodovi koji povezuju sjedište lokalnog *FSB* odjela sa svim *ISP* telekomunikacijskim uslugama u regiji. Veliku sličnost *SORM* sustavu je imao bivši sustav sigurnosti Jugoslavije, koji se koristio razdjelnicima poštanskih telefonskih centrala, kako bi mogli imati nadzor i bez poštanskih službenika. Sličnost sustava je bila u pristupu zaštićenim vodovima koji su izravno povezani s telefonskom centralom fiksnih telefonskih linija. U to vrijeme nisu postojali mobilni telefonski uređaji niti je postojala razmjena informacija kompjutorskim putem, ali su postojale *telex*-centrale i teleprinterski promet, koji je također mogao biti nadziran. Pandan ruskom *SORM* sustavu je američki *PRISM,* o kojem je prethodnih godina puno pisano i govoreno.[74] Nakon 9/11 *NSA* je, kako kažu, postala arogantna i nepredvidiva. U svojim redovima uzgajala je programske stručnjake koji su uspjeli prodrijeti u programske sheme mobilnih telefona koji koriste različite operativne sustave, od iPhonea do Blackberryja i android operativnog sustava. Istovremeno su zavladali internetom i unutar agencije se znalo da raspolaže podacima govorne pošte, slika i poruka koje su prolazile kroz: *MicroSoft*[75], *Yahoo*[76] i *Google*[77]. Pored njih, u idućem razdoblju su *NSA-u* pristupile i druge velike korporacije kao što su: *Facebook*[78], *Paltalk*[79], *Youtube*[80], *Skype*[81] i *AOL.*[82] Dugo poslije je pristupila i korporacija *Apple*[83], a prije vrlo kratkog vremena i *Dropbox*[84], *Twitter*[85], i započeli su pregovori s operativnim sustavom *Linux.*[86] Sustavom *PRISM* sve ove korporacije regrutirane su od strane *NSA,* kojoj su osigurale neometan pristup svojim podacima izravno sa servera, vezanim za podatke o pojedincima redovnih mušterija ili pak *Orwelove* mase bezumnih radnika.

---

[73] Izvor: http://searchwindevelopment.techtarget.com/definition/ISP Pružatelj_internetskih_usluga, Internet service provider – pristupljeno: 10.12.2014.
[74] Harding, L., 2014, *The Snowden files,* The Guardian, London, str. 165.-170.
[75] Pristupio NSA 09/2007.
[76] Pristupio NSA 03/2008.
[77] Pristupio NSA 01/2009.
[78] Pristupio NSA 06/2009.
[79] Pristupio NSA 12/2009.
[80] Pristupio NSA 09/2010.
[81] Pristupio NSA 02/2011.
[82] Pristupio NSA 03/2011.
[83] Pristupio NSA 10/2012.
[84] Pristupio NSA 10/2013.
[85] Pristupio NSA 11/2013.
[86] zatražen pristup od nsa 11/2013., raspravljano na eu parlamentu 12/2014., linus torvalds was approached by nsa for backdoor in linux - nils torvalds (father of linus). izvor: https://www.youtube.com/watch?v=wwryywn7beo – pristupljeno: 30.12.2014.

Način na koji *NSA* pristupa podacima *PRISM* sustava je opisan u nekoliko koraka i objavljen na stranicama *Washington posta.* Prvi je složena procedura "zadavanje zadatka" - pronađi novu metu nadzora, potom nadzornik u *PRISM* pregleda ključne riječi za pretraživanje koje je naveo analitičar (odrednice). Zatim nadzornik prihvaća opravdanu sumnju da meta živi izvan *SAD-a,* a oprema iz pristupnih korporacija zajedno s podacima iz *FBI-a* se odobri i dostavlja pretražene podatke *NSA*, koje onda obrađuje niz analitičkih aplikacija, kao što su *MARINA*[87], koja filtrira i skladišti podatke s interneta, uz prikupljene podatke o telefonskim pozivima aplikacije *MAINWAY*[88], pa *PINWALE*[89] podaci o videosnimcima i na kraju *NUCLEON*[90], za govornu poštu. Nakon određivanja mete, *NSA* ima pristup podacima u realnom vremenu i agencija automatski dobiva obavijest kad meta pošalje *e-mail, SMS*, primi ili pošalje telefonski poziv ili pak samo uključi kompjutor, dok dobar dio podataka iz sustava *PRISM* završi u kabinetu predsjednika *Obame* u vidu analitičkog presjeka. Gotovo istovremeno *NSA* obavlja dijeljenje informacija s pojedinim partnerskim službama prema pravilu "potrebno da zna" koje završi i u njihovim agencijama;

Pored navedenih aplikacija uz *PRISM* sustav se nalazi još niz posebnih programa za nadzor, a odnose se na prikupljanje informacija iz komunikacije optičkih kablova i infrastrukture dok prolaze kroz njih. Program nazvan *UPSTREAM*[91] je paralelan programu *Tempora,* britanske agencije *GCHQ*. Navedenu aplikaciju, koju *NSA* koristi preko *PRISM* sustava, spaja na četiri nadzorna programa od kojih su *FAIRVIEW*[92], *BLARNEY*[93] i *STORMBREW*[94] zaduženi za prikupljanje informacija unutar granica *SAD-a*, dok je program *OAKSTAR*[95], koji sadrži osam potprograma i djeluje poput kišobrana čime odbija višak informacija koje prolaze komunikacijskim kanalima izvan *SAD-a*. Prikupljanje internetskih podataka putem *Upstream* aplikacije može biti obrađeno kroz *XKEYSCORE* aplikaciju kojom

---

[87] izvor: http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents, nsa stores metadata of millions of web users for up to a year, secret files show. – pristupljeno: 30.12.2014.

[88] izvor: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/nsa slides explain the prism data-collection program – pristupljeno: 10.07.21013.

[89] izvor: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/nsa slides explain the prism data-collection program – pristupljeno: 10.07.21013.

[90] izvor: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/nsa slides explain the prism data-collection program – pristupljeno: 10.07.21013.

[91] izvor: https://www.aclu.org/blog/national-security/guide-what-we-now-know-about-nsas-dragnet-searches-your-communications; a guide to what we now know about the nsa's dragnet searches of your communications, – pristupljeno: 08.09.2013.

[92] izvor: http://www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/; forget prism: fairview is the nsa's project to "own the internet", – pristupljeno: 12.07.2013.

[93] izvor: http://electrospaces.blogspot.com/2013/09/prism-as-part-of-blarney-program.html prism as part of the blarney program, – pristupljeno: 21.09.2013.

[94] izvor: http://www.washingtonpost.com/business/economy/the-nsa-slide-you-aventseen/2013/07 /10/32801426 -e8e6-11e2-aa9f-c03a72e2d342_story.html; nsa slide shows surveillance of undersea cables, – pristupljeno: 10.07. 2013.

[95] izvor: http://www.dailydot.com/politics/nsa-spy-prgrams-prism-fairview-blarney/; the definitive guide to nsa spy programs, – pristupljeno: 14.08.2013.

se obavlja indeksiranje analiziranog sustava.[96] Također, *TRAFFICTHIEF* je baza metapretraživača iz podskupa zaduženih da iz pretrage izvuku *metapodatke*;[97] *BOUNDLESS INFORMANT je* alat kojega koristi *NSA* za veliku analizu i vizualizaciju podataka kojom dalje menadžeri agencije prave sažetke u vidu izvještaja za brojčanu aktivnost *meta-podataka* prikupljenih preko izvora u partnerskim službama i putem *www*.[98] Kao što vidimo, sve sa *NSA* ugovorene korporacije i veći korisnici, zatim *web*-stranice i pojedinci koji provode vrijeme na internetu imaju svoj dosje u bazama podataka *NSA*. Iako nikad nije uveden zakon o cenzuri na internetu, to sada više nije ni neophodno, jer dovoljno je razloga da pretpostavimo da *SAD* nadzire kao veliki brat uz *PRISM* sustav i druge brojne aplikacije. Isto tako, već smo rekli da ruski *FSB* koristi *SORM* sustav bez znanja *ISP*, praktično kad god mu je potrebno. Uvidjevši nadzorne sustave, njihovu brojnost, snagu i sposobnost, nije nam jasno da se *cyber*-terorizam uopće vidi na internetu i da ima toliki utjecaj. Jasno da i pored velikog brata postoje određene rupe u sustavu i da jednostavno nije dovoljno učinkovit.

2. PROBLEMI SUSTAVA NADZORA U OBRANI OD *CYBER*-KRIMINALA

Pored velikih sustavnih projekata nadzora nije jasno kako *cyber*-teroristi uspijevaju opstati u *cyber*-prostoru. Jedan od najvećih problema naslijeđenih iz prošlog stoljeća je fleksibilna struktura terorističkih organizacija i njihova sposobnost adaptacije, što je za rezultat imalo sve veće korištenje *cyber*-tehnologije kao rezultat te adaptacije. U ovom kontekstu su u borbi protiv *cyber*-terorizma od ogromne važnosti suradnja, razmjena informacija i koordinacija među nacionalnim institucijama i organizacijama sa svrhom otkrivanja i eliminacije prijetnje, otklanjanja tajnosti i jačanja integriteta njihovih informacijskih sustava i usluga. Prvi problem je što je prethodnih godina *cyber*-terorizam prerastao u jednu od glavnih prijetnji globalnoj sigurnosti kroz uspješno prilagođavanje novoj ekonomskoj i političkoj realnosti međunarodnih odnosa čime je prešao na viši stupanj razvoja. Za manje od jednog desetljeća terorističke grupe su prešle od hijerarhijskih na mrežne strukture, koje se postupno razvijaju u globalni pokret, što pokazuje i ujedinjavanje u pokret ISIL. U kontekstu globalizacije uloga modernih informacijskih tehnologija u međunarodnom terorizmu koja je postala izuzetno velika, terorističke i ekstremističke organizacije sve češće primjenjuju ove tehnologije kao oblik i metodu radikalnih i terorističkih aktivnosti. Tako se ovaj novi fenomen i koncept javlja kao ozbiljna prijetnja svjetskoj sigurnosti u *cyber*-prostoru kroz *cyber*-terorizam, *cyber*-rat, *cyber*-napad, itd. Kada je riječ o *cyber*-terorizmu danas postoji realna opasnost da informatički resursi, a posebno globalne informatičke mreže postanu i veoma učinkovito sredstvo počinjenja u rukama terorista, omogućivši im načine djelovanja o kojima ranije nisu mogli ni sanjati. Ambiciozni projekti za nadzor komunikacija, suočili su se s predvidljivim preprekama:

---

[96] izvor: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/; nsa slides explain the prism data-collection program – pristupljeno: 10.07.21013.

[97] izvor: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/; nsa slides explain the prism data-collection program – pristupljeno: 10.07.21013.

[98] izvor: http://www.brookings.edu/blogs/up-front/posts/2013/06/13-prism-boundless-informant-nsa-surveillance-lempert; prism and boundless informant: is nsa surveillance a threat? – pristupljeno: 10.06.2013.

- nemogućnost procesuiranja velike količine podataka koje dnevno pohranjuje nadzorni sustav,
- poteškoće u identifikaciji vrste aktivnosti koje ne bi smjele biti u suprotnosti ili ograničavati ljudska prava,
- razvoj novih sustava sigurne komunikacije.

Drugi problem nadzora je sam tempo kojim problemi sigurnosti mreža vrlo brzo prerastu sposobnosti nadzora i nadzornih tijela da ih kontroliraju. Naročito zabrinjavajuće je kada se imaju u vidu njene implikacije na prava na privatnost, slobodu izražavanja i udruživanja. Pokušaji izgradnje sustava za kontrolu međunarodne razmjene podataka često su se suočavali sa žestokim otporom privatnih aktera i njihova suradnja s državama u ovoj oblasti je najčešće iznuđena. Razlog za zabrinutost predstavlja i činjenica da postoji ključna tenzija između zaštite privatnosti i poboljšane identifikacije i provjere identiteta korisnika. Ovo svojstvo *cyber*-sigurnosti, teškoće i tehnološka ekspertiza neophodna za identifikaciju online "negativaca", izravno su doveli do drugog problema: činjenice da države i tvrtke često bez odgovarajućeg demokratskog nadzora skupljaju i obrađuju veliku količinu osobnih i privatnih podataka, a radi vlastite sigurnosti. Problem se dodatno pogoršava time što mnoge države nemaju zakone koji reguliraju ovu oblast ili ih imaju vrlo malo. U mnogim od ovih pravnih sustava, čak i kada bi postojala politička volja, ne postoje tehnološki kapaciteti neophodni da se napravi i sprovede takav zakon, čak i kada bi postojao. Odsustvo zakonodavstva i kapaciteta znači da kriminalci mogu anonimno pristupiti internetu iz siromašne zemlje i da u inozemstvu nekažnjeno čine kaznena djela. Kako su online prijetnje po svojoj prirodi često internacionalizirane, također mogu biti neophodna transnacionalna partnerstva.[99] Problemi postaju još izražajniji negoli na nacionalnom planu pa su zajedničke politike i pristupi među regionalnim i međunarodnim akterima još uvijek nedovoljno razvijene. Probleme dodatno otežava to što u sposobnostima po pitanju opreme, stručnosti i, posebno, institucija i nadzora između država postoji veliki jaz, koji će se sve više produbljivati. Javno-privatna suradnja koja je neophodna za sveobuhvatnu i učinkovitu *cyber*-sigurnost, povlači za sobom komplicirana i još neriješena pitanja koja se odnose na nadzor i odgovornost i, naročito, na osnovna prava poput prava na privatnost, slobodu izražavanja i udruživanja. Izazovi koji se tiču *online* sigurnosti stvaraju tenziju između sigurnosti države i sigurnosti pojedinca, s dodatnom dimenzijom moćnih privatnih aktera koji imaju svoje vlastite motive i prioritete. Budući da *online* sigurnost u mnogim državama predstavlja relativno nov problem za aktere na polju sigurnosti, nije još uvijek izgrađen demokratski nadzor, u vidu ombudsmana, parlamentarnih odbora i drugih specijaliziranih tijela koja se s pitanjima sporo hvataju ukoštac. Sve mreže podrazumijevaju suradnju između vlada, privatnog sektora, nevladinih i međunarodnih organizacija, koja akterima omogućava korištenje zemljopisnih, tehnoloških i znanstvenih resursa koje oni sami ne bi mogli osigurati. Države se "spuštaju" ka tvrtkama, dok se one "penju" ka državi. Primjer ovoga je skorašnji

[99] Buckland, B. S./ Schreier, F./ Winkler, T. H., 2010, *Demokratsko upravljanje izazovi cyber bezbednosti*, Forum za sigurnost i demokratiju, DCAF, str. 18.-23.

sporazum o suradnji između *Googlea, Yahooa, Facebooka, Twittera* i drugih privatnih tvrtki i *NSA* SAD.[100]

Suočene kako sa tradicionalnim, tako i sa netradicionalnim sigurnosnim izazovima, države su, djelujući same, loše opremljene. Problemi nadzora pogoršani su iz više razloga, a jedan od njih proizlazi iz razloga *kompleksnosti mreže,* jer je u prostor *cyber*-sigurnosti uključen veliki broj državnih, privatnih, međunarodnih i drugih nedržavnih aktera. Također, probleme nadzora pogoršava i *tehnička kompleksnost*, te činjenica da izrazito tehnička priroda izazova *cyber*-sigurnosti i odgovora na nju, koja je u suprotnosti s činjenicom da nadzorna tijela često nemaju neophodnu stručnost da ih razumiju i odgovarajuće nadziru. Zatim, probleme nadzora pogoršava *pravna kompleksnost*, jer *cyber*-sigurnost nas suočava s kompleksnim pravnim pitanjima koja se odnose na pravo privatnosti i slobodu izražavanja. Isto tako, probleme nadzora mreža pogoršava *heterogenost aktera*. U većini slučajeva, institucije nadzora su organizirane kao agencije ili funkcionalno slična tijela. Tako parlamentarni odbor može nadgledati obavještajne službe i aktivnosti, oružane snage i pravosuđe, ali im to ne daje za pravo nadgledanja mreže privatnih firmi. Problem nadzora pogoršavaju *percepcije mandata,* jer gledano generalno, državna nadzorna tijela se staraju o državnim agencijama za čiji rad su izravno odgovorne. Ovo ostavlja privatne partnere takvih agencija izvan dometa nadzora. Isto tako važan problem nadzora pogoršava *narušavanje odnosa nadređeni/službenik*. Postupci svakog državnog službenika povezani su lancem odgovornosti. Od nadređenog ka službeniku postoji lanac odgovornosti i nadzora između demokratskih institucija i pojedinaca ili agencija koje sprovode državne direktive.[101]

3. ZAKLJUČAK

Kao što vidimo, ni ovi ogromni projekti nisu svemogući i neosporna je činjenica da internet prerasta u globalnu informacijsku infrastrukturu. Njegovo korištenje maksimalno je olakšano za tipičnu korisničku populaciju širom svijeta, zahvaljujući, prije svega, multimedijskom servisu *www* i programima za pretraživanje, kao što su *Google, Yahoo, Ixquick, Duckduckgo* i dr., koji su omogućili korisnicima bliske, grafički orijentirane načine pristupa.[102] Na jedan ili drugi način, internet utječe ili će utjecati na naš život izrazito snažno. On fundamentalno mijenja način društvenog života i rada osiguravajući jeftin medij za dobivanje informacija i međusobnu komunikaciju. Rastući skup servisnih usluga, koje uključuju elektroničku poštu, elektroničke publikacije, elektroničke oglasne table, digitalne biblioteke, videokonferencije, diskusijske grupe, transakcije, zabavu i dr., pretvara ovaj digitalni univerzum u vitalni resurs koji pruža korisnicima nove načine komuniciranja, informiranja, obrazovanja, rada i zabave.[103] Vidimo da je nemoguće obavljati globalni nadzor i "velikog brata", bez obzira na to koliko novca odvojili za to. Jedno je sigurno, a to je da će te

[100] Harding, L., 2014, *The Snowden files*, The Guardian, London, str. 63.-70.
[101] Buckland, B. S./ Schreier, F./ Winkler, T. H., 2010, *Demokratsko upravljanje izazovi cyber bezbednosti*, Forum za sigurnost i demokratiju, DCAF, str. 18.-23.
[102] Petrović, S. R., 2000, *Kompjuterski kriminal*, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, str. 71.
[103] Ibid.

sustave biti potrebno obnavljati i proširivati kako bi bar djelomično zadovoljili potrebe za suzbijanjem štetnih pojava na internetu, kao što je i ova – *cyber*-terorizam.

LITERATURA

Babić, V. (2009). *Kompjuterski kriminal.* Sarajevo: Rabic.
Babić, V. (2013). *Dječja pornografija i Internet – Interdisciplinarni ogledi.* Vitez: Fojnica.
Babić, V. (2015). *Cyber terorizam – suvremena sigurnosna prijetnja*, Novi Travnik: Grafid.
Beggs, C. (2010). *Safeguarding Infrastructure Assets from Cyber-terrorism*. NY: Lambert Academic Publishing.
Buckland, B.S., Schreier, F., Winkler, T.H. (2010). *Demokratsko upravljanje: izazovi cyber bezbednosti.* Forum za sigurnost i demokratiju, DCAF.
Harding, L. (2014). *The Snowden files.* London: The Guardian.
Hoskins, A., Awan, A., O'Loughlin, B. (2011). *Radicalisation and the Media: Connectivity and Terrorism in the New Media.* New York: 270 Medison av.
Hsinchun C., Thoms, S., Tianjun F. (2008). Cyber extremism in Web 2.0: An exploratory study of international Jihadist groups. Tucson: Artificial Intell. Lab., Arizona University.
Mobley, W.B. (2012). *Terrorism and Counter-intelligence: How terrorist groups elude detection.* LA: Columbia Unievrsity.
Petrović, S.R. (2000). *Kompjuterski kriminal*. Beograd: Ministarstvo unutrašnjih poslova Republike Srbije.

Internetski izvori

https://www.nsa.gov/
http://www.gchq.gov.uk/Pages/homepage.aspx
www.fbi.gov
http://www.marketwired.com/press-release/Narus-Announces-Latest-Product-Upgrade-NarusInsight-8-Traffic-Intelligence-Analytics-1628722.htm
http://www.palgrave.com/resources/sample-chapters/9781137426215_sample.pdf str.13.
https://bandcamp.com/copyright StoneGhost
http://www.zdnet.com/article/frenchelon-france-has-nothing-to-envy-in-echelon/Frenchelon
https://www.schneier.com/blog/archives/2014/03/mystic_the_nsas.html
http://www.tadviser.ru/index.php
http://searchwindevelopment.techtarget.com/definition/ISP Pružatelj_internetskih_usluga
https://www.youtube.com/watch?v=wwRYyWn7BEo
http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents
http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
https://www.aclu.org/blog/national-security/guide-what-we-now-know-about-nsas-dragnet-searches-your-communications
http://www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/
http://electrospaces.blogspot.com/2013/09/prism-as-part-of-blarney-program.html
http://www.washingtonpost.com/business/economy/the-nsa-slide-you-aventseen/2013/07/10/32801426 -e8e6-11e2-aa9f-c03a72e2d342_story.html
http://www.dailydot.com/politics/nsa-spy-prgrams-prism-fairview-blarney/
http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

http://www.brookings.edu/blogs/up-front/posts/2013/06/13-prism-boundless-informant-nsa-surveillance-lempert.

Vladica Babić

Zdravko Skakavac

SURVEILLANCE SYSTEMS OF MODERN TECHNICAL DEVICES AND THEIR EFFICIENCY

Summary

Despite enormous efforts to establish a system of control and possibilities of using a seemingly endless choice of different methods and ways that cyber criminals are using to infiltrate computer networks, government, international organizations and private industry, it is clear that there is an urgent need to take a series of steps in the upcoming years in the field of law, politics and technology for data protection, and to repress all these, more and more frequent occurrences in cyberspace. For this purpose, it is necessary to involve all segments of security and regulate the legal framework, adopt international conventions and technical standards. Recommended steps toward international cooperation are mandatory, they should be taken and constantly improved, csince none of these steps cannot completely make the Internet a safe place and repress the cyber crime on the whole.

Key words: *Cyber crime, video-surveillance, cyber space.*

STRUČNI RAD

Alen Sambolec[104]

Davor Solomun[105]

IMINT I ZRAKOPLOVNA TEHNOLOGIJA PRIKUPLJANJA PODATAKA I SIGURNOSNOG DJELOVANJA

Sažetak

U radu se analiziraju različiti aspekti IMINT („imagery intelligence“) tehnologije, kao metode suvremenog obavještajno – sigurnosnog djelovanja. Posebice se prikazuje uloga zrakoplovstva u fazi prikupljanja podataka, kao i tehnologija stvaranja slikovnih zapisa iz zraka – satelitom, zrakoplovom i bespilotnim letjelicama. IMINT metoda neizostavno prethodi svakoj današnjoj sigurnosnoj operaciji, od ratnih djelovanja međunarodnih i NATO snaga u Iraku, Afganistanu, Siriji ili Jemenu, do globalne borbe protiv terorizma i likvidacije samog Osame Bin Ladena u Pakistanu.

Pored tehnoloških određenosti, rad problemski tematizira neadekvatnu zakonsku uređenost u suvremenoj primjeni IMINT-a, te se analiziraju stavovi i reakcije svjetskih medija i vodećih sila na upotrebu suvremenih IMINT platformi, prije svega američkih dronova.

Istraživanje primjenjivosti ove metode u ostvarivanju sigurnosti Republike Hrvatske i komparativna analiza doprinosa zaštiti vanjskih granica Europske unije, krajnji je cilj, a implementacija novog helikoptera AgustaWestland AW139, u floti Zrakoplovne jedinice specijalne policije Ministarstva unutarnjih poslova Republike Hrvatske, predstavlja poseban izazov u ovome radu.

Ključne riječi: *IMINT, špijunski zrakoplov, bespilotna letjelica, obavještajno – sigurnosno djelovanje.*

1. UVOD

Informacijsko doba, koje globalno određuje društveni, a posebice tehnološki razvoj, inoviralo je i oplemenilo brojne znanstvene i stručne discipline. Informacije i sigurnost oduvijek su međuovisni. Informacije u funkciji sigurnosti posebice su važan aspekt toga odnosa, bilo kao instrument kreatora i pružatelja sigurnosti ili kao potreba njenih uživatelja i korisnika.

[104] Alen Sambolec, ing. aeronautike / stručni spec. crim., pilot helikoptera/voditelj programa sigurnosti letenja (Safety Manager), Zapovjedništvo specijalne policije, Zrakoplovna jedinica, MUP RH, alen.sambolec@gmail.com

[105] mr. sc. Davor Solomun, viši predavač i voditelj Centra za policijska istraživanja na Visokoj policijskoj školi u Zagrebu. dsolomun@fkz.hr

Suvremene informacijske tehnologije, čini se, približavaju nas idealnim stanjima *upotrebljivosti relevantnih informacija u realnom vremenu njihova nastanka*. Službama odgovornim za sigurnost država, građana i društava, to je imperativ jer zakašnjela ili netočna informacija pogoduje nesigurnostima.

U širokom spektru načina i tehnologije prikupljanja informacija, središnje je pitanje odabira odgovarajuće metode, odnosno njene učinkovitosti na spram predmeta informacijskog ili obavještajnog interesa.

Iako se kombiniranje metoda smatra školskim pristupom, određeni uvjeti i predmeti obavještajnog interesa ipak zahtijevaju preferiranje onih s naglašenim ljudskim čimbenikom dok su određene situacije nezamislive bez sofisticiranih tehničkih sredstava.

U uvjetima suvremenih prijetnji, ugroza i nesigurnosti, od ilegalne trgovine i krijumčarenja, terorizma, migracija i ratova do globalnih klimatskih i prirodnih tijekova, presudnom se čini uporaba tehnologije stvaranja informacija iz zraka. Zrakoplovstvo i tehnologija stvaranja slikovnih zapisa putem satelita ili bespilotnih letjelica utjelovljuju IMINT („imagery intelligence“) obavještajnu metodu.

Tehnološke savršenosti sredstava i uređaja u funkciji stvaranja snimaka iz zraka, središnja su kategorija ovoga rada. Analiza primjenjivosti ove metode u ostvarivanju sigurnosti Republike Hrvatske i ocjena doprinosa zaštiti vanjskih granica Europske unije, krajnji je cilj, a implementacija novoga helikoptera AgustaWestland AW139, u floti Zrakoplovne jedinice specijalne policije Ministarstva unutarnjih poslova Republike Hrvatske, empirijska je potvrda i predstavlja poseban izazov ovoga rada.

2. POJAM, OKRUŽENJE I RAZVOJ IMINT-A

Obavještajne institucije podatke prikupljaju na tajni način i iz otvorenih (Open Source Intelligence-OSINT), svima dostupnih i legalnih izvora.[106] Tajnim putem informacije se prikupljaju posredstvom ljudskih izvora (Human Intelligence-HUMINT) te tehničkim putem, odnosno kontrolom različitih sredstava veze koja emitiraju određene signale, a što se naziva skupnim imenom SIGINT – Signal Intelligence. Veliki broj podataka koji se slijevaju u sjedišta obavještajnih institucija obrađuje se na jednom mjestu te se potom izrađuju odgovarajuće analize, pri čemu se ocjenjuje stupanj točnosti i stupanj pouzdanosti izvora tih informacija (Bilandžić, 2008: 40).

HUMINT, prikupljanje podataka iz ljudskih izvora, putem informacija prikupljenih od strane obavještajaca u stranim državama, kroz povijest se pokazao poroznim. Državne tajne velikih sila odavale su se drugim državama, motiviranošću, prije svega, ideološkim razlozima njenih vlastitih pripadnika. S druge strane, prikupljanje podataka tehničkim sredstvima postalo je iznimno sofisticirano. I poželjno, jer je eliminiran ljudski faktor iz procesa, što je značilo puno viši stupanj pouzdanosti. Špijunski avioni, bespilotne letjelice, satelitski nadzor, kompjutorska

[106] https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html , preuzeto 01.02.2014.

kriptografija, uređaji za dobivanje različitih vrsta slike i slično, promijenili su načine na koji se prikuplja veći dio obavještajnih podataka, i primat prepustili disciplinama kao što su:

- TECHINT (Technical Intelligence), obavještajna djelatnost posredstvom tehničkih sredstava; prvotno se pojam odnosio na informacije o sustavima naoružanja a danas se odnosi na obavještajne podatke koji su prikupljeni presretanjem različitih elektroničkih signala upotrebom sofisticiranih tehničkih sredstava,
- SIGINT (Signal Intelligence), elektroničko prikupljanje podataka; sve vrste informacija prikupljene putem različitih elektroničkih uređaja, uključujući slijedeće poddiscipline:
- IMINT (Imaginery Intelligence), prikupljanje obavještajnih podataka analizom slika dobivenih različitim oblicima snimanja – fotografske ili digitalne slike prikupljene pomoću orbitalnih (satelitskih) ili kopnenih (avioni ili bespilotne letjelice) sustava, tema daljnjeg istraživanja ovog rada,
- PHOTINT (Photographic Intelligence), prijašnji termin za IMINT, a koristi se za opis fotografija s filma i digitalnih fotografija snimljenih satelitom ili bespilotnim letjelicama,
- RADINT (Radar Intelligence), informacije dobivene upotrebom radarskih signala odaslanih iz nadzemnih satelita, letjelica ili kopnenih izvora (SAR-SyntheticAperture Radar Systems), podmetoda IMINT-a,
- COMINT (Communication Intelligence), prikupljanje obavještajnih podataka presretanjem i nadziranjem telekomunikacija,
- TELINT (Telemetry Intelligence), prikupljanje obavještajnih podataka analizom telemetrije, presretanje podataka odaslanih tijekom testiranja različitih sustava naoružanja,
- ELINT (Electronic Intelligence), prikupljanje podataka nadziranjem elektronske opreme protivnika, presretanje odaslanih elektroničkih emisija koje proistječu iz oružja i sustava za praćenje,
- MASINT (Measures and Signatures Intelligence), prikupljanje podataka znanstvenom i tehničkom obradom obilježja objekata od obavještajnog značaja, noviji oblik SIGINT-a koji koristi sofisticiranije uređaje koji mogu detektirati materijal koji je korišten u različitim tipovima modernog oružja.

U nastavku teksta, kroz problemski pristup stavit će se naglasak upravo na IMINT metode obavještajnog procesa, istražiti različiti modeli koji se primjenjuju u svijetu trenutno, te analizirati uloga zrakoplovstva u IMINT prikupljanju podataka. Također, predmet istraživanja biti će trenutno najsuvremeniji modeli IMINT metoda – upotreba bespilotnih letjelica u svrhu zračnog fotografiranja (eng. imagery sources).

2.1 Pojam IMINT - Imagery Intelligence

IMINT je obavještajna metoda prikupljanja podataka, koja ima zadatak prikupljati i analizirati podatke dobivene zračnim snimkama ili snimke dobivene putem satelita. IMINT je produkt analiza snimki, i predstavlja osnovni element cjelokupne obavještajne slike. Pod

pojmom „imagery“ (eng. slika, predodžba, slikovit prikaz) podrazumijeva se slikovni prikaz koji uključuje prezentaciju objekata reproduciranih elektroničkim putem ili optičkim sredstvima putem filma, digitalnog zapisa, elektoničkihdisplejeva ili drugih medija. Slikovni zapisi najnovije generacije su ezoterične „imagery“ forme, kao što su infracrvena fotografija (eng. „infrared“, FLIR systems – Forward Looking Infra Red), odnosno termovizijske kamere, ili radarske slike.[107] Ovisno o tipu, slikovni zapisi se interpretiraju (analiziraju) putem posebno obučenih stručnjaka – analitičara, kako bi se dobili upotrebljivi obavještajni podaci.

IMINT uključuje eksploataciju podataka u svrhu detekcije, klasificiranja i identificiranja objekata ili organizacija na zemlji. Može biti proizveden s tvrdog ili mekog (digitalnog) slikovnog zapisa. Pod tvrdim zapisom („hard-copy“) podrazumijeva se film, dok se meki slikovni zapis („soft-copy“) prikazuje na elektroničkim terminalima. Oba tipa ovih „imagery“ izvora mogu biti analizirana i interpretirana u različite svrhe za različite korisnike. U prošlosti, bili su ograničeni isključivo na vojne svrhe, dok se u današnje vrijeme sve više koriste u komercijalne svrhe.[108]

U Sjedinjenim Američkim Državama, analiza podataka dobivenih „Imagery Intelligence“ metodama, vrši se u centrima kao što su National Geospatial Intelligence Agency[109], u gradu Bethesda, savezna država Maryland, ili u bazi američkog zrakoplovstva, National Air and Space Intelligence Center[110], Write-Patterson Air Force Base, grad Dayton, savezna država Ohio. Ova dva centra ključni su elementi američke fotografske analitike, te potpora svim operacijama američke vlade i vodeća dva takva centra u svijetu.

Slika br.1: Analiza snimki iz zraka – IMINT metoda[111]

[107] http://www.intelligence.gov/mission/data-gathering.html , preuzeto 02.02.2014.
[108] http://www.fas.org/irp/nsa/ioss/threat96/part02.htm , preuzeto 02.02.2014.
[109] https://www.nga.mil/Pages/default.aspx , preuzeto 03.02.2014.
[110] http://www.afisr.af.mil/units/nasic/index.asp , preuzeto 03.02.2014.
[111] http://en.wikipedia.org/wiki/Imagery_intelligence , preuzeto 04.02.2014.

2.2. Povijesni razvoj IMINT metode

Korištenje slikovnih zapisa, crteža ili fotografija u obavještajne svrhe ima dugu povijest. Prije izuma fotografije, izviđači – skauti diljem svijeta prepričavali su viđeno svojim vojnim zapovjednicima, i crtali im slike i mape u blatu ili prašini, kako bi im što bolje ilustrirali viđeno. Izumom fotografije 1830. godine, u Američkom Građanskom Ratu bilježe se fotografije neprijateljskih snaga s raznih uzvisina, planina, letećih balona i slično.

Razvoj kamere i filmske tehnologije (manje i brže kamere, s efikasnijim lećama), zajedno s izumom zrakoplova, donose prvo ozbiljnije korištenje zračnog fotografiranja u Prvom Svjetskom Ratu. Slikaju se linije fronti u svrhu taktičkih operacija, te prikupljaju informacije o neprijateljskim tvornicama, lukama, brodogradilištima i brodovima, s ciljem kratkoročnog i dugoročnog strateškog planiranja. Tijekom Drugog Svjetskog Rata bilježi se još ozbiljnija upotreba operacija „imagery intelligence“, gdje britanski RAF koristi posebno razvijen avion Spitfire PRs kojeg je bilo uklonjeno naoružanje i radio-oprema, a ugrađeni dodatni spremnici goriva i pet termo-grijanih kamera koje su omogućavale jako dobre rezultate, s visine od 30.000 stopa, pri brzini od 650 km/h. Odmah nakon Drugog Svjetskog Rata, daljinska („long-range“) zračna izviđanja poduzimana su putem posebno prerađenih mlaznih bombardera, dok Korejski Rat donosi razvoj prvih, posebno dizajniranih i opremljenih zrakoplova („photo-reconnaissance“). Tijekom Hladnog Rata, razvoj strateških mogućnosti SSSR-a doveo je do toga da su obavještajne potrebe prikupljanja podataka SAD-a rezultirale razvojem nekih novih strateških platformi, špijunskih zrakoplova U-2 i SR-71, i nešto kasnije ruskog MIG-25 Foxbat. Ovi zrakoplovi, s ljudskom posadom, i koji su letjeli na ekstremno velikim visinama, bili su specijalno dizajnirani za ulazak u neprijateljski teritorij u svrhu fotografiranja terena. Usporedo s razvojem špijunskih zrakoplova, krajem 50-tih godina prošlog stoljeća započinje era satelita i razvoj tehnologije za prikupljanje „imagery“ obavještajnih podataka iz svemira, koja u kombinaciji sa bespilotnim letjelicama, traje i danas. U tablici 1 prikazani su najznačajniji pripadnici ere špijunskih zrakoplova.

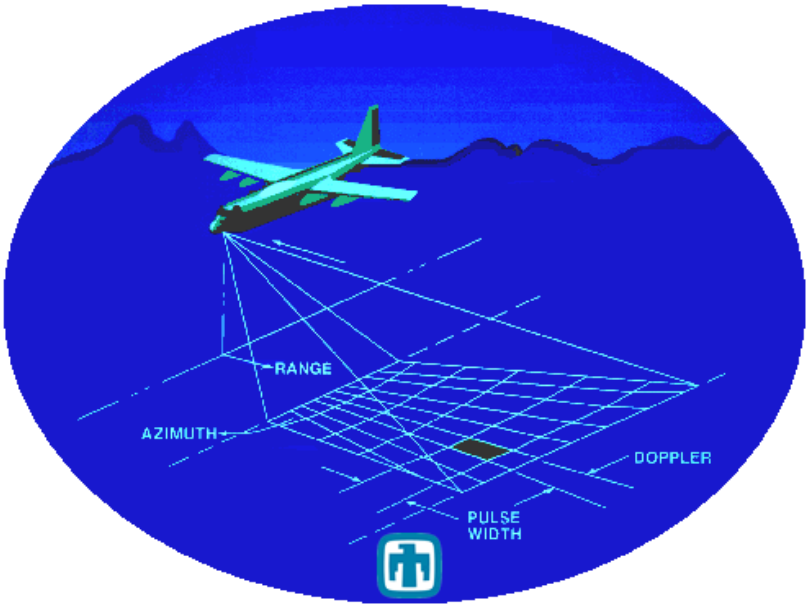
Tablica br.1: Najpoznatiji špijunski zrakoplovi u povijesti

ZRAKOPLOV	GODINA	IMINT ZNAČAJKE
Spitfire PR	1940.-1945.	Prvi pravi izvidničko-špijunski zrakoplov na svijetu, korišten u II Svj. Ratu, RAF, opremljen s 5 termogrijanih kamera, 30.000 stopa, 650 kmh
Lockheed U-2	1960.	Najslavniji špijunski zrakoplov u povijesti, koristi se i danas, snima s visine 21.000 m (70.000 stopa), danju/noću/svi vremenski uvjeti, u prošklosti bio opremljen kamerama, danas najmodernijim SAR/EO/ IC sustavima
Lockheed SR-71 Blackbird	1964. – 1998.	Najbrži špijunski zrakoplov u povijesti (3.3 Mach), s rekordnim plafonom leta 26.000 m (80.000 stopa), korišten u doba Hladnog rata
MIG-25R Foxbat	1970.	Ruski odgovor na SR-71 i U-2, dostizao visinu 24.400 m (78.000 stopa) i brzinu 3.2 Mach, oznaka R označava špijunsko-izvidničku inačicu

2.3. Najznačajniji IMINT satelitski sustavi

Krajem 50-tih godina prošlog stoljeća započela je era satelita i razvoj tehnologije za prikupljanje „imagery“ obavještajnih podataka iz svemira. Upotreba svemirskih letjelica (eng. spacecraft), u prikupljanju slikovnih zapisa iznad zabranjenih, neprijateljskih područja eliminirala je opasnost od napada ili obaranja zrakoplova, ali kreirala puno kompleksnije, skuplje i manje fleksibilne sustave za prikupljanje IMINT podataka. Novija generacija IMINT satelita, kao što je američki Lockheed KH-11 prvi puta je lansirana 1976. godine i koristili su posebno razvijene CCD čipove (eng. charge-coupleddevice) za digitalnu pohranu ultra-ljubičastih snimaka, preteče današnjih digitalnih kamera. U zadnjih 20-tak godina razvijeni su mnogi sustavi koji su značajno unaprijedili „imagery intelligence“ ili prikupljanje

fotografskih obavještajnih podataka. Elektro-Optički senzori (EO/digitalne kamere) ušle su u širu uporabu. Razvojem sintetičkog snimanja odnosno SAR sustava (Synthetic Aperture Radar[112]), omogućeno je nadziranje i snimanje meta i ciljeva na zemlji noću, kroz oblake, odnosno u svim vremenskim uvjetima. SAR slikovni zapisi analitičarima otkrivaju obavještajne podatke koji nisu vidljivi na konvencionalnim fotografijama. Sustav funkcionira na principu odašiljanja radarskih impulsa iz zraka na zemlju, putem nekoliko antena različitih dužina, prikupljanja povratnih signala i njihovog, sintetičkog pretvaranja u digitalnu sliku visoke rezolucije. Danas je IMINT nezamisliv bez SAR/EO/IR sustava, koji se ugrađuju na satelitske sustave, špijunske zrakoplove i bespilotne letjelice, tzv. dronove. Tablica.2 prikazuje neke od najpoznatijih špijunskih satelita koji su se koristili kroz povijest i neke koji se koriste i danas.



Slika br. 2: SyntheticAperture Radar System (SAR)[113]

[112]http://www.radartutorial.eu/20.airborne/ab07.en.html , preuzeto 16.02.2014.
[113]http://www.jaxa.jp/projects/sat/jers1/index_e.html, preuzeto 16.02.2014.

Tablica br. 2: Najpoznatiji IMINT sateliti

SATELIT	GODINA	IMINT ZNAČAJKE
Corona / Gambit	1959.-1984.	Prvi američki satelit iz programa Discoverer-14, koji je 1960. uspješno vraćen iz zemljine orbite, sa snimkama površine Zemlje
Zenit	1961.-1994.	U periodu je SSSR lansirao preko 500 špijunskih film-return satelita serije ZENIT
LandSat MSI	1972.	Prvi Multi Spectral Imagery civilni komercijalni fotografski satelit lansiran od SAD-a
Spot MSI	1986.	Francuski pan-kromatski multi-spectral imagery špijunski satelit
ERS-1	1990.	Europska Svemirska Agencija ESA razvila je svoj sintetički radarski sustav, EO/IR
JERS-1	1996.	Japanski Imagery Satelit, koristi se u prikupljanje podataka na globalnoj razini, opeservaciju zemlje, zaštitu šuma, okoliša, ribarstava, i za slučaj prirodnih katastrofa
YAOGAN-19	2012.	Kineski špijunsko-izvidnički satelit najnovije generacije, prikuplja podatke za potrebe kineske obavještajne službe MCC
Radar Sat-1	1995.	Kanadski špijunski satelit, razvijen vlastitim snagama, SAR sustav
EROS A-1	2003.	Izraelski špijunski imagery satelit, postavljen zajedno sa satelitima QuickBird i OrbView
IKONOS	1999.	Prvi privatni imagery satelit lansiran od strane tvrtke Space Imaging Inc., podružnica tvrtke Lockheed, korišten u pronalaženju Osame Bin ladena

Upravo putem **IKONOS** „imagery intelligence“ satelita, 02. svibnja 2011. godine snimljeno je skrovište Osame Bin Ladena u Pakistanu, i korišteno u pripremi akcije američkih Navy SEAL postrojbi (slika br.3).

Slika br. 3: IKONOS snimka skrovišta Osame Bin Ladena, 02. svibanj 2011.[114]

Značaj IMINT obavještajne metode u današnjem vremenu, i njenu komparativnu prednost u odnosu na ostale metode ne treba posebno naglašavati. Terorističke organizacije u svijetu danas gotovo više i ne koriste radio ili elektronsku komunikacijsku opremu, niti internet, upravo zbog izbjegavanja SIGINT i COMINT metoda prikupljanja obavještajnih podataka od strane svjetskih obavještajnih službi. U globalnom ratu protiv terorizma, obzirom na njegove današnje, ranije spomenute karakteristike – asimetričnost i nekonvencionalnost, kao i nepristupačnost terena na kojima se skrivaju vodeći ljudi Al-Qaide (npr. planinska područja Afgansitana, Somalije, Jemena i sl.) ili ako govorimo o nuklearnim postrojenjima u Iranu, IMINT najčešće ostaje jedino raspoloživo rješenje.

3. BESPILOTNE LETJELICE I IMINT

Bespilotna letjelica ili UAV (eng. unmannned aerial vehicle), danas još u svijetu poznata i kao **„DRON“**, je letjelica ili zrakoplov bez posade, koji se može nadzirati na daljinu ili letjeti samostalno uporabom unaprijed programiranog plana leta ili pomoću složenih autonomnih dinamičkih sustava. Koristi se u vojne i obavještajne svrhe s ciljem izviđanja i snimanja terena, ali i za brojne civilne zadaće, kao što su policijska praćenja, istraživanja terena ili vatrogasni zadaci. Veličine letjelica su u rasponu od samo nekoliko milimetara (mikro UAV) do veličine zrakoplova s rasponom krila 40 m (Global Hawk). Uz minijaturizaciju tehnologije tijekom osamdesetih i devedesetih godina 20.stoljeća, zanimanje za bespilotne letjelice je

[114] http://www.fas.org/irp/imint/docs/rst/Sect6/Sect6_14.html , preuzeto 08.02.2014.

značajno poraslo. Prva generacija bila je uglavnom namijenjena izviđanju, dok su danas neke opremljene s naoružanjem, kao što je model MQ-1 Predator koji uključuje rakete zrak-zemlja.

Također, razvoj i stalno poboljšavanje performansi bespilotnih letjelica omogućava instaliranje sve više sofisticirane opreme, kao što su infracrvene kamere, termalne kamere, foto-video oprema, oprema za prisluškivanje i slično, čime se učinkovitost ovih metoda obavještajnog prikupljanja podataka neprestano povećava.

Danas postoji dosta proizvođača bespilotnih letjelica a glavni su Lockheed Martin, Boeing i Northrop Grumman od američkih proizvođača, te europski EADS, Alpi Aviation, Diamond Aircraft, SAAB i BAE Systems. Posebno iskustvo u proizvodnji i uporabi bespilotnih letjelica ima Izrael. Tamošnja tvrtka Israel Aerospace Industries (IAI) proizvodi bespilotnu letjelicu Heron 1 (1150 kg) koja je najveći konkurent američkom Predatoru MQ-1. Heron je u upotrebi u sve tri grane izraelskih oružanih snaga i igra značajnu ulogu u elektronskom prikupljanju podataka od strane izraelske obavještajne službe (ELINT metode). Korisnici ove letjelice su Turska, Francuska i još neke zemlje EU. U veljači 2009. tri letjelice i nadzorna zemaljska postaja postali su operativni u zrakoplovnoj bazi Bagram u Afganistanu. Kanadske snage iznajmile su jednu bespilotnu letjelicu tipa Heron kako bi je rabile u sklopu programa Noctua u Afganistanu. Danas preko pedeset zemalja raspolaže bespilotnim letjelicama. Obzirom na funkciju, UAV se dijele u 6 osnovnih skupina, i to na ciljničke (target drones), špijunsko-izvidničke, borbene, istraživačko-razvojne ili ekološke, logističke i civilno-komercijalne.

Obzirom na desetke modela bespilotnih letjelica koji se koriste danas u svijetu, u tekstu koji slijedi spomenut će se samo oni koji se koriste u IMINT svrhe, i to nekoliko najaktualnijih modela. Kroz problemski pristup, istražit će se različiti aspekti upotrebe bespilotnih letjelica danas u svijetu. Kontroverzna izvidničko-vojna upotreba „dronova“, osobito njihovo ubojito djelovanje, izazivaju velike polemike u društvu i negativne reakcije javnog mijenja, kao i kritike u svjetskim medijima.

Tablica br.3: Najpoznatije (neke) IMINT bespilotnih letjelica današnjice

DRON	GODINA	IMINT ZNAČAJKE
ELBIT Skylark-I/II	1996.-2006.	Izrael, laka bespilotna letjelica, dužina 2.2m raspon krila 2.96m, težina 10kg. Izdržljivost u zraku 2h, dolet 10km (Skylark II 60km). Koristi ih i HV. Svrha bespilotni nadzor i različite IMINT zadaće, u realnom vremenu šalje video sliku u centar na zemlji.
ELBIT Hermes 90/450/900	1994.-2015.	Izraelski dron MALE klase (Medium Altitude Long Range), Težina 1180kg, korisni teret 350kg, dostiže visinu 9146m (30.000 stopa) /36 sati. Koristi se u tzv. ISTAR misijama (Intelligence, Surveillance, Target, Reconnaissance), opremljena EO/IR/SAR/laser, Comint GSM, Elint itd.
GENERAL ATOMICS Predator RQ-1/MQ-1/MQ-9 Reaper	1997.-2007.	Najpoznatiji i najkorišteniji dron na svijetu, RQ-1 (MALE klasa), MQ-9 doseže 50.000 stopa. Dron MQ-9 Reaper nosi 360 kg internog i 1360 kg vanjskog tereta, za IMINT zadaće koristi SAR/EO/IR sustave te lasersko praćenje i označavanje meta; od naoružanja opremljen je raketama HELLFIRE-II i 2 laserski vođene bombe GBU-12 ili EGBU-49, teške 227 kg. Letjelicom se upravlja iz zemaljske upravljačke postaje GCS (Ground Control Station)
NORTHROP GRUMMAN RQ-4 GLOBAL HAWK / EURO HAWK	2008.	RQ-4 je trenutno najskuplja i najsofisticiranija bespilotna letjelica na svijetu, namijenjena misijama nadzora, praćenja i snimanja iz zraka na velikim visinama (HALE klasa-High Altitude Long Endurance, 60.000 stopa). Raspon krila 40m, dužina 14.5m, težina na polijetanju 14.628 kg, 1360 kg korisnog tereta, radijus djelovanja 26.000 km. Opremljen je najsofistiranijom IMINT opremom današnjice SAR/EO/IR, GMTI-Ground Movement Target Indicator. Glavni nedostatak je izrazito visoka cijena od 227 milijuna dolara.
ZALA-421	2012.	Bespilotna letjelica ruske proizvodnje, minijaturnih dimenzija, raspon krila 80cm, dužina 41cm, težina 9kg. Mala, prijenosna, praktična i vrlo pouzdana IMINT platforma. Plafon rada 3600 m, izdržljivost u zraku 90 min.
SCHIEBEL CAMCOPTER S-100 / GORIZONT AIR-S100	2005.	Bespilotna letjelica razvijena od austrijske tvrtke Schiebel, u studenom 2011. Predstavljena ruska inačica Gorizont Air-S100. Dostiže visine 18.000 stopa (5500 m) i može ponijeti do 50 kg opreme; oprema se s EO/IR L-3 Wescam FLIR sustavom, MX-10 IC sustavom
ALTIUS-M	2016.	Ruska bespilotna letjelica najnovije generacije, MALE klase, razvijena kao odgovor na američki predator MQ-9 Reaper. Proizvodi je ruski zavod Sokol, a elektroniku ruska tvrtka Tranzas. Biti će opremljena najnovijim SAR/EO/IR Imint sustavima. Predstavljanje se očekuje u 2016. godini.

4. IMINT I PROBLEMI U PRIMJENI

Pretražujući internetske izvore i pročavanjem trenutnih svjetskih trendova u primjeni IMINT metoda, može se naići na brojne kritičke osvrte ili tekstove koji se bave problemima suvremenog IMINT-a. U američkom časopisu Homeland Securitiy Today, u broju iz 26. travnja 2010. godine, objavljen je zanimljiv članak pod naslovom „IMINT Processing Problems Impact War on Terror“ [115], u kojem se autor Anthony L. Kimery bavi praktičnim problemima s kojima se susreću SAD prilikom primjene suvremenih IMINT obavještajnih metoda. Na „GEOINT 2009“ simpoziju u San Antonio-u, savezna država Texas u listopadu 2009., Lt. Gen. David Deptula, zamjenik voditelja osoblja u američkom ratnom zrakoplovstvu za obavještajni rad, nadzor i izviđanje, naglasio je da „imagery intelligence“ trenutno igra ključnu ulogu pronalaženju i otkrivanju, kao i procesuiranju terorizma diljem svijeta, te da će u budućnosti taj značaj rasti.

Međutim, nekoliko mjeseci kasnije, U.S. Government Accountability Office (GAO) upozorava američki Kongres da su mogućnosti obavještajne zajednice (IC – Intelligence Community) da prikupi i analizira slikovne zapise prikupljene putem špijunskih IMINT izvora ozbiljno narušene, te da postoji niz nedostataka, što je izazvalo dosta problema u prekomorskoj borbi protiv Al-Qaide i s njom povezanih skupina (AQAM – Al-Qaida Associated Movements).

GAO naglašava da su IMINT izvori nedvojbeno vrijedni u lociranju individualnih terorista, terorističkih objekata, sigurnih kuća i slično. Međutim, ponekad je tih prikupljenih podataka previše i oni bi trebali biti čvršće povezani i umreženi s drugim obavještajnim izvorima, kao što su SIGINT i HUMINT. Najveći problem je što se podaci ne mogu dovoljno brzo obraditi i analizirati. GAO također, 17. ožujka 2010. u svom obraćanju oružanim snagama („House Committee on Armed Services Subcommittees on Air and Land Forces and Seapower and Expeditionary Forces“), upozorava kako mogućnosti prikupljanja „imagery intelligence“ podataka iz zraka ne premašuje samo tehničke mogućnosti prijenosa podataka zemaljskim postajama, već nadmoćno premašuje broj IMINT analitičara koji te podatke trebaju obraditi.

Direktor agencije GAO, Davi M. D´Agostino naglašava da brojni ISR sustavi (eng. ISR – intelligence, surveillance and reconnaissance) prikupljanja IMINT podataka, iz zraka, bilo s ljudskim posadama, ili iz bespilotnih letjelica, ili putem svemirskih sustava, ili drugih izviđačkih morskih ili zemaljskih sustava, količinom podataka predstavljaju ozbiljan izazov vojnim i sigurnosnim obrambenim agencijama, u smislu obrade, analize i korištenja podataka.

Primjerice, GAO upozorava, da se jedva polovica podataka prikupljenih bespilotnom letjelicom Predator-RQ u praćenju i snimanju Al-Qaide može dalje eksploatirati. Količina digitalnih podataka nadmoćno premašuje analitičke mogućnosti obavještajne zajednice (IC).

Biti sposoban brzo i efikasno sintetizirati „tsunami“ slikovnih zapisa prikupljenih dronovima, naročito FMV zapisa (eng. FMV – full motion video[116]), i proslijediti ih ljudima koji su ih trebali „jučer“, postao je **osnovni izazov** današnjeg IMINT-a u svjetskom ratu protiv

[115] http://www.hstoday.us/blogs/the-kimery-report/blog/imint-processing-problems-impact-war-on-terror/4961ddab3a70e6883667bafe91fc0c0d.html , preuzeto 04.03.2014.
[116] http://www.lockheedmartin.com/us/products/fmv.html , preuzeto 05.03.2014.

terorizma. Daptula upozorava kako ćemo u bliskoj budućnosti „naći sebe kako plivamo u mnoštvu senzora i utapajući se u podacima“. Neki članovi IC zajednice govore da se to već događa.

Tijekom praćenja terorista, osobito FMV metodom u realnom vremenu, potrebno je imati dobro uvježbane analitičare koji fizički motre zaslone nekoliko, potpuno različitih video prijenosa. Ponekad ih je za posao koji obavlja jedan analitičar, potrebno i nekoliko, ovisno o okolnostima. Problem nedovoljnog broja adekvatno osposobljenog broja IMINT analitičara prisutan je već duže vrijeme. Nestručne ili pogrešne procjene FMV zračnih snimki često imaju neželjene posljedice.

U svom govoru na Geoint konferenciji, Maj.Gen. Bradley Heithold, zapovjednik obavještajne službe USAF-a, objavio je kako je za praćenje i eliminiranje Abu Musab Al Zarqawija, vođe Al-Qaide u Iraku 2006. godine, bilo potrebno neprekidno 7-dnevno letenje Predator drona, koji je tjedan dana prije akcije, 24 sata dnevno pratio osobu, kako bi protuterorističke snage mogle izračunati njegovu lokaciju sa 100% sigurnošću.

Heithold ističe kako je potreban ogroman napor u pronalaženju i lociranju terorista. Nakon što se dobiju IMINT i SIGINT obavještajni podaci s U-2 i Predator špijunskih letjelica, potreban je netko tko će pregledati sve zapise, kadar po kadar, identificirati prijetnje, zatvoriti logične krugove života na tom području i spojiti ih s ostalim obavještajnim podacima, kako bi se dobili podaci s visokim stupnjem pouzdanosti.

Američka tvrtka Harris Corporation proizvela je video analitički sustav koji velikom brzinom obrađuje sve slikovne zapise i sprječava preopterećenost sustava instalacijom naprednih širokopojasnih podatkovnih linkova na prikupljačkim platformama. Tvtka također proizvodi ručne prijenosne video-prijemnike za vojnike na bojišnici, koji im omogućavaju izravno (eng. real-time imagery)[117] pregledavanje zračnih snimki područja u kojem se nalaze. Na ovaj način rasterećuje se analitički sustav i IMINT informacija dovodi izravno do krajnjeg korisnika.

Slika br. 4: Harris Corporation Data Exploitation[118]

[117] http://govcomm.harris.com/solutions/products/defense/unmanned-systems.asp , preuzeto 06.03.2014.
[118] http://govcomm.harris.com/solutions/products/defense/unmanned-systems.asp , preuzeto 06.03.2014.

Kao rješenje problema „prekomjerne količine podataka“, Hay ističe strategiju „mission-focus“, gdje se većina podataka u pripremi i potpori misije (npr. praćenje konvoja vozila do područja misije, tzv. „en-route segment“) odbacuje i ne analizira u detalje, već se analitičari fokusiraju na samu misiju (npr. dolazak konvoja vozila na odredište i početak planirane misije). Širina frekvencijskih područja također predstavlja ograničavajući faktor u satelitskoj i zemaljskoj komunikaciji. Prevelika količina prikupljenih podataka često se ne može poslati, primiti i spremiti na zemaljske servere, radi daljnje analitike.

Osnivanjem nove agencije ratnog zrakoplovstva, Air Force ISR Agency[119] (ISR – intelligence, surveillance and reconnaissance) i uvođenjem interoperabilne mreže DCGS (Distributed Common Ground / Surface System) omogućio se pristup podacima svim korisnicma obavještajne zajednice. Sustav DCGS postao je tako glavno obavještajno, nadzorno i izviđačko oružje američkog ratnog zrakoplovstva. DCGS koristi 20 geografski odvojenih i umreženih zemaljskih postaja, koje objedinjavaju sve obavještajne podatke prikupljene špijunskim letjelicama U-2, RQ-4 Global Hawk, MQ-9 Reaper i MQ-1 Predator.[120]

Prikupljene IMINT podatke, dobivene putem DCGS sustava, obrađuju specijalizirani analitičari slikovnih zapisa (eng. imagery analists), pripadnici „30-tog Obavještajnog skvadrona“ U.S. Air Force-a.

4.1. Dronovi i mišljenja javnosti – Public Opinion

Razvojem dronova i njihovom upotrebom u fazi obavještajnog prikupljanja podataka – snimki iz zraka, odnosno u IMINT zadaćama, kombinirano s njihovim ubojitim djelovanjem, sve češće se mogu pročitati vijesti o stradavanju nevinih civila. Razvoj modernih IMINT platformi otvorio je neke nove, „dodatne“ mogućnosti kao što su izravna likvidacija neprijatelja, nakon što je lociran, uočen, snimljen ili praćen tijekom IMINT zadaće. Ovaj novi oblik ratovanja donio je jednu sasvim novu dimenziju u suvremenim taktikama ratovanja, ali i bitno povećao značaj IMINTA, koji je postao sastavni dio svake operacije u Iraku, Afganistanu, Siriji ili Iranu. Međutim, ova strategija izaziva broje kontraverze i kritike svjetske javnosti, jer u napadima dronova svakodnevno stradavaju nedužni civili – žene, djeca i starci. Slučajevi poput događaja u Jemenu, kada je 13. prosinca 2013. godine američka bespilotna letjelica MQ-9 Reaper, tijekom redovne ISR zadaće, greškom pobila svadbenu povorku, zamijenivši je konvojem Al-Qaide, izazivaju zgražanje javnosti i kritike svjetskih medija.[121] Iako je „greška“ pripisana bespilotnoj letjelici, očito je da je u pitanju ljudski faktor, odnosno pogrešno tumačenje FMV (full motion video) zapisa od strane operatera letjelice, tijekom IMINT zadaće. Uz kritike svjetske javnosti, događaj je oštro osuđen i od strane UN-ovog Odbora za ljudska prava, sa sjedištem u Ženevi.[122] U listopadu 2013. godine svijet je obišla priča američkog pilota bespilotnih letjelica Predator i Reaper, oboljelog od

[119] http://www.afisr.af.mil/library/factsheets , preuzeto 07.03.2014.
[120] http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104525/air-force-distributed-common-ground-system.aspx , preuzeto 07.03.2014.

[121] http://www.jutarnji.hr/uzas-u-jemenu-bespilotna-letjelica-greskom-pobila-15-civila-u-svadbenoj-povorci-/1146619 , preuzeto 08.03.2014.
[122] http://www.un.org/apps/news/story.asp/story.asp?NewsID=46831&Cr=yemen&Cr1 , preuzeto 08.03.2014.

PTSP-a, koji je priznao da je u periodu između 2007. i 2011., upravljajući UAV letjelicama iz baze u Nevadi, ubio više od 1600 ljudi u operacijama „attack-dronova“ u Afganistanu, Pakistanu i Iraku.[123] Britanski dnevni list The Guardian 13. veljače 2013. godine, u članku „Nato air strike kills civilians in eastern Afganistan“, opisuje kako je u zadnjoj NATO akciji usmjerenoj na likvidaciju četvorice talibanskih vođa, ubijeno deset nevinih civila, uključujući četiri žene i petoro djece.[124]

Operacije američkih dronova u Pakistanu trenutno su predmet najvećih kritika. Područje Sjevernog Waziristana, koje graniči s Afganistanom, izloženo je danonoćnim preletima američkih dronova, koje osim IMINT zadaća, vrše napade iz zraka na terorističke skupine[125]. Izvješća navode brojne slučajeve ubojstava nevinih muškaraca, žena i djece. Obzirom na izvješća u protekle dvije godine, Amnesty International u listopadu 2013. godine izražava ozbiljnu zabrinutost zbog napada koji su rezultirali egzekucijom nevinih, i pita se, ima li u njima elemenata ratnog zločina.[126]

U američkom društvu također traje debata oko etičnosti upotrebe dronova, međutim trenutno je svedena na raspravu oko ubijanja američkih državljana diljem svijeta, osumnjičenih za terorizam.[127] U studenom 2013. godine u Ženevi se sastao UN-ov odbor kako bi raspravio potencijalne opasnosti ove kontroverzne tehnologije, te se spominje i mogućnost skore zabrane tzv. „attack-dronova“.[128]

4.2. Globalna anti-dron kampanja

Posebni UN-ov izvjestitelj za ljudska prava i anti-terorizam Ben Emmerson, nakon više od godinu dana istraživanja napada dronova, 28. veljače 2014. podnio je posebno izvješće UN-u. [129] izvješću se analizira 30 različitih slučajeva napada dronovima, u razdoblju između 2006. i 2013. godine u kojima su stradali nevini civili, na područjima Afganistana, Jemena, Pakistana, Somalije i Gaze. Također, izvješće spominje podatke Human Rights Watch organizacije, prema kojima su SAD od 2009. godine izvele 86 ubojitih antiterorističkih napada dronovima, u kojima je do kraja 2013. ubijeno više od 500 ljudi. Iako su većina njih bili pripadnici militantnih skupina povezanih s Al-Qaidom, zabrinjava podatak da je u tim napadima stradala do 71 nedužna civilna osoba.[130] Emmerson u izvješću navodi da radna grupa National Dialogue Conference zahtjeva hitno smanjenje napadačkih operacija dronovima. Također, inzistira na tome da globalni rat protiv terorizma ne smije uzimati nevine žrtve i naglašava odgovornost država u poduzimanju promptnih istraga i podnošenje detaljnih izvješća javnosti sa svim bitnim činjenicama. Organzacija HRW (Human Rights

[123] http://www.jutarnji.hr/tuzna-prica-navigatora-bespilotnih-letjelica-cetiri-godine-gledao-je-kako-ginu-clanovi-al-qa-ide--ali-i-civili/1135469 , preuzeto 09.03.2014.
[124] http://www.theguardian.com/world/2013/feb/13/nato-air-strike-civilians-afghanistan , preuzeto 09.03.2014.
[125] http://online.wsj.com/news/articles/SB123803414843244161 , preuzeto 09.03.2014.
[126] http://www.amnestyusa.org/research/reports/will-i-be-next-us-drone-strikes-in-pakistan , preuzeto 10.03.2014.
[127] http://www.oregonlive.com/politics/index.ssf/2013/03/ron_wyden_says_cia_confirmatio.html , preuzeto 10.03.2014.
[128] http://www.jutarnji.hr/un-ce-zabraniti--robote-ubojice-/1139616 , preuzeto 10.03.2014.
[129] http://justsecurity.org/wp-content/uploads/2014/02/Special-Rapporteur-Rapporteur-Emmerson-Drones-2014.pdf , preuzeto 12.03.2014.
[130] http://dissenter.firedoglake.com/2014/03/03/drone-war-in-yemen-three-killed-in-latest-strike-un-report-demands-facts-on-civilian-deaths , preuzeto 12.03.2014.

Watch) trenutno vodi snažnu kampanju za zabranu ubojitih napada dronovima.[131] U Pakistanu, zemlji koja je, uz Afganistan, trenutno pod najvećim udarom američkih „attack-dronova“, traje također snažna anti-dronovska kampanja. Građani Pakistana kao i domaći mediji kritiziraju vlastitu vladu jer je NATO savezu dozvolila danonoćno nadziranje vlastitog teritorija, u svrhu borbe protiv globalnog terorista. Problem je u tome što NATO obilato koristi to odobrenje, te uz redovite IMINT zadaće, svakodnevno vrši napade iz zraka, pri čemu često stradavaju nevini civili. Pakistanski anti-dron aktivist i novinar Kareem Khan je u prosincu 2009. u napadu drona izgubio brata i maloljetnog sina. O tom događaju svjedočio je i pred Euroskim Parlamentom.

Tijekom 2013. godine Bijela Kuća je poduzela konkrentne mjere i radnje kako bi se na saveznom nivou zakonski regulirala upotreba dronova. Usporedo se bilježe slične aktivnosti i u pojedinim saveznim državama i lokalnim okruzima. Namjera je strogo zabraniti bilo kakvo naoružavanje dronova, a od službi sigurnosti prikupiti dovoljno čvrsta jamstva o zaštiti privatnosti građana prije slanja dronova u „imagery intelligence“ misije.[132]

Početkom 2014. godine, savezne američke države Washington i Wisconsin postale su deseta i jedanaesta savezna država koje su ograničile upotrebu dronova.[133] Washington propisima HB 2789[134] od 17. veljače 2014. godine ograničava upotrebu vladinih bespilotnih letjelica na situacije gdje je sigurnost građanskih prava zajamčena, tijekom vojnog treninga, i u nekim izvanrednim slučajevima kada se radi o spašavanju ljudskih života. Dronovi se još mogu koristiti u snimanju divljih predjela u svrhu zaštite okoliša. Pobornici ove legislative ističu zabrinutost građana mogućnošću snimanja i špijuniranja u svojim domovima, na svojim privatnim imanjima i sl., od strane Vlade, a da za to niti ne znaju. U svrhu fotografiranja zemljišta, dronovi mogu biti korišteni isključivo uz prethodno odobrenje vlasnika zemljišta. Senat savezne države Wisconsin, dana 18. veljače 2014. godine izglasao je zakon kojim se upotreba bespilotnih letjelica, tzv. dronova u svrhe audio i video snimanja proglašava kriminalnom radnjom. Također, svako naoružavanje drona tretira se kao kriminalni akt.[135]

Internetski portal Aljazeera-Balkan u članku iz 01.siječnja 2016. navodi podatak da je tehnologija dronova proglašena jednom od tri najbrže rastuće tehnologije u svijetu u 2015. godini.[136] Kako je i predviđano, 2015. je bila godina dronova. Ostvaren je rast prodaje bespilotnih letjelica od 20 posto i godišnji promet na tržištu iznosi 1,4 milijarde dolara. Iako dronovi predstavljaju noćnu moru aerodromima, prodaju potiču fotografije i filmovi snimljeni iz zraka dronovima, a koji se objavljuju na društvenim mrežama. Statistički podaci pokazuju drastičan rast takvih objava na društvenoj mreži Facebook.

---

[131] https://www.hrw.org/topic/counterterrorism/targeted-killings-and-drones , preuzeto 13.03.2014.
[132] http://news.cnet.com/8301-13578_3-57573183-38/house-orders-pentagon-to-disclose-domestic-drone-use , preuzeto 14.03.2014.
[133] http://www.truthrevolt.org/news/washington-and-wisconsin-pass-anti-drone-laws , preuzeto 14.03.2014.
[134] http://apps.leg.wa.gov/documents/billdocs/2013-14/Pdf/Bills/House%20Bills/2789.pdf , preuzeto 15.03.2014.
[135] http://www.washingtontimes.com/news/2014/feb/18/wis-senate-to-vote-on-bill-limiting-use-of-drones , preuzeto 18.03.2014.
[136] http://balkans.aljazeera.net/vijesti/najtrazenija-tehnologija-u-2015-godini

5. IMINT I ZAKONSKA NEODREĐENOST - STAVOVI EUROPSKE (EASA) I HRVATSKE AGENCIJE ZA CIVILNO ZRAKOPLOVSTVO (CCAA)

Europska agencija za sigurnost civilnog zračnog prometa (EASA) objavila je 18.12.2015. godine tehničko mišljenje (Technical Opinion) za sustave bespilotnih letjelica.[137] Tehničko mišljenje rezultat je konzultacija u vezi s pozivom na javnu raspravu br. A-NPA-2015-10[138] na koji je stiglo 3400 komentara. On uključuje 27 prijedloga za izradu pravnog okvira bez obzira na operativnu masu bespilotne letjelice. Svrha je postavljanje pravnog temelja za budući rad te kako bi poslužio kao smjernica za države članice EU za daljni razvoj i izmjenu nacionalnih propisa koji reguliraju sustave bespilotnih letjelica (dronova). Republika Hrvatska kao punopravna članica EU, odnosno Hrvatska Agencija za Civilno Zrakoplovstvo (HACZ) kao punopravna članica EASA-e, u potpunosti će slijediti smjernice zadane EU regulativom.

Obzirom na naglu ekspanziju „dronova“ zadnjih nekoliko godina i njihovu financijsku pristupačnost, za očekivati je donošenje zakonske regulative već ove godine.

Slika br. 5: Dron

U članku iz 02. veljače 2016. internetski portal Aljazeera-Balkan iznosi zanimljive podatke o rastu proizvodnje, prodaje i upotrebe dronova.[139] Tehnologija, koja je do jučer bila rezervirana samo za vojne svrhe, niskom cijenom i dostupnošću nalazi sve veću primjenu i u civilnom svijetu, što će uzročno-posljedičnom vezom izazvati i određene promjene u zakonskoj regulativi.

Obzirom da je ovo vrlo aktualna problematika, ostaje za vidjeti u kom smjeru će se stvari glede dronova, njihove upotrebe i njihovih mogućnosti dalje razvijati. Za očekivati je daljnji tehnološki razvoj i njihovu sve veću primjenu na vojnom planu – što zbog brzog razvoja tehnologije, što zbog njihove iznimne korisnosti i povećanju sigurnosti u vojnim operacijama. Na civilnom planu, gdje upotreba bespilotnih letjelica u svrhu „imagery intelligence“ ograničava građanske slobode i narušava privatnost ljudi, za očekivati je daljnje jačanje zakonske regulative, kojom će se upotreba dronova u policijske i sigurnosne svrhe strogo, pravno-procesno ograničiti.

---

[137] http://www.ccaa.hr/hrvatski/novosti_7/europska-agencija-za-sigurnost-zracnog-prometa-objavila-technical-opinion-za-sustave-bespilotnih-zrakoplova_692/
[138] NPA - (Notices for Proposal Ammendments)
[139] http://balkans.aljazeera.net/vijesti/raste-upotreba-dronova-u-civilne-svrhe

6. FRONTEX I IMINT U ZAŠTITI VANJSKIH GRANICA EU

FRONTEX je agencija Europske Unije za sigurnost vanjskih granica. Odgovorna je za kooridinaciju aktivnosti nacionalnih graničnih službi u nadzoru vanjske granice EU s državama nečlanicama. Sjedište Frontexa je u Varšavi, Poljska.

Nadzor iz zraka i izviđanje vanjskih granica jedna je od osnovnih komponenti granične kontrole EU. Trenutno se poduzimaju brojne različite aktivnosti u tom smislu, a kao osnovni izazovi ističu se:

- detekcija i lociranje malih brodova na moru (slučaj Lampedusa i sl.),
- neprestano poboljšavanje izviđačkih mogućnosti graničnih patrola, zrakoplova i brodova,
- integriranje svih postojećih sustava u jedan, i eliminiranje raznih ograničavajućih faktora.[140]

Ovi izazovi nameću uvođenje široke lepeze najmodernijih fleksibilnih više-senzorskih sustava visokih performansi, instaliranih i operiranih s različitih pilotski upravljanih i bespilotnih IMINT platformi. Široko-pojasni nadzorni sustav (Wide Area Surveillance System) objedinjava različite tipove senzora sa svrhom stvaranja lokalne operativne slike za određeno područje. Komponente sustava uključuju sustave za detekciju (zemaljski radari, pasivni infra-crveni sustavi – IR, seizmički sustavi i sl.), sustave za klasificiranje objekata u pokretu (elektro-optički EO/IR imagery sustavi) kao i sustav EUROSUR (European Surveillance System)[141] koji objedinjava podatke prikupljene putem višenamjenskih senzora u jednu jedinstvenu, kombiniranu sliku – tzv. situational awareness view. EUROSUR sustav je glavni obavještajni nadzorni sustav FRONTEX-a.

FRONTEX igra ključnu ulogu u premošćivanju prepreka između proizvođača opreme i korisnika, kako bi zajednica proizvođača imala jasnu sliku potreba i izazova s kojima se susreću EU granične službe u Schengen sustavu.

U tom kontekstu razvojni odjel Frontex-a (Research and Development Unit of Frontex) 10. travnja 2014. godine u Varšavi organizira radni sastanak na temu „Border Surveillance Sensors and Platforms: Challenges and Opportunities“. Cilj radionice je prezentacija i debata o upotrebi bespilotnih letjelica u IMINT svrhe, zakonska regulativa, industrijska dostignuća, tehnološke inovacije i sl.

[140] http://frontex.europa.eu/news/invitation-for-border-surveillance-workshop-2014-OfPDf6 , preuzeto 23.03.2014.
[141] http://frontex.europa.eu/intelligence/eurosur , preuzeto 23.03.2014.

Slika br. 6: EUROSUR[142] kontrolni centar

Republika Hrvatska već nekoliko godina intenzivno radi na postizanju Schengenskih standarda u zaštiti državne granice. U tom smislu, u sklopu prijekta „Schengen Facility Fund“, MUP RH je nabavio dva najmodernija helikoptera AW139, proizvedena od strane europskog konzorcija AgustaWestland. Cijena helikoptera je 119 milijuna kuna i prvi od dva helikoptera isporučen je Republici Hrvatskoj 20. siječnja 2016.[143]

Slika br. 7: FRONTEX – termovizijska snimka iz zraka[144]

6.1. Helikopter AW139 i njegova primjena u MUP-u RH, u zaštiti državne granice

U Međunarodnoj zračnoj luci u Zagrebu u srijedu, 20. siječnja, održana je svečana primopredaja helikoptera AgustaWestland AW139. Ugovor o primopredaji helikoptera vrijednog 119 milijuna kuna s PDV-om potpisao je glavni ravnatelj policije Vlado Dominić sa Stefanom Villantijem iz kompanije Finmeccanica.

---

[142] http://frontex.europa.eu/photo/eurosur-LD3NF7 , preuzeto 23.03.2014.
[143] http://www.mup.hr/228630.aspx
[144] http://frontex.europa.eu/photo/eurosur-LD3NF7 , preuzeto 02.04.2014.

Riječ je o potpuno novom helikopteru koji je nabavljen iz Schengen Facility Fonda kojim će piloti MUP-a RH nadzirati državnu granicu i sudjelovati u aktivnostima u sklopu Frontexa (Europska agencija za upravljanje operativnom suradnjom na vanjskim granicama država članica EU).

Helikopter AW139 je višenamjenski helikopter više srednje klase (utility), trenutno je jedan od najmodernijih helikoptera na svijetu i najprodavaniji helikopter u svojoj klasi (klasa 6 tona), u zadnjih 10 godina. Težina praznog helikoptera iznosi 4500 kg, dok maksimalna težina na polijetanju iznossi 6800 kg, što znači da helikopter može ponijeti 2300 kg korisnog tereta. AW139 certificiran je za 2 pilota i maksimalno 15 putnika (high-density konfiguracija), može dosegnuti maksimalnu visinu od 20.000 stopa (6000 m) i razviti maksimalnu brzinu od 167 čvorova (308 km/h).

Slika br. 8: Helikopter AW139

U policijskoj konfiguraciji (low-enforcement) AW139 najčešće se oprema u varijanti 2+8 (2 pilotska sjedala, 7 putničkih i jednim sjedalom operatera radne FLIR stanice). U helikopteru se nalazi informatička oprema i FLIR kamera u prednjem djelu, a služi za nadzor mora, granice, potragu brodova i ljudi. Također, unutra se nalazi radna stanica operatera koji upravlja tom kamerom i traži nestalu osobu ili osobe u slučaju nekakvog nezakonitog prelaska granice. Na slici br.21 prikazan je najskuplji i najsofisticiraniji dio opreme helikoptera, termovizijski sustav – FLIR (Forward Looking Infrared Red).[145]

[145] http://www.flir.com/surveillance/display/?id=64173

Slika br. 9: Sustav FLIR

Sustav instaliran na helikopterima MUP-a je termovizijski sustav najnovije generacije klase FLIR UltraForce HD koji omogućava IMINT zadaće na najvišem nivou. Sustav teži samo 28 kg i smještan je u nosu helikoptera. Značajke sustava UltraForce HD su:

- brza instalacija i integracija,
- elektro-optički zrakoplovni sustav visoke rezolucije (EO/HD),
- HD širokokutna kamera 1920x1080 u boji, 20x zoom, koja maksimalizira pretraživanje u dnevnim uvjetima, u uvjetima zore i sumraka, na velikim udaljenostima (npr. čitanje registarske oznake na udaljenosti od nekoliko km, pronalaženje tijela do 20cm ispod zemlje i sl.),
- izvanredne stabilizacijske mogućnosti, kompezacija vibracija i kretnji helikoptera, osobito značajno kod rada na većim udaljenostima,
- spotter / laser funkcija i sl.

Slika br. 10: Upravljačka stanica operatera FLIR sustava

Drugi sustav značajan za provođenje IMINT misija je trenutno najmoderniji sustav za pretraživanje na tržištu (u daljnjem tekstu: searchlight) TRAKKABEAM A-800.[146] Trakkabeam A-800 je potpuno automatizirani višenamjenski (multi-mission) sustav za

[146] http://www.trakkacorp.com/products/a-800

pretraživanje, s mogućnošću okretanja po svim osima. Sustav ima unutarnje ugrađen kotač s nekoliko različitih filtera, koji omogućavaju promjenu spektra u samo jednoj sekundi (infracrveni spektar, vidljivi crveni, žuti i bijeli svjetlosni spektar). Infracrveni filter koristi se noću u kombinaciji s NVG tehnologijom (nigh-vision googles), i razvija snop IC-svjetlosti nevidljiv ljudkom oku (vidljiv isključivo kroz NVG).

Sustav A-800 na helikopteru AW139 MUP-a RH smješten je na lijevoj prednjoj strani i omogućava misije zračnog nadzora i pretraživanja (airborne surveillance), misije traganja i spašavanja na kopnu i moru (SAR), misije borbenog traganja i spašavanja (CSAR), prikrivane policijske operacije i tajne sigurnosne operacije i sl.

Slika br. 11: Trakkabeam A-800

Nabavka dva najmodernija policijska helikoptera odjeknula je i u svjetskim zrakoplovnim krugovima, i objavljena je u svim vodećim svjetskim zrakoplovnim časopisima.[147] Također, bitno je naglasiti da će i drugi helikopter AW139 nabavljen u svrhu nadzora državne granice, čija se isporuka očekuje u srpnju 2016., biti opremljen istom opremom. U postupku je opremanje i druga dva nova helikoptera EC-135 u floti MUP-a RH istom opremom, nabavljena 2013. godine vlastitim sredstvima.

U **tehnološkom smislu**, zadovoljstvo je zaključiti da MUP RH, u misijama zaštite državne granice RH i misijama zaštite vanjskih granica EU, koristi trenutno najmoderniju opremu koja se u ovom trenutku može nabaviti na svjetskom tržištu. Nabavka navedene opreme dostupna je samo zemljama članicama EU i NATO saveza.

Prema mišljenju nekih zrakoplovnih stručnjaka, MUP RH sada raspolaže najmodernijom flotom policijskih helikoptera u Europskoj Uniji.

7. ZAKLJUČAK

U današnjem globalnom ratu protiv terorizma, zahtjevi za novim i tajnim metodama prikupljanja podataka veći su nego ikad. Potraga za relevantnim informacijama o kretanjima i planovima Al-Qaide, ISIL-a i njima bliskih terorističkih skupina, koja zahtjeva tajne metode prikupljanja s garancijom točnosti i ekskluzivnosti, predstavlja izazov za operativne i obavještajne zajednice. Nedostupnost vodećih ljudi terorističkih skupina, koji se skrivaju u

[147] http://www.finmeccanica.co.uk/-/aw1221

planinskim lancima Afganistana, Pakistana, Jemena, Sirije ili pustinjskim predjelima Saudijske Arabije, bez struje, interneta i sredstava komunikacije, obavještajnim službama ne ostavljaju previše mogućnosti. IMINT se nameće kao jedina učinkovita obavještajna metoda. Bez logističke potpore IMINT-a, više se ne može zamisliti niti jedna vojna operacija NATO snaga u Afganistanu, Iraku ili Siriji. IMINT u odnosu na druge obavještajne metode iziskuje složene sustave s kojim se provode i koji zahtjevaju visoka financijska sredstva, što pak limitira njegovu rasprostranjenost. Može se zaključiti, da trenutno u segmentu IMINT-a, Sjedinjene Američke Države i članice NATO saveza imaju stratešku i obavještajnu prednost u odnosu na ostale velesile, prije svega Rusiju i Kinu, ali i na glavne terorističke skupine.

Etički apekt upotrebe dronova i nedostatak međunarodne zakonske regulative je problem koji se nameće u posljednje vrijeme. Razvoj dronova kao IMINT platformi, koji usporedo sa špijunskim zadaćama imaju mogućnost ubojito djelovati na ciljeve na zemlji, otvorio je neka pitanja na koja još nema odgovora.

Zadnjih nekoliko godina bilježi se strahovito brzi rast proizvodnje i prodaje jeftinih civilnih varijanti bespilotnih letjelica (dronova), koje se najčešće koriste u svrhe zračnog fotografiranja. Nekontrolirano i nestručno upravljanje civilnim dronovima, koji bez problema mogu dosegnuti visinu od 500 m, počelo je ozbiljno narušavati sigurnost civilnog zračnog prometa i predstavlja noćnu moru svake međunarodne zračne luke. U tom smislu, europska agencija za sigurnost zrakoplovstva EASA ubrzano radi na donošenju zakonske regulative i ograniičenju korištenja bespilotnih letjelica.

Ne kraju treba istaći značaj i ulogu IMINT metoda u čuvanju državne granice RH i vanjskih granica EU. U tehnološkom smislu, možemo zaljučiti da je MUP RH u zadnjih nekoliko godina napravio značajan iskorak u približavanju Schengenskim standardima i da je već sada u korak s najopremljenijim policijskim snagama u EU. Nabavkom dva nova „high-tech“ helikoptera AW139, opremljena najsofisticiranijom „surveillance / IMINT“ opremom, postavljaju se novi tehnološki i sigurnosni standardi u okruženju.

LITERATURA

Knjige i članci

Bilandžić, M. (2008). Poslovno obavještajno djelovanje, Zagreb: AGM.

Dupre, R. E. (2011). Guide to Imagery Intelligence, *Intelligencer: Journal of U.S. Intelligence Studies,* (18), 2, 62-63.

Encyclopaedia Britannica (1985). sv.21, str. 454.

Javorović B., Bilandžić, M. (2007). *Poslovne informacije i business intelligence*. Zagreb: Golden marketing – Tehnička knjiga.

Javorović, B. (1997). Terorizam. *Policija i sigurnost,* (VI), 1-2, 1-56.

Kimery, A. L. (2010). *IMINT Processing*. *Problems Impact War on Terror* http://www.hstoday.us/blogs/the-kimery-report/blog/imint-processing-problems-impact-war-on-terror/4961ddab3a70e6883667bafe91fc0c0d.html

Klaić, B. (1974). *Veliki rječnik stranih riječi,* Zagreb: Zora.

Klasan, V. (2012). Utjecaj profileracije oružja za masovno uništenje na sigurnost EU, *National security and the future,* (13), 1-2, 127-301.

Mičić, D. (2010). Iskustva sa bespilotnim letjelicama II dio, *Hrvatski vojnik*, (VII) 281, 26-29. http://www.hrvatski-vojnik.hr/hrvatski-vojnik/2812010/iskustva2.asp
Radaković, S. (2007). Avioni za električno izviđanje, *Hrvatski vojnik*, (IV), 123. http://www.hrvatski-vojnik.hr/hrvatski-vojnik/1232007/avioni.asp
Taylor, S., A. (2010). Uloga obavještajne djelatnosti u nacionalnoj sigurnosti. U: Collins, A. (ur.) *Suvremene sigurnosne studije*. Zagreb: Politička kultura, 284-308.
Zelenika, R. (2000). *Metodologija i tehnologija izrade znanstvenog i stručnog rada*, Rijeka: Ekonomski fakultet.

Internetski izvori

ALJAZEERA, http://balkans.aljazeera.net/vijesti/najtrazenija-tehnologija-u-2015-godini , preuzeto 15. 1. 2016.
ALJAZEERA, http://balkans.aljazeera.net/vijesti/raste-upotreba-dronova-u-civilne-svrhe , preuzeto 10. 2. 2016.
ANALIZA SNIMKI IZ ZRAKA, http://en.wikipedia.org/wiki/Imagery_intelligence , preuzeto 04.02.2014.
ANTIDRONE, http://news.cnet.com/8301-13578_3-57575863-38/anti-drone-revolt-prompts-push-for-new-federal-state-laws , preuzeto 14.03.2014.
BILLDOCS, http://apps.leg.wa.gov/documents/billdocs/2013-14/Pdf/Bills/House%20Bills/2789.pdf , preuzeto 15.03.2014.
DRONES, https://www.hrw.org/topic/counterterrorism/targeted-killings-and-drones , preuzeto 13.03.2014.
EASA, http://frontex.europa.eu/news/invitation-for-border-surveillance-workshop-2014-OfPDf6 , preuzeto 23.03.2014.
EASA, http://www.ccaa.hr/hrvatski/novosti_7/europska-agencija-za-sigurnost-zracnog-prometa-objavila-technical-opinion-za-sustave-bespilotnih-zrakoplova_692/
EUROSUR, http://frontex.europa.eu/photo/eurosur-LD3NF7 , preuzeto 02.04.2014.
FINNMECANICA, http://www.finmeccanica.co.uk/-/aw1221
FLIR, http://www.flir.com/surveillance/display/?id=64173
FLIR, http://www.flir.com/US , preuzeto 01.03.2014.
FLIR, http://www.intelligence.gov/mission/data-gathering.html , preuzeto 02.02.2014.
FRONTEX, http://frontex.europa.eu/intelligence/eurosur , preuzeto 23.03.2014.
FRONTEX, http://frontex.europa.eu/photo/eurosur-LD3NF7 , preuzeto 23.03.2014.
GAO, http://www.gao.gov/products/GAO-10-331 , preuzeto 06.03.2014.
GUARDIAN, http://www.theguardian.com/world/2013/feb/13/nato-air-strike-civilians-afghanistan , preuzeto 09.03.2014.
HARRIS, http://govcomm.harris.com/solutions/products/defense/unmanned-systems.asp , preuzeto 06.03.2014.
HARRIS, http://govcomm.harris.com/solutions/products/defense/unmanned-systems.asp , preuzeto 06.03.2014.
HOMELAND SECURITY TODAY, http://www.hstoday.us/blogs/the-kimery-report/blog/imint-processing-problems-impact-war-on-terror/4961ddab3a70e6883667bafe91fc0c0d.html , preuzeto 04.03.2014.
IKONOS, BIN LADEN, http://www.fas.org/irp/imint/docs/rst/Sect6/Sect6_14.html , preuzeto 08.02.2014.
IMINT, http://www.fas.org/irp/nsa/ioss/threat96/part02.htm , preuzeto 02.02.2014.
JEMEN, http://dissenter.firedoglake.com/2014/03/03/drone-war-in-yemen-three-killed-in-latest-strike-un-report-demands-facts-on-civilian-deaths , preuzeto 12.03.2014.

JUTARNJI LIST, http://www.jutarnji.hr/un-ce-zabraniti--robote-ubojice-/1139616 , preuzeto 10.03.2014.
JUTARNJI LIST, JEMEN, http://www.jutarnji.hr/uzas-u-jemenu-bespilotna-letjelica-greskom-pobila-15-civila-u-svadbenoj-povorci-/1146619 , preuzeto 08.03.2014.
LOCKHEED, http://www.lockheedmartin.com/us/products/fmv.html , preuzeto 05.03.2014.
MUP RH, http://www.mup.hr/228630.aspx
NASIC, http://www.afisr.af.mil/units/nasic/index.asp , preuzeto 03.02.2014.
NGA, https://www.nga.mil/Pages/default.aspx , preuzeto 03.02.2014.
OSINT, https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html , preuzeto 01.02.2014.
PAKISTAN, http://www.aljazeera.com/news/asia/2014/02/pakistan-anti-drone-campaigner-missing-201421016542748960 2.html , preuzeto 13.03.2014.
PENTAGON, http://news.cnet.com/8301-13578_3-57573183-38/house-orders-pentagon-to-disclose-domestic-drone-use , preuzeto 14.03.2014.
PRIČA NAVIGATORA DRONOVA, http://www.jutarnji.hr/tuzna-prica-navigatora-bespilotnih-letjelica-cetiri-godine-gledao-je-kako-ginu-clanovi-al-qa-ide--ali-i-civili/1135469 , preuzeto 09.03.2014.
SAR, http://www.radartutorial.eu/20.airborne/ab07.en.html , preuzeto 16.02.2014.
SPECIAL REPORT, http://justsecurity.org/wp-content/uploads/2014/02/Special-Rapporteur-Rapporteur- Emmerson-Drones-2014.pdf , preuzeto 12.03.2014.
TRAKKABEAM A-800, http://www.trakkacorp.com/products/a-800
UN O JEMENU, http://www.un.org/apps/news/story.asp/story.asp?NewsID=46831&Cr=yemen&Cr1 , preuzeto 08.03.2014.
USAF ISR, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104525/air-force-distributed-common-ground-system.aspx , preuzeto 07.03.2014.
USAF ISR,[1] http://www.afisr.af.mil/library/factsheets , preuzeto 07.03.2014.
WAHINNGTON POST, http://www.truthrevolt.org/news/washington-and-wisconsin-pass-anti-drone-laws , preuzeto 14.03.2014.
WASHINGTON TIMES, http://www.washingtontimes.com/news/2014/feb/18/wis-senate-to-vote-on-bill-limiting-use-of-drones , preuzeto 18.03.2014.
WSJ, http://online.wsj.com/news/articles/SB123803414843244161 , preuzeto 09.03.2014.
WYDEN, http://www.oregonlive.com/politics/index.ssf/2013/03/ron_wyden_says_cia_confirmatio.html , preuzeto 10.03.2014.

Alen Sambolec

Davor Solomun

IMINT AND AEROSPACE TECHNOLOGY FOR DATA COLLECTION AND SECURITY ACTIVITIES

Summary

The paper presents and analyses various aspects of Imagery Intelligence Technologies (IMINT) as one of the contemporary intelligence-security methods Aerial image data acquisition phase via either aircraft, satellites or Unmanned Air Systems (UAS) discussed in particular. IMNIT phase opens each contemporary security operation ranging for example from international military and NATO forces in Iraq, Afganistan, Siria or Yemen to the elimination of Mr Osama Bin Laden in Pakistan.

In addition to technological aspects the paper discusses inappropriate regulatory requirements related to contemporary IMINT application. Related to this the position and reaction of global media and leading global powers to the application of contemporary IMNIT platforms (US drones) in particular has been analyzed.

The final outcome of the research is the applicability of IMNIT method as one of security enablers for the Republic of Croatia as well as comparative analysis of the contribution to the protection of external European Union borders. The particular challenge of the research is related to the implementation of new AgustaWestland AW139 helicopter by Ministry of the Interior of the Republic of Croatia, Special Police Forces.

Key words: *IMINT, Intelligence Aircraft, Unmanned Air Systems, Intelligence-Security Activities.*

STRUČNI RAD

Davorka Martinjak[148]
Anita Matijević[149]
Renata Odeljan[150]

OBRAZAC ZA PROCJENU RIZIKA OD PONAVLJANJA NASILNIČKOG PONAŠANJA U OBITELJI

Sažetak

Temeljem višegodišnje prakse policijskih postupanja u predmetima nasilja u obitelji prepoznata je potreba za kreiranjem učinkovite metode, kojom bi se provodila procjena rizika budućeg nasilja u obitelji. Svrha izrade standardiziranog obrasca procjene rizika (checklist) je od višestrukog značaja, naime odluke o mjerama opreza i zaštitnim mjerama, odluke o uvjetima za uhićenje i privođenje počinitelja sucu, predlaganje zadržavanja te predlaganje uključivanja drugih institucija u rad s počiniteljem bit će objektivnije i mjerodavnije. Identifikacija rizičnih čimbenika značajnih za procjenu rizika temeljila se na rezultatima istraživanja 235 policijskih spisa i sudskih presuda povodom počinjenja ubojstava i pokušaja ubojstava na štetu članova obitelji u razdoblju od 01.01.2005. do 31.12.2010. godine u Republici Hrvatskoj. Temeljem navedene identifikacije rizičnih čimbenika izrađen je Obrazac za procjenu rizika od ponavljanja nasilničkog ponašanja u obitelji koji će u sljedećoj testnoj fazi (šest mjeseci) primjene koristiti policijski službenici u svakodnevnoj praksi, nakon čega će uslijediti konačna verifikacija instrumentarija (check liste).

Ključne riječi: *nasilje u obitelji, procjena rizika, policijski službenici, prevencija.*

1. UVOD

Područje policijskog rada vezano uz obiteljsko nasilje i dalje je iznimno aktualno, a ishodište navedene aktualnosti nalazimo u statističkim pokazateljima koji ukazuju na kontinuitet ove pojave u društvu. Također, aktualizaciji teme obiteljskog nasilja doprinijelo je i sve jasnije opredjeljenje društvene zajednice za razvoj i promicanje ljudskih prava pa se tako zaštita prava žrtava smatra jednim od prioriteta. Ključni društveni resori koji u fokusu svog rada imaju ovu problematiku ugradili su u svoje strateške ciljeve jačanje kapaciteta prevencije i podizanje kvalitete operativnosti u svakodnevnom radu. U postizanju ovih ciljeva došlo je do značajnih pomaka u zakonodavnom određenju, edukaciji stručnjaka i međuresornoj suradnji.

Iako su prve zakonodavne norme u području obiteljskog nasilja utemeljene 1998. godine Obiteljskim zakonom, vidljiv je kontinuirani proces njihovih poboljšanja. Naime, nakon što je Republika Hrvatska postala punopravna članica Europske unije, bilo je potrebno uskladiti

[148] Dr. sc. Davorka Martinjak, viši predavač, Visoka Policijska škola, Zagreb, e-mail: dmartinjak@fkz.hr
[149] Anita Matijević, MUP, Ravnateljstvo policije, UKP, Odjel maloljetničke delinkvencije i kriminaliteta na šteti mladeži i obitelji, e-mail: amatijevic@mup.hr
[150] Mr. sc. Renata Odeljan, viši predavač, Visoka policijska škola, Zagreb, e-mail: rodeljan@fkz.hr

postojeće zakonodavne okvire s međunarodnim. Bitno je naglasiti da je Republika Hrvatska svoje temeljno opredjeljenje o očuvanju ljudskih prava iskazala od početka svoje opstojnosti potpisivanjem i ratificiranjem Konvencije o ukidanju svih oblika diskriminacije žena (CEDAW) iz 1979. godine i njezina Fakultativnog protokola iz 1999. godine, potpisivanjem Konvencije o pravima djeteta Ujedinjenih naroda te Konvencije za zaštitu ljudskih prava i temeljnih sloboda Vijeća Europe. Jedan od značajnijih dokumenata Vijeća Europe koji je utjecao na promjenu domaćeg zakonodavstva je Konvencija o sprečavanju i borbi protiv nasilja nad ženama i nasilja u obitelji iz 2011. godine, koju je Republika Hrvatska potpisala (za sada nije ratificirana) u siječnju 2013. godine. Ona donosi nove standarde i sveobuhvatni pristup problematici, od širenja javne svijesti o ovom problemu, preko kaznenopravne reakcije do socijalne potpore žrtvama (Radić, Radina, 2014). Navedene zakonodavne promjene vezane uz ovu problematiku napravljene su u dijelu Kaznenog zakona koji je stupio na snagu 2013. godine. Naime, tada je izmijenjeno niz definicija pojmova, a uvedeni su i neki novi pojmovi i izbrisan je članak Nasilničko ponašanje u obitelji, a činjenica da je netko počinio kazneno djelo s elementima nasilja prema bliskoj osobi propisana je kao kvalifikatorna okolnost u osam kaznenih djela kojima se inkriminira neki oblik ponašanja s elementima nasilja.

Za policijsku praksu od posebnog je značaja istaći da je Ravnateljstvo policije, neposredno nakon što je Republika Hrvatska 2013. godine potpisala Konvenciju, svim ustrojstvenim jedinicama MUP-a poslala instruktivnu uputu da je policija dužna u okviru svoje nadležnosti poduzimati mjere sukladno kriterijima proizašlim iz Konvencije:

- da su zasnovane na razumijevanju nasilja nad ženama i nasilja u obitelji iz rodne perspektive i da su usmjerene na ljudska prava i sigurnost žrtve
- da su zasnovane na holističkom pristupu koji sagledava odnos između žrtve, počinitelja i djece u kontekstu šireg društvenog okruženja
- osobito da imaju za cilj izbjegavanje sekundarne viktimizacije.

Spremnost za pronalaženjem što kvalitetnijih rješenja te uvažavanje i uočavanje poteškoća u provedivosti nekih zakonskih odredbi, najbolje je vidljiva u primjeru Izmjena i dopuna Kaznenog zakona iz 2015. godine u koji se ponovno uvrstilo kazneno djelo Nasilje u obitelji u čl.179 a. čime se proširila zakonska inkriminacija određenih oblika nasilja u obitelji.

Osim navedenih Konvencija, značajan doprinos razvoju reakcija na nasilje u obitelji imala je i Direktiva 2012/29 Europske unije o uspostavi minimalnih standarda, prava, podrške i zaštite žrtava zločina. Tako je Zakon o kaznenom postupku i Kazneni zakon implementirao niz njenih odredbi čime se postigla značajna usmjerenost na podršku i zaštitu prava žrtve tijekom kaznenog postupka. U operacionalizaciji ove Direktive, a s ciljem informiranja žrtve o njenim pravima i mogućnostima podrške i pomoći ustanova koje se bave ovom problematikom, Ministarstvo unutarnjih poslova izradilo je posebne obrasce i brošure koje se daju žrtvi već kod prvog kontakta s policijskim službenikom.

Navedene međunarodne smjernice koje su rezultirale intervencijama u domaće zakonodavstvo nesumnjivo su od velikog značaja, međutim, potrebno je posebno naglasiti da su domaća znanstvena i stručna javnost do sada kontinuirano ulagale velike napore u razvoj

zakonodavnih i postupovnih rješenja problematike nasilja u obitelji što je rezultiralo brojnim zakonskim i podzakonskim aktima (Prekršajni zakon, Zakon o zaštiti od nasilja u obitelji, Protokol o postupanju u slučaju nasilja u obitelji, Protokol u postupanju u slučaju seksualnog nasilja, Pravilnik o načinu izvršenja sigurnosnih mjera zabrane približavanja i udaljenja iz zajedničkog kućanstva i dr.).

Također, neupitno je da je razvoj zakonske regulative pratio i razvoj kontinuirane edukacije stručnjaka i međuresorske suradnje, što je u studenom 2010. godine rezultiralo osnivanjem Nacionalnog tima za prevenciju i suzbijanje nasilja nad ženama te županijskih timova za prevenciju i suzbijanje nasilja nad ženama, a sve temeljem Sporazuma o suradnji državnih tijela nadležnih za prevenciju i suzbijanje nasilja u obitelji kojeg su potpisala slijedeća ministarstva: Ministarstvo pravosuđa, Ministarstvo socijalne politike i mladih, Ministarstvo zdravlja, Ministarstvo znanosti obrazovanja i sporta, Ministarstvo uprave i Ministarstvo unutarnjih poslova. Nacionalni tim surađuje s brojnim obrazovnim institucijama i udrugama civilnog društva te provodi međuresorske edukacije županijskih timova, u kojima, uz predstavnike ministarstva kao potpisnika Sporazuma, sudjeluju i predstavnici općinskih državnih odvjetništava, županijskih sudova, obiteljskih sudova, Psihijatrijske bolnice za djecu i mladež, Poliklinika za zaštitu djece grada Zagreba te nevladine udruge. Praksa je pokazala da je ovakav način edukacije vrlo efikasan jer se uz stjecanje novih znanja razmjenjuju i iskustva te dogovaraju modeli postupanja, dakle, razvija se suradnički pristup koji je od strane stručnjaka koji su neposredno uključeni u rješavanje problematike obiteljskog nasilja uspješno ocijenjen.

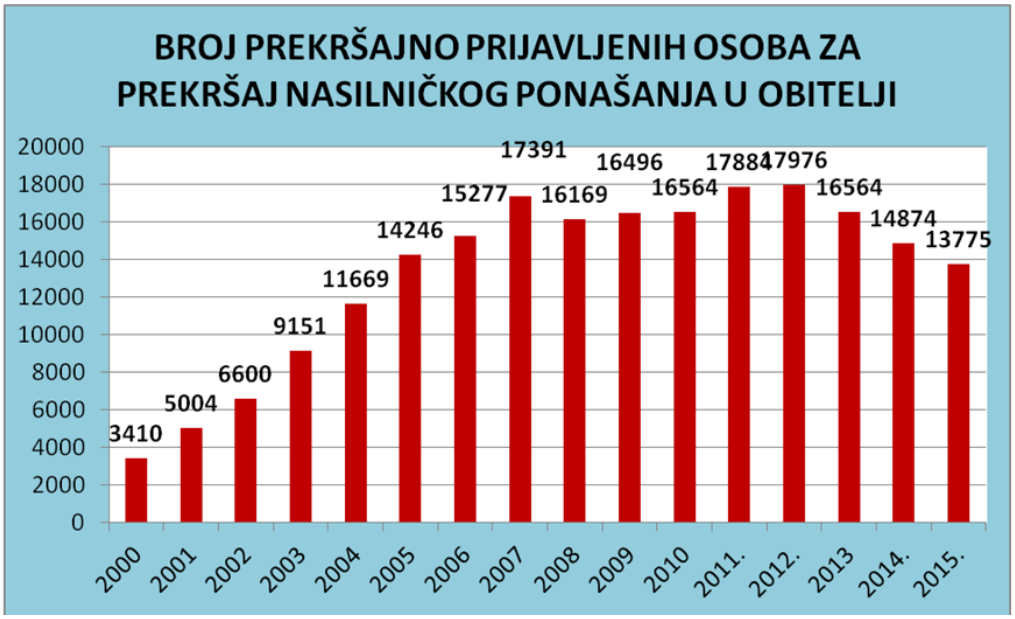
U cilju jačanja kapaciteta prevencije nasilja u obitelji Ministarstvo unutarnjih poslova provodi mjere Nacionalne politike za ravnopravnost spolova za razdoblje od 2011. do 2015. godine, te Nacionalne strategije za zaštitu od nasilja u obitelji za razdoblje od 2011. do 2016. godine, a mjere i ciljevi proizašli iz navedenih dokumenata implementirani su u provedbenim dokumentima, godišnjem planu rada te strateškim planovima Ministarstva. Krajnji rezultat navedenih strateških opredjeljenja su brojni preventivni projekti pokrenuti od strane policije na nacionalnoj i na regionalnim razinama, poput projekta „Živim život bez nasilja“, „Imam izbor“, „Podrška žrtvama kaznenih djela i prekršaja“.

Namjera ovog kratkog i segmentiranog prikaza razvoja društvenog odgovora na problematiku obiteljskog nasilja u posljednjih nekoliko godina bila je ukazati na kontinuitet i spremnost društva da podigne razinu kvalitete postupanja u slučajevima nasilja u obitelji, međutim, s pravom se pitamo je li to dovoljno promatrajući na godišnjoj razini broj počinjenih prekršaja i ubojstava u obitelji (grafikon 1. i 2.).

Kako je rasla svijest društva o štetnosti nasilja u obitelji, tako je rasla educiranost policijskih službenika što je rezultiralo kontinuiranim povećanjem prijavljivanja i otkrivanja prekršaja nasilničkog ponašanja u obitelji. Kontinuum rasta prekinut je 2013. godine kada je ukinuto kazneno djelo iz čl.215.a Nasilničko ponašanje u obitelji pa je dio nasilničkog ponašanja u obitelji procesuiran, umjesto u prekršajnom postupku, u kaznenom, što je dovelo do povećanja broja kaznenih djela s elementima nasilja. Nadalje, bilježi se broj ubojstava među članovima obitelji u odnosu na ukupan broj ubojstava, uz određene oscilacije u opadanju.

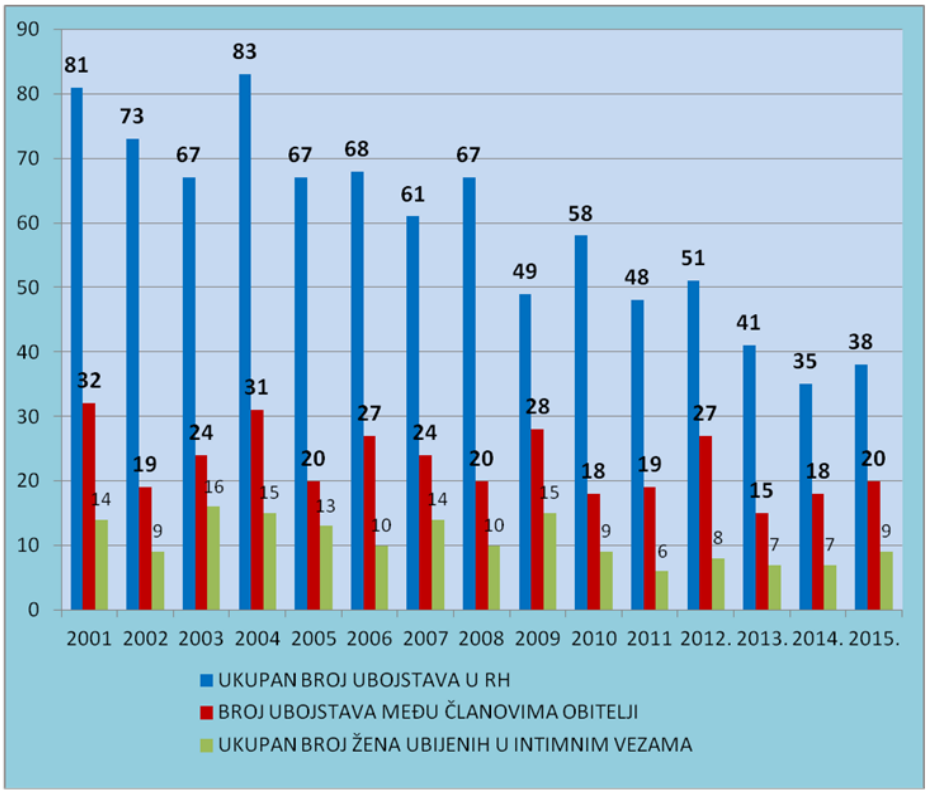
Možda je opravdano ovu pojavu barem djelomično pripisati uspješnim rezultatima prevencijskih programa koji su se provodili u prethodnom razdoblju.

Grafikon 1 - primjena čl. 4. Zakona o zaštiti od nasilja u obitelji – prekršaj «Nasilničko ponašanje u obitelji» u Republici Hrvatskoj za razdoblje od 01.01.2000. do 31.12.2015. god.



Izvor: Statistički pokazatelji, MUP-a RH 2008. – 2010.

Grafikon 2 - ukupan broj ubojstava u RH, ubojstava među članovima obitelj, te ukupan broj žena ubijenih u intimnim vezama



Izvor: Statistički pokazatelji MUP-a, RH

2. PRIMJENA LISTA PROCJENE RIZIKA U POLICIJSKOM POSTUPANJU

Praćenjem policijskih postupanja u slučajevima obiteljskog nasilja u zadnjih su se nekoliko godina iskristalizirale kritične točke u radu policije. Kako bi se unaprijedilo policijsko postupanje 2012. godine izrađen je provedbeni dokument pod nazivom *Standardizirani operativni postupak policije u slučajevima nasilja u obitelji* u kojem je jasno i detaljno razrađeno postupanje policije u slučajevima nasilja u obitelji, a sve s ciljem postizanja nacionalnog standarda policijskog postupanja prilikom pružanja intervencije povodom obiteljskog nasilja. Kvaliteta ovog SOP-a očituje se u jednostavnom i pristupačnom objašnjenju svakog pojedinog segmenta policijske intervencije pa ga se može nazvati i svojevrsnim vodičem koji policijskog službenika „korak po korak" vodi kroz intervenciju.

Već je u radu navedeno da je prevencija nasilja u obitelji strateški cilj MUP-a, da se kontinuirano analiziraju postupanja te identificiraju kritične točke, odnosno da se pronalaze novi načini njihovih rješavanja. Sve navedeno možemo pronaći u definicijama strategijskog menadžmenta (Buble i sur., 2005, Buble, 2008., Sikavica i sur. 2008) te se i policijsko postupanje u slučajevima nasilja u obitelji može promatrati kroz perspektivu procesa kojim se treba upravljati na način da se identificiraju mogući rizici te da ih se prati, kontrolira i njima upravlja.

O važnosti uvođenja procesa upravljanja rizikom govore Labaš i sur. (2012) koji smatraju da navedeni proces nije više samo potreba nego i imperativ ukoliko želimo slijediti iskustvo zemalja s policijskom tradicijom. Nadalje, autori ističu da su, osim na strateškoj razini, rizici u postupanju dio svakodnevnog rada, a upravljanje njima donosi povećanje učinkovitosti, u smislu povećanja sigurnosti građana, ali i bolje percepcije javnosti prema radu policije. Zato je svrsishodno nastojati utvrditi očekivane rizike koji se pojavljuju pri neposrednom pružanju policijskih usluga i tretirati ih na odgovarajući način internim nadzornim mehanizmima i aktivnostima.

Svjesni da neka kaznena djela i buduća ponašanja, posebice u slučajevima obiteljskog nasilja ne možemo predvidjeti, no možemo poduzeti određene mjere koje bi imale za cilj:

- prevenirati novo nasilje
- poboljšati dosljednost i utemeljenost odluka
- zaštiti žrtvu

Matijević, (2011) navodi kako Priručnik za kriminalističko istraživanje obiteljskog zlostavljanja britanske policije procjenu rizika definira kao proces procjenjivanja vjerojatnosti i prirode rizika koji predstavlja počinitelj za određenu žrtvu, djecu ili druge. Prema navedenom priručniku, svaka procjena rizika treba uključivati postupanje po ranije danim uputama, razumljive termine u opisivanju procjene rizika i kategorizacije, primjenu profesionalne procjene policijskog službenika, osiguranje dodatnih izvora informacija, kontinuiranu edukaciju policijskih službenika, superviziju specijaliziranih policijskih službenika za obiteljsko nasilje, identifikaciju osoba visokih rizika, obavijest žrtvi da se počinitelj smatra visokorizičnim za počinjenje novog napada te poduzimanje mjera zaštite žrtve.

Brojni su primjeri europskih zemalja u kojima policija primjenjuje liste procjene rizika budućeg ponašanja počinitelja, a o dobivenim rezultatima ovise odluke u samom postupku policije, ali i mjere iz nadležnosti pravosuđa. Svakako je važno naglasiti da liste ne jamče apsolutnu sigurnost u procjeni rizika te da je procjena rizika proces, a lista procjene rizika je alat koji pomaže policijskom službeniku da donese ispravnu odluku o daljnjem postupanju.

Temeljem izučavanja literature te nadasve na temelju iskustava domaćih stručnjaka u ovom području zaključujemo da su modeli procjene rizika u Engleskoj i Walsu, Austriji i Češkoj vrijedni primjeri koji mogu poslužiti kao model u kreiranju liste procjene rizika za potrebe hrvatske policije.

2.1. Procjena rizika od nasilja u obitelji, uznemiravanja te nasilja počinjenog zbog povrede časti (*domestic abuse, stalking and honour based violence - dash lista*)

U Engleskoj i Walesu postoji udruženje nazvano MARAC (Multi Agency Risk Assessment - Međuresorni tim za procjenu rizika) koju čine policija, državne institucije i udruge koje se bave podrškom i tretmanom počinitelja nasilja u obitelji, a u program MARAC ulaze počinitelji koji su procijenjeni kao visokorizični za ponavljanje nasilja u obitelji.

Za potrebe MARAC-a civilne organizacije koriste CAADA (*Coordinated Action Against Domestic Abuse* - Organizirano postupanje u slučajevima nasilja u obitelji) DASH (*Risk Identification Checklist* - Obrazac za procjenu rizika) dok policija kao standardan obrazac za procjenu rizika koristi *DASH Risk Identification Checklist* (Popis identificiranih rizika) koji je malo šira verzija *CADDA DASH RISK*.

DASH Risk Identification Checklist obuhvaća odgovore na pitanja podijeljena u četiri cjeline: trenutna situacija, djeca/uzdržavane osobe, povijest nasilja, počinitelj/zlostavljač. Na kraju obrasca ostavljen je prostor za slobodan tekst za dodatne napomene žrtve ili policijskog službenika.

Ovisno o rezultatima popisa procjene rizika i osobnoj profesionalnoj procjeni policijskog službenika ili drugog službenika počinitelji se temeljem danih odgovora u obliku DA i NE, rangiraju u tri kategorije: standardan, srednji i visok.

Nakon svake procjene rizika treba slijediti upravljanje detektiranim rizikom, Britanska policija upravljanje rizikom provodi kroz takozvani *RARA* (Remove, Avoid, Reduce and Accept) model:

- otkloniti rizik: uhititi počinitelja i pritvoriti ga
- izbjeći rizik: smjestiti žrtvu/važnog svjedoka u sklonište i/ili na počinitelju nepoznatu lokaciju
- smanjiti rizik: zajedničkom intervencijom, sigurnosnim planom za žrtvu, reagirati na kršenje mjera pod jamčevinom, koristi proaktivne zakonske mjere i uključiti slučaj u MARAC

– prihvatiti rizik: kontinuirano vršiti ponovnu procjenu rizika, kontinuirano multiagencijski intervenirati i planirati, pružati podršku žrtvi uz pristanak žrtve i počinitelja da budu uključeni u MARAC ili sličnu multiagencijsku mrežu

Stručnjaci su se usuglasili da sobe za koje se na CAADA DASH ili DASH RIC prikupi više od 14 pozitivnih odgovora, ali i osobe za koje je prikupljen manji broj bodova, ali policijski službenik ili stručnjak u NGO/socijalnoj skrbi/zdravstvu procjeni da se ipak radi o visoko rizičnom pojedincu uključuju se u MARAC, odnosno žrtvi se unutar multiagencijske mreže pruža podrška i pomoć, izrađuje se i provodi sigurnosni plan te planira i provodi rad s počiniteljem.

2.2.Skala procjene rizika (*Danger Assessment Scale*)

Danger Assessment Scale je lista procjene rizika koju koristi austrijska policija koja kao odgovor na nasilje u obitelji također nudi multiagencijski pristup rješavanju problema kroz suradnju policije i nevladinih i vladinih organizacija.

Danger Assessment Scale američke autorice dr.sc. Jacquelyn Campbell, koristi se u policijskim sustavima i sustavima zdravstva posljednjih 25 godina; 2004. godine skala je modificirana u nekoliko pitanja, ali se temeljni dio nije mijenjao.

Upitnik obuhvaća pitanja o povećanju učestalosti ili težine fizičkog nasilja, posjedovanju/korištenju/prijetnjama vatrenim oružjem, prekidu zajednice i napuštanju zajednice u posljednje vrijeme, radnom statusu, prijetnjama ubojstvom, ranijim uhićenjima počinitelja, očinstvu nad djetetom u zajednici, prisili na seksualne aktivnosti, pokušajima davljenja, zlouporabi droga, alkohola, kontroli nad žrtvom, ljubomori, nasilju tijekom trudnoće, prijetnjama ili pokušajima suicida, prijetnjama ubojstvom djeci, subjektivnoj procjeni žrtve o stupnju vjerojatnosti da počinitelj ubije djecu, praćenju, uhođenju, oštećenju stvari, uznemiravanju putem telefona, prijetnjama ili pokušajima žrtve da počini suicid.

Pitanja, odnosno odgovori rangiraju se u četiri grupe: mala razina rizika, postojanje rizika, visoka razina rizika i jako visoki rizik.

*2.3.*Procjena rizika od nasilja u bračnoj zajednici (*Spousal Assault Risk Appraisal – SARA)*

Spousal Assault Risk Apprisal (SARA) kanadskih autora Kropp, Hart, Webster i Eaves kreiran je 1994. godine, a 2000. godine modificiran od strane Randalla Kroppa temelji se na empirijskim indikatorima rizika. Pitanja su podijeljena na tri glavna područja: kriminalna prošlost, psihosocijalna prilagodba, povijest partnerskog nasilja.

U obrazacu je ostavljen prostor za slobodan unos teksta za druge utvrđene rizične faktore te procjenu rizika napada partnera ili bivšeg partnera kao i procjenu ugroženosti drugih osoba (djece, novog partnera i sl.).

Mogući odgovori su: odsutno, moguće i prisutno, s maksimalnim brojem od 40 bodova. Rizik od počinjenja novog napada se kategorizira kao: nizak, umjeren i visok.

U procesu procjene rizika od ponavljanja, eskaliranja nasilja u obitelji *SARA* listu koristi češka policija, pri čemu su kao i druge države u okruženju usmjereni na multiagencijski pristup u rješavanju obiteljskog i drugog nasilja u domu te osiguranje potrebne podrške i pomoći žrtvama (Matijević, 2011).

3. OBRAZAC ZA PROCJENU RIZIKA OD PONAVLJANJA NASILNIČKOG PONAŠANJA U OBITELJI

Pri uvođenju novih metoda u pristupu rješavanja identificiranih kritičnih točaka kao što su, primjerice, procjena rizika počinitelja od ponavljanja nasilničkog ponašanja u obitelji, predstavlja izazov koji podrazumijeva traženje odgovora na pitanja kada i na koji način procjenjivati rizik, tko će ga raditi i zašto? Drugim riječima, što će se poduzeti s dobivenom procjenom, odnosno kako će se upravljati identificiranim rizikom. Obzirom na široki raspon mogućnosti procjenjivanja rizika u svakoj pojedinoj policijskoj radnji prilikom interveniranja u slučajevima obiteljskog nasilja, fokus treba staviti na procjenu rizika u svrhu donošenja što bolje procjene budućeg ponašanja počinitelja nasilja u obitelji. Za potrebe policijske prakse, a temeljem znanstvenog istraživanja koje je provedeno na području RH u razdoblju od 2005. do 2010. godine (Pavliček i sur., 2014) izrađen je standardizirani „Obrazac procjene rizika od ponavljanja nasilničkog ponašanja u obitelji“.

Svrha obrasca procjene rizika je dati policijskom službeniku koji pruža intervenciju povodom nasilja u obitelji alat koji će mu pomoći identificirati počinitelje koji su u riziku ili visokom riziku za počinjenje novog i/ili još težeg nasilja, ponavljanja i/ili eskaliranja nasilja sve do ubojstva.

Cilj obrasca je da se identificirani rizici stave pod nadzor, odnosno da se njima upravlja, čime bi se postiglo smanjenje mogućih negativnih posljedica. Ako policijski službenici budu koristili obrazac za procjenu rizika u svom svakodnevnom radu, moći će objektivnije i argumentirano donositi odluke o daljnjem postupanju s počiniteljem - o njegovom eventualnom uhićenju, privođenju, određivanju mjera opreza, određenju neke od zaštitnih mjera, ili nekom obliku pomoći žrtvi.

Obrazac je namijenjen policijskim službenicima koji pružaju intervenciju povodom dojave o nasilju u obitelji za prvu procjenu i pomoć pri donošenju odluke o daljnjem tijeku postupanja (privođenje, mjere opreza, predlaganje adekvatnih zaštitnih mjera ili mjera opreza). Posebnu primjenu ovaj Obrazac će imati za liniju rada maloljetničke delinkvencije i kriminaliteta na štetu mladeži i obitelji jer će ga specijalizirani policijski službenici koristiti kao bazu za daljnji proces procjene, odnosno pri donošenju odluke u kojem smjeru je potrebno nastaviti policijsko postupanje.

Pri izradi Obrasca uvažena je činjenica da je procjena rizika sistematičan, sveobuhvatni proces u koji je potrebno uključiti što je moguće više izvora. Potrebno je u zajednički kontekst staviti osobine ličnosti, posebna obilježja počinitelja i žrtve, realne životne okolnosti, detektirati okolnosti koje mogu biti okidač za ponavljanje nasilja i tek potom donijeti procjenu mogućeg rizika, kao i plan koji sadržava razloge zbog kojih se procjena rizika uopće

radi uključujući plan aktivnosti koje će se poduzeti kako bi se buduće nasilje spriječilo. U daljnjem tekstu razraditi će se najčešći rizici nasilja u obitelji.

3.1.Rizici vezani uz oblike počinjenog nasilja

Kao opće prihvaćene visoke čimbenika rizika možemo izdvojiti prijetnje smrću žrtvi ili njoj bliskoj osobi, nasilništvo prema djeci ili drugim članovima obitelji te posebno okrutne oblike nasilništva koje podrazumijevaju ponižavajuće ponašanje ili iživljavanje na žrtvi. Također, visok rizik predstavljaju i ponašanja počinitelja kojima se ograničava žrtva u njenom kretanju, kontroliraju njeni kontakti te financijska sredstva kojima ona raspolaže. Iz prakse je poznato da su osobito opasne izjave: „Prije ću te ubiti nego ti dati razvod“, „Bit ćeš moja ili ničija“, „Pripadaš meni i neće te nitko drugi imati“; zato je važno prepoznati opasnost takvih izjava te utvrditi kome sve počinitelj prijeti te sadržaj tih prijetnji.

3.2.Rizici vezani uz oružje

Upotreba vatrenog oružja u izvršenju kaznenih djela ubojstva i pokušaja ubojstva među članovima obitelji na drugom je mjestu po obliku sredstava izvršenja navedenih kaznenih djela u RH (Pavliček i dr., 2014), točnije 32,2 posto od svih počinjenih ubojstava i pokušaja ubojstava među članovima obitelji počinjeno je uporabom vatrenog oružja. Do sličnog zaključka došli su i Belknap i suradnici (2012) naime, oni su u svom istraživanju dobili pokazatelj da čak 8 od 12 ubojstava bude počinjeno vatrenim oružjem. Navedeni pokazatelji konkretna su smjernica da posjedovanje oružja u slučajevima obiteljskog nasilja predstavlja rizik kojem se treba posvetiti posebna pozornost.

3.3.Iskaz žrtve

Prilikom obavljanja razgovora sa žrtvom obiteljskog nasilja policijski službenik će na posebno obazriv i taktički ispravan način vođenja razgovora utvrditi osobni stav žrtve u odnosu na počinitelja i situaciju nasilja koja joj se dogodila. Ovaj dio policijskog posla smatramo vrlo složenim jer žrtve često zbog straha od počinitelja prikrivaju stvarnu situaciju u obitelji pa ih je potrebno ohrabriti ili će davati iskaz prepun nepovezanih i naizgled nebitnih činjenica temeljem kojih je teško stvoriti jasnu sliku o događaju ukoliko žrtvu ne usmjerimo na izravnost i konkretnost u izjavljivanju. Procjena stanja i izjave žrtve uz elementarnu edukaciju koja policijskom službeniku pomaže u obavljanju zadaća, iziskuje i subjektivni osjećaj policijskog službenika koji se temelji na iskustvu i neposrednom opažanju i doživljaju da „nešto“ nije u redu ili da bi se „nešto“ moglo dogoditi. Bez obzira na moguće poteškoće vezane uz žrtvine izjave, svakako je potrebno utvrditi što žrtva smatra da je počinitelj u stanju učiniti slijedeće, na čemu se temelji njezina procjena te sukladno tome i svim ostalim prikupljenim saznanjima odrediti daljnje policijsko postupanje.

3.4.Rizici vezani uz raniju prijavljivanost počinitelja

Prema Pavliček i sur. (2014), u 12 % slučajeva ubojstava i pokušaja ubojstava među članovima obitelji počinitelj je od ranije evidentiran za kaznena djela i prekršaje s elementima nasilja, s time da je kod recidivizam vrlo bitno naglasiti da je u ovim slučajevima „tamna

brojka“ kriminaliteta izrazito visoka jer je istim istraživanjem utvrđeno da je u više od 50 posto slučajeva od ranije postojalo nasilja u obitelji ali da nije bilo prijavljivano.

Posebnu se pažnju prilikom policijskog postupanja mora posvetiti utvrđivanju činjenice o počiniteljevom učestalijem nasilničkom ponašanju u zadnjih godinu dana i porastu intenziteta iskazanog nasilja tijekom kojeg počinitelj gubi kontrolu nad svojim postupcima, jer to predstavlja izrazito visok rizik od ponavljanja.

3.5.Rizici vezani uz karakteristike počinitelja

Poznavanje obilježja počinitelja kao što su suicidalnost, duševna bolest, ovisnost o alkoholu ili drogi, socijalna izoliranost ili pripadnost nekoj etničkoj skupini mogu pridonijeti procjeni rizičnosti od budućeg nasilničkog ponašanja, jer socijalne i osobne karakteristike predstavljaju kontinuirani obrazac ponašanja važan za procjenu rizika.

Raniji pokušaji suicida ili prijetnje da će izvršiti suicid upućuju na vjerojatnost ponavljanja nasilničkog ponašanja, čemu u prilog govore pokazatelji iz istraživanja Pavliček i dr. (2014) da je 12, 8 % počinitelja ubojstva i pokušaja ubojstva člana obitelji pokušalo suicid u ranijem razdoblju. Nadalje, iz dobivenih pokazatelja proizlazi da je čak 40,4 % počinitelja obuhvaćenih navedenim istraživanjem bilo ovisno a alkoholu te 9,8 % o psihoaktivnim sredstvima, a da je kod 36 % počinitelja evidentiran neki oblik duševne bolesti. Motiv počinjenja obiteljskog nasilja s teškim posljedicama najčešće je netrpeljivost i to u 25 % slučajeva, a odmah poslije po učestalosti dolazi ljubomora i to u 15 % slučajeva. Patološka ljubomora kao karakterno obilježje počinitelja predstavlja rizik jer je za očekivati da će se s takvim ponašanjem nastaviti ukoliko počinitelj nije spreman promijeniti svoje ponašanjem uz stručnu pomoć.

3.6.Rizici vezani uz neke značajnije događaje

Praksa nam govori da je vrlo značajno za rizik od budućeg ponašanja utvrditi je li se neposredno prije nasilnog događaja zbio neki poseban događaj (neriješeni imovinsko pravni odnosi, financijske poteškoće, ostanak bez posla, zdravstveni problem,brakorazvodna parnica, problem oko kontakata s djecom, preljub) jer on može biti poticaj za ponavljanje nasilja, a posebice je velik rizik od eskalacije novog nasilja nakon policijske intervencije, kada je počinitelj ljut na žrtvu jer je tražila policijsku zaštitu.

Na temelju znanstvenog istraživanja provedenog na području Republike Hrvatske te metoda procjene rizika, koje koriste druge policije, kao dobar primjer kreiran je hrvatski Obrazac procjene rizika od ponavljanja nasilničkog ponašanja.

Obrazac procjene rizika od ponavljanja nasilničkog ponašanja POLICIJSKA UPRAVA /ODJEL/ POLICIJSKA POSTAJA:	BROJ SPISA		
IME I PREZIME POČINITELJA	dob počinitelja, datum izvršenja, zakonska kvalifikacija djela		
IME I PREZIME ŽRTVE	dob žrtve, srodnički odnos sa počiniteljem		
UPIŠI OZNAKU X U KOLONE PONUĐENIH ODGOVORA	ne	da	napomena
Je li počinitelj prijetio da će usmrtiti žrtvu ili njoj blisku osobu			
Je li počinitelj bio nasilan prema djeci			
Je li počinitelj bio nasilan prema drugim članovima kućanstva ili drugim osobama Ukoliko da, je li im nanosio ozljede			(kome i na koji način)
Je li počinitelj žrtvu ranije pratio, uhodio, nadzirao			
Je li počinitelj žrtvu ograničavao u kretanju, kontrolirao financijska sredstva, kontakte s drugima			
Je li počinitelj iskazivao/iskazuje pretjeranu ili patološku ljubomoru u seksualnom smislu i/ili posesivnost prema žrtvi			
Je li počinitelj seksualno zlostavljao žrtvu			
Je li počinitelj fizički zlostavljao žrtvu Ukoliko da, je li žrtva zadobila ozljede Je li žrtvi ugrožavao život gušenjem, davljenjem			
Je li se počinitelj ponašao posebno okrutno, ponižavajuće ili bestijalno prema žrtvi			
Posjeduje li ili je počinitelj posjedovao oružje, ukoliko da, koje oružje i je li korišteno za prijetnje ili nanošenje ozljeda			
Iskazuje li žrtva strah od počinitelja			
Ponaša li se počinitelj učestalije nasilno, je li nasilje jačeg intenziteta (u posljednjih godinu dana)			
Je li počinitelj bio ranije evidentiran kao počinitelj nasilja prema bliskoj osobi: – kaznenog djela – prekršaja – nekog dr. kaznenog djela/prekršaja s elementima nasilja ***Posebno dodatno vrednovati ukoliko je višestruki počinitelj prekršaja ili kaznenih djela***			
Je li prekršio izrečenu mjeru opreza ili zaštitnu mjeru (u posljednjih godinu dana)?			
Postoje li saznanja o ranijem **neprijavljenom** nasilničkom ponašanju počinitelja?			(kome i na koji način)
Postoje li saznanja da je počinitelj pokušao suicid ili prijetio da će to učiniti?			
Je li počinitelj dijagnosticiran kao psihijatrijski bolesnik			

Je li počinitelj socijalno izoliran Je li žrtva socijalno izolirana			
Je li se počinitelj nasilnički ponašao pod utjecajem alkohola, droga			
Je li inače prekomjerno konzumira, alkohol, koristi droge			
Je li počinitelj pripada nekoj etničkoj, kulturnoj skupini koja nije domicilna, zajednice koja ima drugačiju kulturu i običaje			
Je li se neposredno prije nasilnog događaja zbio neki poseban događaj (neriješeni imovinsko pravni odnosi, financijske poteškoće, ostanak bez posla, ostanak bez stana, zdravstveni problem, nova dijagnoza, preljub – čiji ili nešto dugo)			
Je li u tijeku proces brakorazvoda/ili je žrtva počinitelja napustila ili najavila da će ga napustiti			
Postoji li problem oko kontakata s djecom (kakav)			
OPAŽANJA POLICIJSKOG SLUŽBENIKA NA MJESTU DOGAĐAJA: emocionalna i dr. stanja žrtve i počinitelja: uznemirenost, strah, agresivnost, hladnokrvnost, primijećene ozljede, oštećene stvari, žrtva osoba sa invaliditetom ili posebno ranjiva zbog drugih razloga : dijete, psihički bolesnik, starija osoba, strani državljanin, trudnica			

Temeljem saznanja pribavljenih od žrtve

_____

Upitnik ispunio policijski službenik/ca

ALARMANTNO VISOK RIZIK je bilo koja kombinacija potvrdnih odgovora u pitanjima o prijetnjama ubojstvom, iskazanim namjerama ili promišljanjima o samoubojstvu tijekom brakorazvoda ili prekida veze uz iskazivanje seksualne ljubomore primjerice > 25 +3/6 kritičnih pitanja

VISOK RIZIK; POSTOJEĆI RIZIK; NIZAK RIZIK: O -5 bodova izuzev kritičnih pitanja

4. ZAKLJUČAK

Trendovi razvoja policijskog rada posljednjih se godina kreću u smjeru postizanja više razine kvalitete policijskog rada kroz pronalaženje učinkovitih metoda (alata) verificiranih od strane znanosti i prakse. Jedna od metoda koja je proizašla iz teorijskih i znanstvenih istraživanja, a koja je svoje mjesto pronašla u policijskoj praksi brojnih zemalja je primjena lista procjene rizika od ponavljanja određenog ponašanja. U ovom radu prikazane su različite metode u procjeni rizika te rezultati nekih domaćih istraživanja kako bi se lakše identificirali rizični čimbenici značajni za procjenu rizika. Temeljem navedene identifikacije izrađen je Obrazac za procjenu rizika od ponavljanja nasilničkog ponašanja u obitelji. U slijedećoj testnoj fazi (šest mjeseci) obrazac će se koristiti u svakodnevnoj policijskoj praksi, nakon čega će uslijediti konačna verifikacija. Policijske službenike koji će u testnoj fazi primjenjivati ovaj Obrazac dodatno će se educirati te će se po završetku testne primjene od istih tražiti mišljenje kako bi se utvrdile eventualne poteškoće u primjeni. Očekujemo da će za evaluaciju i kasniju primjenu biti zainteresirani i drugi sudionici u procesu suzbijanja nasilničkog ponašanja u društvu, kao što su pravosuđe, centri za socijalni rad, nevladine udruge, od kojih će se zatražiti mišljenje i eventualni prijedlozi s ciljem poboljšanja samog Obrasca i njegove primjene.

LITERATURA

Belknap, L., Larson, D.L., Abrams, L.M., Garcia, C., Anderson-Block, K. (2012). Types of Intimate Partner Homicides Committed by Women. Self-Defense, Proxy/Retaliation, and Sexual Proprietariness, Homicide Studies 16(4) 359-379.

Buble, M., Cingula, M., Dujanić, M., Dulčić, Ž., Gonan Božac, M., Galetić, L., Ljubić, F., Pfeifer, S., Tipurić, D. (2005). Strateški menadžment. Zagreb: Sinergija.

Buble, M. (2006). Osnove menadžmenta. Zagreb: Sinergija.

Labaš, D., Dujmović, Z., Magušić, F., (2012). Procedure policijskih postupanja kroz rizike u funkciji upravljanja ljudskim potencijalima. Zbornik radova Menadžment i sigurnost, 7. znanstveno stručne konferencije, str. 376-388.

Matijević, A. (2011). Komparativni prikaz procjena rizika kod počinitelja nasilja u obitelji Policija i sigurnost, Zagreb, godina 20. (2011), broj 2, str. 223-229.

Pavliček, J., Kondor Langer, M., Milivojević, L., Odeljan, R., Matijević, A., Modrić, I., Damjanović, N. (2014). Ubojstva u obitelji. Zagreb: Međunarodno kriminalističko udruženje.

Radić, I., Radina, A. (2014). Zaštita od nasilja u obitelji: obiteljskopravni, prekršajnopravni i kaznenopravni aspekt. Zbornik radova Pravnog fakulteta u Splitu, god. 51, 3/2014., str. 727.-754.

Sikavica, P., Bahtijarević-Šiber, F., Pološki Vokić, N. (2008). Temelji menadžmenta. Zagreb: Školska knjiga.

Davorka Martinjak
Anita Matijević
Renata Odeljan

CHECKLIST FOR RISK ANALYSIS OF DOMESTIC VIOLENCE RECIDIVISM

Summary

Based upon a long-lasting policing practice involving domestic violence a need has been recognized to develop effective methods for making risk assessments of future domestic violence incidents. The purpose of a standardized risk assessment form (also known as checklist) is of great importance since decisions on precautionary and protection measures, decisions on conditions for the arrested and for bringing perpetrators to justice, retention proposals, as well as proposals to include other institutions in working with the offender will be more objective and more relevant. Risk factors relevant for risk assessment have been identified based upon a research involving 235 police files and court decisions involving family member murders and attempted murders committed in the Republic of Croatia in the period from 1 January 2005 through 31 December 2010. This risk factor identification resulted in the checklist for assessing the risk of repeated domestic violence, which will be used by police officers on a daily basis in the next six-month testing phase, followed by a final verification of the instrument.

Key words: *domestic violence, risk assessment, police officers, prevention.*

STRUČNI RAD

Spomenko Relić[151]

USPOREĐIVANJE KONTAKATA MOBILNIH UREĐAJA OSTVARENIH PREKO ĆELIJA BAZNIH STANICA

Sažetak

Uz pretpostavku da je nepoznati korisnik, najčešće počinitelj kaznenog djela, koristio mobilni uređaj za ostvarivanje kontakata u događajima koji su određeni prostorno (ciljana područja) i vremenski (vremenska razdoblja), uspoređivanje podataka o kontaktima na ćelijama baznih stanica telekomunikacijskih operatora može rezultirati identifikacijskim podacima jednog mobilnog uređaja ili više njih koji su zabilježeni na više ciljanih područja, a dobiveni podaci mogu djelotvorno usmjeriti kriminalističko istraživanje, skratiti utrošeno vrijeme i smanjiti troškove.

U radu se daje pregled zakonskih osnova za pribavljanje i obradu podataka o telekomunikacijskom prometu, daju se objašnjenja osnovnih tehničkih pojmova potrebna za razumijevanje obrađivane teme te prikaz strukture i značenja ulaznih podataka koji se obrađuju sa smjernicama za optimiziranje odabira ulaznih podataka. Koristeći simbolični primjer ulaznih podataka za skupove ćelija baznih stanica koje pokrivaju različita ciljana područja, objašnjava se metoda uspoređivanja podataka pogodna za računalnu obradu i optimizirana za brže dobivanje rezultata. Zasebno se obrađuje primjer djelomičnog preklapanja skupova ćelija ciljanih područja s dopunom metode uspoređivanja podataka koja smanjuje količinu "lažno pozitivnih" rezultata uz postizanje većeg broja mogućih rezultata. Objašnjavaju se posebnosti uspoređivanja kontakata u slučaju potpunog preklapanja skupova ćelija ciljanih područja (isto ciljano područje u različitim vremenskim razdobljima).

Ključne riječi: *telekomunikacijski promet, ćelije baznih stanica, uspoređivanje kontakata, preklapanje skupova ćelija, optimiziranje.*

1. UVOD

Suvremeno društvo brzo se razvija u tehnološkom smislu. Širokom krugu građana dostupni su sve napredniji načini komunikacije koji se razvijaju i unapređuju praktično svakodnevno, olakšavajući na taj način život i na osobnoj i na poslovnoj razini. Takav tehnološki razvoj društveno je ne samo prihvatljiv nego i poželjan; bez njega teško je i zamisliti gospodarski rast i razvoj što je nužnost modernog društva.

Naivno bi bilo misliti da tehnologiju, a time i tehnološki napredne načine komunikacije koriste samo oni koji poštuju zakone. Nove tehnologije vrlo brzo su usvojili i koriste ih počinitelji kaznenih djela jer im to pruža bitnu prednost pred "konkurencijom"

[151] Spomenko Relić, dipl. ing., MUP RH, Policijska uprava virovitičko-podravska, Služba kriminalističke policije, e-mail: srelic@mup.hr

drugih počinitelja, ali i prednost ispred policije čija je zadaća otkriti i obraditi postojeća i spriječiti moguća nova kaznena djela. Zato je nužno da policija neprekidno usvaja i koristi nove tehnologije, a zbog uvijek prisutne ograničenosti dostupnih resursa vrlo je poželjno razvijati metode obrade dostupnih podataka koje daju kvalitetnije konačne rezultate.

Temeljem zakonskih odredbi policija u RH ima mogućnost pribavljanja podataka o uspostavljanju telekomunikacijskih kontakata mobilnih uređaja u određenom vremenu i ostvarenih preko ćelija baznih stanica koje pokrivaju određeno područje. Ako je počinitelj određenog kaznenog djela koristio mobilni uređaj za komunikaciju u traženom vremenu i na traženom području, podaci o kontaktu i korištenom mobilnom uređaju bit će sadržani u skupu pribavljenih podataka. Problem koji ovdje treba riješiti jest izdvajanje i utvrđivanje mobilnog uređaja mogućeg počinitelja, odnosno što manjeg broja mogućih mobilnih uređaja (interesantni mobilni uređaji) iz redovno velikog skupa ulaznih podataka. Za rješavanje je prvo potrebno utvrditi barem još jedan dodatni događaj[152] određen prostorno i vremenski, za koji postoji što veća vjerojatnost da je i u njemu korišten mobilni uređaj s podacima koji su u skladu s onima iz prvog promatranog događaja te pribaviti podatke o uspostavljanju telekomunikacijskih kontakata mobilnih uređaja kao i za prvi događaj. Tek tada je moguće pristupiti uspoređivanja podataka i izdvojiti mobilne uređaje koji se pojavljuju u više interesantnih događaja.

Zbog količine podataka u ulaznim skupovima podataka praktično je nužno za to koristiti računalnu obradu podataka. Jedan od postupaka koji se pokazao uspješnim u praksi je primjena vizualnoga analitičkog programa *i2 Analyst's Notebook*, no zbog načina korištenja takvog programskog alata postoje određene poteškoće u dobivanju kvalitetnijih rezultata obrade u slučajevima kada se skupovi ćelija za područja obrađivanih događaja djelomično preklapaju.

Zato je korisno razviti metode obrade podataka pohranjenih u prikladne računalne baze podataka koje će što više suziti skup mogućih rezultata i time izbjeći "lažno pozitivne" rezultate. Rezultati takve obrade mogu se dalje dodatno obrađivati vizualnim analitičkim programom ili izravno koristiti u daljnjoj operativnoj obradi.

2. ZAKONSKE OSNOVE ZA PRIBAVLJANJE I OBRADU PODATAKA[153]

Policijska ovlast pribavljanja podataka o uspostavljanju telekomunikacijskog kontakta temeljena je na Zakonu o policijskim poslovima i ovlastima[154], koji u članku 68. stavku 1. određuje da policija može od davatelja komunikacijskih usluga zatražiti provjeru istovjetnosti, trajanja i učestalosti komunikacije s određenim elektroničkim komunikacijskim adresama radi:

[152] Dodatni događaj u širem smislu; povoljno bi bilo da predstavlja *drugo* kazneno djelo sa sličnim načinom izvršenja, ali ako se takvo kazneno djelo ne može odrediti, dodatni događaj može se pokušati odrediti, npr. pomoću postavljene pretpostavke izvršenja poznatog kaznenog djela (scenarij).

[153] Namjera je dati osnovni pregled zakonskih osnova za pribavljanje i obradu podataka o uspostavljanju telekomunikacijskog kontakta, a ne prikazati sve okolnosti i posljedice navedenih zakonskih odredbi.

[154] Zakon o policijskim poslovima i ovlastima. Narodne novine 76/09., 92/14., članak 68.

- *sprječavanja i otkrivanja kaznenih djela za koja se progoni po službenoj dužnosti i njihovih počinitelja*
- sprječavanja opasnosti i nasilja
- traganja za osobama i predmetima.

Stavak 2. istog članka određuje da zahtjev za podacima može obuhvaćati i utvrđivanje položaja komunikacijskog uređaja i utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju te identifikacijske oznake uređaja.

Zahtjev je temeljen na *pisanom odobrenju* načelnika Uprave kriminalističke policije ili načelnika Policijskog nacionalnog ureda za suzbijanje korupcije i organiziranog kriminaliteta ili načelnika policijske uprave, a u njihovoj odsutnosti osoba koje ih zamjenjuju. Pritom se odobrenje temelji na činjenicama iz kojih je vidljivo da se *drugim radnjama nije mogao ili se neće moći postići cilj policijskog posla ili bi postizanje tog cilja bilo povezano s nerazmjernim teškoćama*.

Osim temeljem članka 68. Zakona o policijskim poslovima i ovlastima, podatke o položaju komunikacijskog uređaja policija može zatražiti i temeljem članka 80. istog Zakona[155], no zbog različite naravi i oblika takvih podataka oni se ne koriste kod obrada podataka koje se ovdje razmatraju.

Pribavljeni podaci koriste se za analitičke obrade i operativno usmjeravanje kriminalističkih istraživanja, a ako se podaci o uspostavljanju telekomunikacijskog kontakta žele koristiti kao dokaz u kaznenom postupku, tada takve podatke policija treba pribaviti na zahtjev državnog odvjetnika i na temelju naloga suca istrage ili na temelju pisanog pristanka registriranog vlasnika ili korisnika komunikacijskog sredstva, što je određeno u članku 339.a Zakona o kaznenom postupku[156].

Zakon o policijskim poslovima i ovlastima u članku 1. stavku 1. točki 8. određuje analitičku obradu kao postupak analize dostupnih saznanja iz javnih i drugih izvora te podataka dobivenih na temelju primjene pojedinih policijskih ovlasti, dok u članku 11. stavku 2. određuje da se analitička obrada može provesti radi utvrđivanja razloga za provedbu kriminalističkog istraživanja te tijekom kriminalističkog istraživanja.

Obveza telekomunikacijski operatora za čuvanju podataka o telekomunikacijskom prometu za razdoblje od posljednjih 12 mjeseci određena je u članku 20. Uredbe o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama.

[155]Zakon o policijskim poslovima i ovlastima. Narodne novine 76/09., 92/14., članak 80.
[156]Zakon o kaznenom postupku. Narodne novine145/13., 152/14., članak 339.a.

3. OSNOVNI TEHNIČKI POJMOVI

Telekomunikacijski operator je pravna osoba koja na temelju propisa i/ili ugovora raspolaže javnom telekomunikacijskom mrežom ili dijelovima povezanim s tom mrežom i obavlja poslove mrežnog operatora i davatelja telekomunikacijskih usluga[157].

Mobilni telefon ili mobitel (engl. *mobile phone*, često i *cell phone*) prijenosni je (mobilni) elektronički uređaj koji može pozvati ili biti pozvan od drugog sličnog uređaja i na taj način ostvariti kontakt[158]. Za uspostavljanje kontakta koristi se bežično spajanje na mrežu baznih stanica.

IMEI broj (engl. *International Mobile Equipment Identity*) jedinstveni je broj dodijeljen svakom mobilnom uređaju; može biti korišten za ograničenje pristupa mobilnog uređaja pojedinim mobilnim mrežama (npr. iz poslovnih razloga ili zbog onemogućavanja korištenja ukradenih uređaja).

IMSI broj (engl. *International Mobile Subscriber Identity*) i *MSISDN* broj (engl. *Mobile Station International Subscriber Directory Number*) važni su brojevi za identificiranje pretplatnika na mobilnoj telefonskoj mreži; IMSI broj pohranjen je na SIM kartici (engl. *Subscriber Identity Module* – kartica koja se umeće u mobilni uređaj) i koristi se kao ključ u "bazi pretplatnika", dok je MSISDN zapravo telefonski broj koji se bira za uspostavu kontakta mobilnim uređajem. SIM kartica ima jedinstveni IMSI broj koji se ne mijenja, dok se MSISDN broj s vremenom može promijeniti, a moguće je čak i da SIM kartica istodobno ima pridijeljen sekundarni MSISDN broj (npr. za podatkovni promet).

Bazna stanica (engl. *Base Transceiver Station* – BTS, *cell site, cell tower*) u smislu mobilne telefonije je skup primopredajnika koji omogućuju kontakt između mobilnih telefona i šire telefonske mreže; u fizičkom smislu to je povišena struktura na koju su smješteni primopredajnici, tj. antene i drugi elektronički uređaji koji osiguravaju bežičnu vezu radiovalovima između mobitela (odnosno mobilnih uređaja općenito) i bazne stanice te između različitih baznih stanica.

Ćelija (engl. *cell*) zemljopisno je područje koje pokriva signal jednog od primopredajnika za komunikaciju između mobilnog uređaja i bazne stanice, smještenog na baznoj stanici; zbog toga se često i za određenu antenu primopredajnika koristi naziv *ćelija*. Sva komunikacija između mobilnog uređaja i bazne stanice, dok je mobilni uređaj na području pokrivenosti određene ćelije, odvija se preko primopredajnika koji svojim signalom pokriva tu ćeliju i ima svoju identifikaciju (*Cell ID*).

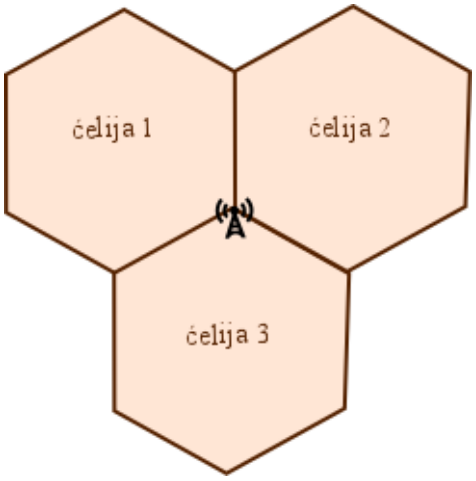
Pokrivenost ćelija često se prikazuje u obliku pravilnih heksagona (što je dovoljno za razinu pojednostavljivanja prilikom obrade pojedinih tema), no u stvarnosti je to područje nepravilnog oblika na koji najviše utječe konfiguracija terena (postoje i drugi utjecaji, npr. atmosferske prilike). Područje pokrivanja ćelije najčešće podsjeća na laticu cvijeta, pa je za

---

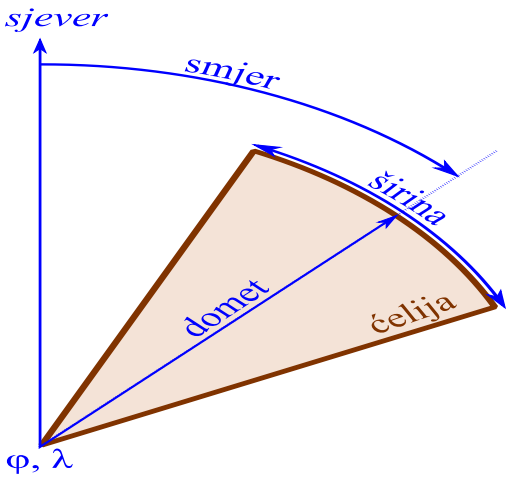
[157]Uredba o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama. Narodne novine 64/08., 76/13., članak 3.

[158]U početku razvoja mobilne komunikacije glavna je bila funkcija glasovne komunikacije, no u novije vrijeme dodane su funkcije kratkih tekstualnih poruka (SMS, engl. *Short Message Service*), kratkih slikovnih poruka (MMS, engl. Multimedia Messaging *Service*), videopoziva, prijenosa podataka…

točniji pojednostavljeni prikaz moguće uzeti oblik kružnog isječka, koji je određen lokacijom bazne stanice (zemljopisna dužina – φ i zemljopisna širina – λ), smjerom primopredajnika u odnosu na sjever, širinom snopa signala i dometom signala.



Slika 1: Prikaz baznih stanica s pokrivenošću ćelija u obliku pravilnih heksagona



Slika 1: Prikaz pokrivenosti ćelije u obliku kružnog isječka

4. ULAZNI PODACI

Zahtjev za dostavu podataka o telekomunikacijskom prometu, koji je zabilježen na svim ćelijama baznih stanica koje pokrivaju određeno područje sadrži dva osnovna podatka: *ciljano područje* i *vremensko razdoblje*. Područje se uobičajeno određuje adresom (županija, mjesto, ulica, kućni broj) ili zemljopisnom dužinom i širinom[159], a vremensko razdoblje je određeno početnim i završnim vremenom[160] za koje se traže podaci o uspostavljanju kontakata.

Osim određivanja ciljanog područja adresom ili zemljopisnom dužinom i širinom, postoji još i mogućnost traženja podataka o telekomunikacijskom prometu koji je zabilježen na *određenim* ćelijama operatora, ali u tom slučaju tražitelj podataka treba prije podnošenja zahtjeva znati skup ćelija koje pokrivaju ciljano područje. Jedan od načina da se dođe do tih podataka jest odlazak na ciljano područje i korištenje "pametnog telefona" s instaliranom namjenskom aplikacijom za očitavanje ćelije koja ga pokriva signalom (za svakog od telekomunikacijskih operatora). Za to je potrebno odabrati vrijeme s približno jednakim uvjetima opterećenja ćelija i u interesantnom događaju jer se ne očitavaju sve ćelije pojedinog operatora koje pokrivaju ciljano područje nego samo ona s kojom je mobilni uređaj trenutno povezan. To je ujedno i bitno ograničenje u prikupljanju podataka o ćelijama, jer je kod

[159] Ciljano područje može biti zadano i površinom oko zemljopisne točke, no veličina područja utječe na količinu ulaznih podataka i može uzrokovati povećanje "lažno pozitivnih" rezultata kasnije obrade podataka.

[160] Potrebno je posvetiti pažnju određivanju početnog i završnog vremena razdoblja: poželjno je da razdoblje bude što uže (manja količina podataka, manje "lažno pozitivnih" rezultata), ali dovoljno široko da sigurno obuhvati vrijeme interesantnog događaja.

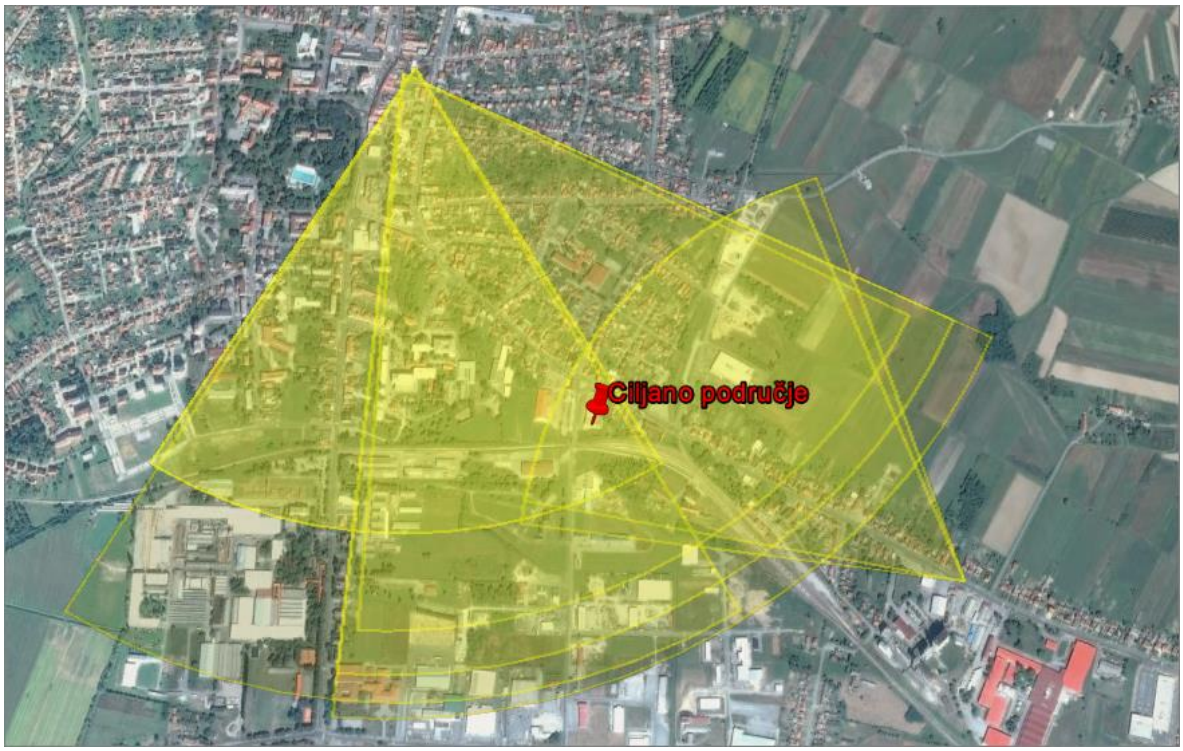
drugačijih uvjeta opterećenja ćelija moguće da neka druga ćelija istog telekomunikacijskog operatora ostvaruje vezu s mobilnim uređajem.

Podaci koji se dostavljaju na zahtjev dolaze u obliku datoteka za svaku pojedinu ćeliju koja pokriva ciljano područje, čime je (u slučaju zahtjeva s ciljanim područjem određenim adresom ili zemljopisnom dužinom i širinom) poznat *skup svih ćelija koje ga pokrivaju*.

U datotekama se nalaze podaci o telekomunikacijskom prometu zabilježenom na pojedinoj ćeliji u traženom razdoblju, a za daljnju obradu zanimljive su sljedeće grupe podataka svakog zapisa kontakta:

- *vremenski podaci* (vrijeme kontakta, trajanje)
- *identifikacijski* podaci *jednog od uređaja, tj. telefona* u komunikaciji (uređaj A):
- MSISDN, tj. telefonski broj A
- IMSI broj SIM kartice uređaja A (podatak nije uvijek zabilježen)
- IMEI broj mobilnog uređaja A (podatak nije uvijek zabilježen)
- *identifikacijski podaci ćelije* preko koje je *uređaj A* ostvario kontakt – Cell ID[161]
- *identifikacijski podaci drugog od uređaja, tj. telefona* u komunikaciji (uređaj B):
- MSISDN, tj. telefonski broj B
- IMSI broj SIM kartice uređaja B (podatak nije uvijek zabilježen)
- IMEI broj mobilnog uređaja B (podatak nije uvijek zabilježen)
- *identifikacijski podaci ćelije* preko koje je *uređaj B* ostvario kontakt (podatak nije uvijek zabilježen)
- *ostali podaci* (redni broj zapisa, vrsta usluge, smjer kontakta...).

[161] U praksi, identifikator ćelije sastoji se od dva broja: *Network ID* i *Cell ID*, no radi jednostavnosti daljnjih prikaza može se smatrati da je *Cell ID* broj koji jedinstveno određuje ćeliju.



Slika 2: ciljano područje pokriveno skupom ćelija baznih stanica

Na slici 3 prikazan je primjer pojednostavljenog grafičkog prikaza pokrivenosti ciljanog područja skupom ćelija baznih stanica prikazanih u obliku kružnog isječka.
Za potrebe uspoređivanja kontakata potrebno je još pribaviti podatke o telekomunikacijskom prometu za barem još jedno područje ili više ciljanih područja.

4.1.Optimiziranje odabira ulaznih podataka

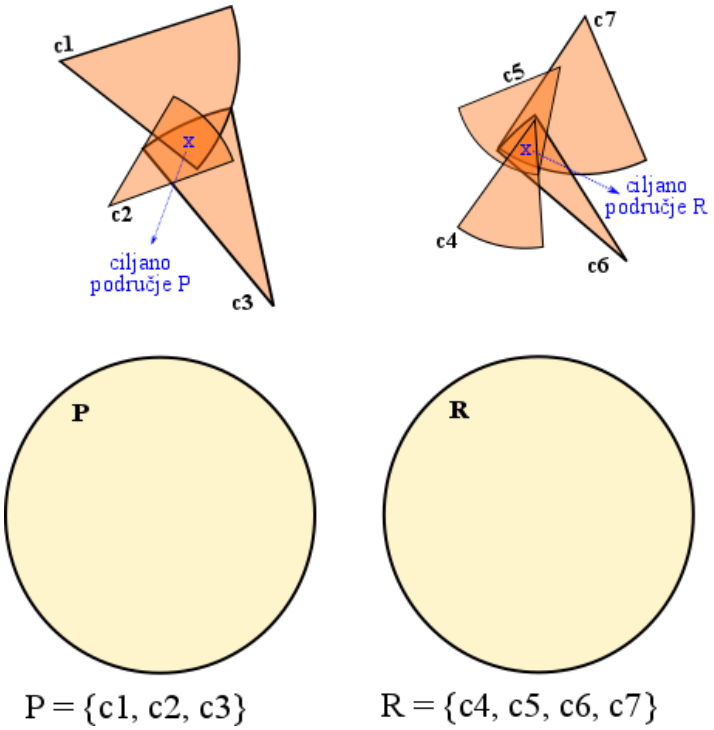
Već i prije postavljanja zahtjeva za dostavljanje podataka o telekomunikacijskom prometu korisno je poduzeti mjere koje će omogućiti da ulazni podaci budu što pogodniji za obradu. Za svako ciljano područje korisno je:
– *suziti područje*, čime se smanjuje skup ćelija koje ga pokrivaju
– utvrditi *što kraće vremensko razdoblje* traženih podataka
– odabrati *ciljano područje udaljenije od ostalih* ciljanih područja
– odabrati *više ciljanih područja*.

Iako često nije moguće ispuniti sve navedeno, ovim postupcima se smanjuje mogućnost "lažno pozitivnih" rezultata kasnije obrade podataka, odnosno smanjuje se mogućnost da se u rezultatima obrade pojave mobilni uređaji "legalnih" korisnika, tj. onih koji su se iz zakonitih razloga našli na više ciljanih područja (na primjer profesionalni vozači, osobe koje prilikom izlazaka posjećuju više mjesta i slično).

5. OPIS METODE USPOREĐIVANJA PODATAKA

Temeljna postavka za provođenje uspoređivanja podataka o kontaktima ostvarenim preko više skupova ćelija baznih stanica je pretpostavka da je nepoznati korisnik (najčešće počinitelj kaznenog djela) koristio mobilni uređaj za ostvarivanje kontakata u najmanje dva događaja, koji su određeni prostorno (ciljana područja) i vremenski (ciljana vremenska razdoblja). Ako obrada podataka rezultira identifikacijskim podacima jednog mobilnog uređaja ili više njih koji su zabilježeni na više ciljanih područja, dobiveni podaci mogu djelotvorno usmjeriti kriminalističko istraživanje te time skratiti vrijeme obrade i smanjiti troškove kriminalističkog istraživanja.

Ulazni podaci za obradu nalaze se u najmanje dva skupa datoteka. Svaki skup datoteka određuje skup ćelija koje pokrivaju pojedino ciljano područje, a ti skupovi mogu se imenovati oznakama, primjerice *P*, *R* itd.



Slika 3: Primjer dva ciljana područja sa dva skupa ćelija koje ih pokrivaju

Iz primjera na slici 4 može se vidjeti da se sve ćelije iz pojedinog skupa ćelija preklapaju na ciljanom području te da ukupno pokrivaju šire područje od ciljanog područja. Za obradu je bitno da ćelije iz pojedinog skupa pokrivaju ciljano područje, odnosno ako se u trenutku uspostavljanja kontakta mobilni uređaj nalazio na ciljanom području onda se njegova komunikacija sigurno odvijala preko jedne od ćelija iz skupa ćelija koje pokrivaju to ciljano područje.

Prije uspoređivanja potrebno je pripremiti za obradu ulazne podatke iz pribavljenih datoteka, a pogodan način za to je njihovo učitavanje u računalnu bazu podataka u obliku koji će biti prilagođen učinkovitom postupku uspoređivanja.

Vrijeme	*AUređaj*	*AĆelija*	*BUređaj*	*BĆelija*	*Ostali podaci*
v1	T1	c1	T4		...
v2	T2	c1	T5	c9	...
v3	T3	c1	T1	c4	...

Tablica 1: Simbolični prikaz strukture podataka u ulaznoj datoteci

Kao što je prikazano u tablici 1, svaki zapis o kontaktu u datoteci sastoji se od nekoliko grupa podataka, od kojih se za uspoređivanje koriste:
Vrijeme – podatak o vremenu uspostavljanja kontakta (datum, sat, minuta, sekunda)

AUređaj – jedan od mobilnih uređaja u komunikaciji (MSISDN, IMSI ili IMEI)[162]
AĆelija – ćelija preko koje je prvi mobilni uređaj ostvario komunikaciju (Cell ID)
BUređaj – drugi mobilni uređaj u komunikaciji (MSISDN, IMSI ili IMEI)
BĆelija – ćelija preko koje je drugi mobilni uređaj ostvario komunikaciju (Cell ID).

Struktura ulaznih datoteka je takva da je podatak *AĆelija* uvijek isti u cijeloj datoteci i to je upravo ona ćelija (Cell ID) čiji je telekomunikacijski promet sadržan u toj datoteci, što omogućuje prikupljanje podataka o skupu ćelija koje pokrivaju ciljano područje tijekom postupka punjenja baze podataka ulaznim podacima.

Iako su svi mobilni uređaji *AUređaj* zabilježeni na ćeliji *AĆelija* koja se nalazi u skupu ćelija koje pokrivaju zadano ciljano područje, bilo bi pogrešno zanemariti mogućnost da je i uređaj *BUređaj* zabilježen na ćeliji *AĆelija* (tj. *BĆelija=AĆelija*) ili da je zabilježen na nekoj drugoj ćeliji koja je u skupu ćelija koje pokrivaju ciljano područje.

Način zapisa ulaznih podataka sadrži i informaciju koja su dva mobilna uređaja ostvarila kontakt (*AUređaj* i *BUređaj* u istom zapisu), no ta informacija nije prijeko potrebna za kasnije uspoređivanje.

Ulazni podaci u bazu podataka se spremaju u sljedećem obliku:

Tablica 2: Simbolični prikaz strukture tablice kontakata u bazi podataka

KVrijeme	***KUređaj***	***KĆelija***	***KOznaka***	***KZastavica***	
v1	T1	c1			
v2	T2	c1			
v3	T3	c1			
v1	T4				→ nema podatka o ćeliji!
v2	T5	c9			
v3	T1	c4			

[162] U pojedinoj obradi uspoređivanjem kontakata, identifikacijski podatak mobilnih uređaja mora biti iz *iste* vrste brojeva (MSISDN, IMSI ili IMEI).

Ulazni podaci B strane (podatak *BUređaj*, *BĆelija*) razdvojeni su od A strane (podaci *AUređaj*, *AĆelija*), pridruženi su im podaci o vremenu kontakta (podatak *Vrijeme*) i dodani su kao zasebni zapisi u tablicu kontakata u bazi podataka (polja *KVrijeme, KUređaj i KĆelija*), izuzevši one zapise B strane koje nemaju podatak o ćeliji jer takvi zapisi nisu potrebni za uspoređivanje. Tablici su dodana još i polja *KOznaka* i *KZastavica* koja će se koristiti kasnije u postupku uspoređivanja.

Osim tablice kontakata, u bazi podataka potrebna je i tablica[163] ciljanih područja:

Tablica 3: Simbolični prikaz strukture tablice ciljanih područja u bazi podataka

CPOznaka	***PocVrijeme***	***ZavVrijeme***	***CPĆelija***
P	pv1	zv1	c1
P	pv1	zv1	c2
P	pv1	zv1	c3
R	pv2	zv2	c4
R	pv2	zv2	c5
R	pv2	zv2	c6
R	pv2	zv2	c7

U tablici ciljanih područja nalazi se polje *CPOznaka* (oznaka ciljanog područja), *PocVrijeme* i *ZavVrijeme* (početno i završno vrijeme ciljanog vremenskog razdoblja) i polje *CPĆelija* (ćelija koja pokriva ciljano područje). Ova tablica puni se podacima tijekom postupka spremanja ulaznih podataka iz datoteka u bazu podataka.

Nakon punjenja baze podataka ulaznim podacima iz *svih* datoteka, tablica kontakata u bazi sadrži skup vremenski određenih kontakata svih mobilnih uređaja koji su te kontakte ostvarivali preko zabilježenih ćelija, a tablica ciljanih područja sadrži sve skupove ćelija koje pokrivaju pojedina ciljana područja u zadanom vremenskom razdoblju (skupovi *P*, *R*...).

Sljedeći korak koji je potrebno obaviti jest obilježavanje zapisa u tablici kontakata oznakom ciljanog područja iz tablice ciljanih područja. Za svaki zapis iz tablice kontakata provjerava se nalazi li se korištena ćelija u tablici ciljanih područja i je li vrijeme kontakta unutar ciljanog vremenskog razdoblja, a ako su ti uvjeti ispunjeni oznaka ciljanog područja upisuje se u zapis tablice kontakata. Zapisi koji na kraju obilježavanja nemaju nikakvu oznaku ciljanog područja ne koriste se u kasnijem uspoređivanju.

[163] U bazi podataka može se nalaziti u obliku dvije tablice iz kojih se upitom stvara konačan oblik podataka.

Tablica 4: Simbolični prikaz tablice kontakata nakon upisa oznake ciljanih područja

KVrijeme	***KUređaj***	***KĆelija***	***KOznaka***	***KZastavica***	
v1	T1	c1	P		
v2	T2	c1	P		
v3	T3	c1	P		
v2	T5	c9			→ c9 ne pokriva cilj. područje
v3	T1	c4	R		

Nakon ovakve pripreme ulaznih podataka konačno slijedi uspoređivanje zapisa iz tablice kontakata da bi se utvrdilo je li neki mobilni uređaj ostvarivao kontakte preko ćelija iz više skupova ciljanih područja. Za svaki zapis iz tablice kontakata u kojem je upisana oznaka ciljanog područja (zapis koji se uspoređuje – *i*), provjeravaju se svi ostali zapisi iz iste tablice koji imaju upisane oznake ciljanog područja (zapis s kojim se uspoređuje – *j*) i utvrđuje se jesu li ispunjeni uvjeti da je identifikacijski podatak mobilnog uređaja iz zapisa *j* isti kao u zapisu *i* ($KUređaj_j = KUređaj_i$) i da je istodobno oznaka ciljanog područja zapisa *j* različita od one u zapisu *i* ($KOznaka_j \neq KOznaka_i$). Ako su ovi uvjeti ispunjeni, oba zapisa obilježavaju se kao pozitivan rezultat uspoređivanja uključivanjem "zastavice" *KZastavica*. Postupak uspoređivanja potrebno je nastaviti i obaviti za *sve* zapise iz tablice zapisa (koji imaju upisane oznake ciljanih područja) jer je moguće da je više mobilnih uređaja ostvarivalo kontakte preko ćelija iz više skupova ciljanih područja.

Treba napomenuti da je osnovna svrha podataka o vremenskim razdobljima kontakata ciljanih područja u ovom postupku zapravo kontrola vjerojatnosti da se u rezultatima obrade pojave mobilni uređaji "legalnih" korisnika. Iako je razumno pretpostaviti da se isti mobilni uređaj nije mogao istodobno pojaviti na više ciljanih područja, zbog nesigurnosti u procjeni vremena događaja mogući su i slučajevi preklapanja vremenskih razdoblja ciljanih područja, no to nije prepreka za korištenje opisane metode uspoređivanja.

Tablica 5: Simbolični prikaz tablice kontakata nakon uspoređivanja i označavanja rezultata

KVrijeme	***KUređaj***	***KĆelija***	***KOznaka***	***KZastavica***	
v1	T1	c1	P	DA	→ *T1* na ciljanom području *P*
v2	T2	c1	P		
v3	T3	c1	P		
v2	T5	c9			
v3	T1	c4	R	DA	→ *T1* na ciljanom području *R*

Završenim postupkom uspoređivanja u tablici kontakata nalaze se obilježeni svi kontakti (ako takvi postoje) s mobilnim uređajima koji su ostvarivali kontakte preko ćelija iz više skupova ciljanih područja. Iz tako obrađene tablice kontakata jednostavno je izdvojiti

popis svih mobilnih uređaja iz zapisa koji imaju uključenu "zastavicu" *KZastavica*, što predstavlja završni rezultat koji se želio postići uspoređivanjem podataka.

Za potrebe preglednog opisa osnova metode uspoređivanja podataka korišten je jednostavan primjer sa simboličnim prikazom ukupno 5 kontakata (tablice 4 i 5) od koji 4 zapisa imaju upisane oznake ciljanih područja, a bilo je potrebno izvršiti ukupno 4·3=12 uspoređivanja zapisa. U stvarnim uvjetima tablica kontakata može imati nekoliko tisuća, pa i nekoliko desetaka tisuća zapisa (s upisanim oznakama ciljanih područja): koristeći opisanu metodu uspoređivanja za 1000 zapisa bilo bi potrebno oko 1 000 000 uspoređivanja, a za 10 000 zapisa gotovo 100 000 000 uspoređivanja zapisa. To je previše za prosječna osobna računala na kojima bi obrada predugo trajala i nužna je dodatna optimizacija postupka uspoređivanja.

Zato se kod uspoređivanja pojedinog zapisa o kontaktu kao uspoređivani kontakti uzimaju samo oni zapisi koji imaju iste identifikacijske podatke mobilnog uređaja, a uspoređivanje se ne provodi sa zapisima koji su već bili uspoređivani. Procjena broja potrebnih uspoređivanja takvim postupkom može se izraziti formulom:

$$u \approx \frac{m \cdot \overline{k_m} \cdot (\overline{k_m} - 1)}{2} = \frac{(k : \overline{k_m}) \cdot \overline{k_m} \cdot (\overline{k_m} - 1)}{2} = \frac{k \cdot (\overline{k_m} - 1)}{2}$$

gdje je u – procjena ukupnog broja uspoređivanja, m – ukupan broj mobilnih uređaja, $\overline{k_m}$ – prosječan broj kontakata po mobilnom uređaju, k – ukupan broj kontakata. Za prosječnu vrijednost $\overline{k_m}$=2,2 kontakta po mobilnom uređaju[164] procijenjeni broj potrebnih uspoređivanja prema prethodnoj formuli iznosi oko 60% od ukupnog broja kontakata, što je znatno povoljnije za računalnu obradu (iako i dalje previše za bilo kakav oblik ručnog uspoređivanja).

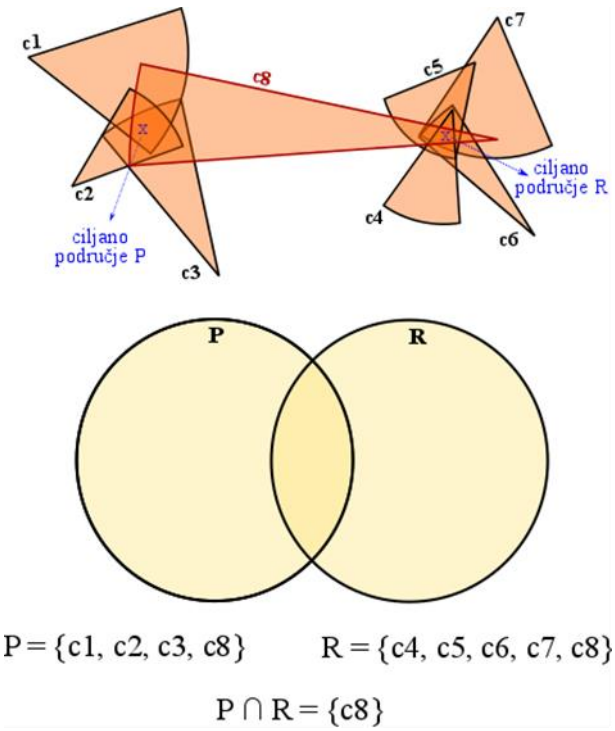
6. POSEBNI SLUČAJEVI RASPOREDA ĆELIJA CILJANIH PODRUČJA

Za opisivanje metode uspoređivanja podataka o kontaktima u prethodnom poglavlju korišten je primjer s ciljanim područjima čiji se skupovi ćelija međusobno ne preklapaju, tj. nema ćelija koje se nalaze u više skupova ćelija ciljanih područja, što znači da nema ćelija koje pokrivaju više ciljanih područja. U praksi se pojavljuju i slučajevi u kojima se *skupovi* ćelija međusobno djelomično ili potpuno preklapaju, pa je takve slučajeve potrebno dodatno objasniti i prilagoditi metode obrade kako bi se dobili što kvalitetniji rezultati.

6.1. Djelomično preklapanje skupova ćelija ciljanih područja

Djelomično preklapanje skupova ćelija ciljanih područja događa se u slučajevima kada su ciljana područja zemljopisno dovoljno blizu da ih pokriva ista ćelija (jedna ili više njih), ali i dalje postoje ćelije koje pokrivaju samo pojedino ciljano područje.

[164] U primjeru iz prakse sa nešto manje od 18 000 kontakata, dobivena je prosječna vrijednost od 2,2 kontakta po mobilnom uređaju.



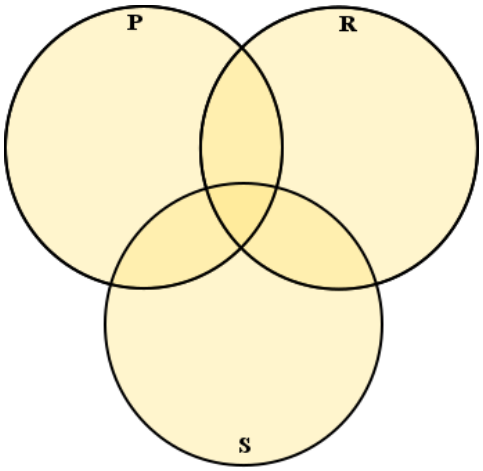
Slika 4: Primjer dva ciljana područja s djelomično preklapajućim skupovima ćelija koje ih pokrivaju

Nas slici 5 prikazan je primjer u kojem ćelije c1, c2 i c3 pokrivaju *samo* ciljano područje *P*, ćelije c4, c5, c6 i c7 pokrivaju *samo* ciljano područje *R*, dok ćelija c8 pokriva ciljano područje *P i* ciljano područje *R*.

Koristeći opisanu metodu uspoređivanja kontakata na ovom primjeru, identifikacijski podaci pojedinih mobilnih uređaja koji su ostvarili kontakt preko ćelije c8 u vremenskom razdoblju ciljanog područja *P*, ako su ostvarili i kontakt preko ćelije c8 u vremenskom razdoblju ciljanog područja *R*, naći će se u rezultatima uspoređivanja kao oni koji su zabilježeni na oba ciljana područja (uz moguće identifikacijske podatke i drugih mobilnih uređaja). Ako ćelija c8 iz primjera pokriva područje na kojem se svakodnevno nalazi veći broj uglavnom iste grupe ljudi (što je u većini slučajeva točno), u rezultatima uspoređivanja naći će se veliki broj identifikacijskih podataka mobilnih uređaja korisnika koji, primjerice žive ili rade na području pokrivenosti ćelije c8 ("domaće osobe") i ostvarivali su kontakte s *iste* zemljopisne lokacije (iz svog doma ili s radnog mjesta).

Takvi podaci predstavljaju "lažno pozitivne" rezultate i nastoji se što više smanjiti njihov broj, a to se može postići izuzimanjem ćelije c8 iz skupa ćelija koje se uspoređuju. Iako postoji mogućnost da su i korisnici interesantnih mobilnih uređaja (odnosno počinitelji kaznenih djela) ostvarivali kontakte upravo preko ćelije c8, metodom uspoređivanja takvi se mobilni uređaji ionako ne mogu izdvojiti iz skupine mobilnih uređaja korištenih od strane "domaćih osoba", pa je izuzimanje ćelije c8 u ovakvom primjeru prihvatljivo.

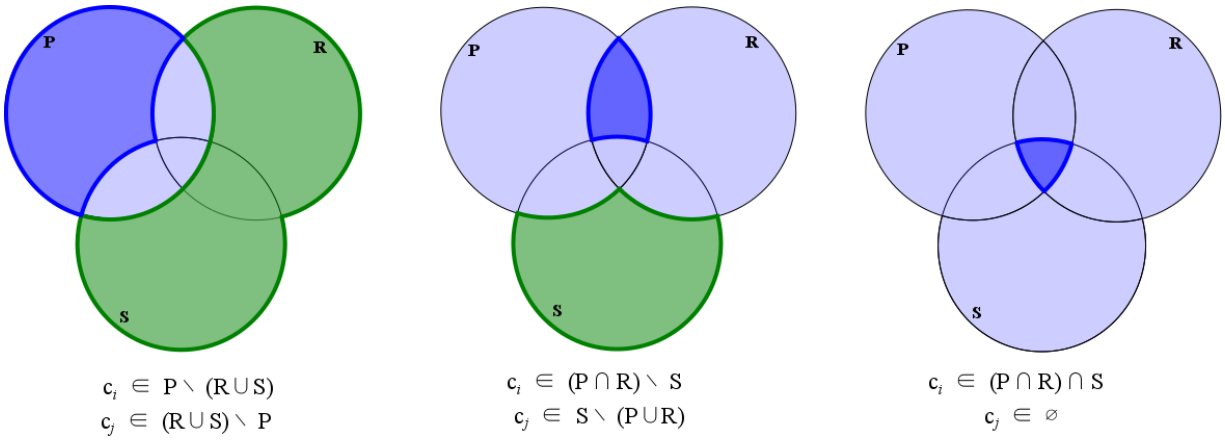
U praksi su mogući i slučajevi složenijega djelomičnog preklapanja skupova ćelija tri ciljana područja ili više njih, pa je potrebno razmotriti način isključivanja ćelija iz postupka uspoređivanja kako bi se postigao što veći broj mogućih rezultata obrade uz što manje "lažno pozitivnih" rezultata. Razmatranje je moguće učinkovito provesti na primjeru tri djelomično preklapajuća skupa ćelija ciljanih područja.



Slika 5: Složeniji primjer tri djelomično preklapajuća skupa ćelija ciljanih područja

U odnosu na postupak uspoređivanja, razlikuju se tri grupe podskupova ćelija u kojima može biti ćelija korištena u kontaktu koji se uspoređuje (c_i):

a) podskup ćelija koje pokrivaju *samo jedno* ciljano područje
b) podskup ćelija koje pokrivaju *više,* ali *ne sva* ciljana područja
c) podskup ćelija koje pokrivaju *sva* ciljana područje.



a) *b)* *c)*

Slika 6: Različiti slučajevi uspoređivanja u ovisnosti o ćeliji kontakta koji se uspoređuje

U prvom slučaju, kada korištena ćelija kontakta koji se uspoređuje c_i pokriva *samo* ciljano područje *P* (slika 7 a), ćelija kontakta s kojim se uspoređuje c_j ne smije biti u skupu

ćelija koje pokrivaju područje *P* (*cijeli* skup *P*), kako bi se izbjegli mobilni uređaji korišteni od strane "domaćih osoba" s ciljanog područja *P*, odnosno (u prikazanom primjeru) c_j treba biti u podskupu ćelija koje pokrivaju ciljana područja *R* ili *S* i *ne pokrivaju* ciljano područje *P*. Treba uočiti da u ovom primjeru ćelija c_j može (između ostalog) biti i u podskupu ćelija koje pokrivaju *oba* ciljana područja *R* i *S*, ali *ne pokrivaju* ciljano područje *P*. Te ćelije c_j prihvatljive su za uspoređivanje jer se u rezultatima obrade ne bi trebali pojaviti mobilni uređaji "domaćih osoba" s područja *R* i *S* zato što će takve uređaje iz rezultata isključiti uvjet da su njihovi kontakti bili evidentirani na ćeliji c_i koja pokriva *samo* ciljano područje *P*.

U drugom slučaju, kada korištena ćelija kontakta koji se uspoređuje c_i pokriva *oba* ciljana područja *P* i *R* i *ne pokriva* ciljano područje *S* (slika 7 b), ćelija kontakta s kojim se uspoređuje c_j treba biti u podskupu ćelija koje ne pokrivaju niti ciljano područje *P* niti ciljano područje *R*, odnosno (u prikazanom primjeru) c_j treba biti u podskupu ćelija koje pokrivaju *samo* ciljano područje *S*. Slično kao i u prvom slučaju, u rezultatima obrade ne bi se trebali pojaviti mobilni uređaji "domaćih osoba" s područja *P* i *R* zato što će takve uređaje iz rezultata isključiti uvjet da su njihovi kontakti bili evidentirani na ćeliji c_j koja pokriva *samo* ciljano područje *S*.

U zadnjem slučaju, kada korištena ćelija kontakta koji se uspoređuje c_i pokriva *sva* ciljana područja *P*, *R* i *S* (slika 7 b), ne može se vršiti uspoređivanje jer bi ćelija kontakta s kojim se uspoređuje c_j trebala biti u podskupu ćelija koje ne pokrivaju niti jedno od ciljanih područja *P*, *R* ili *S*, a takvih ćelija nema (prazan skup).

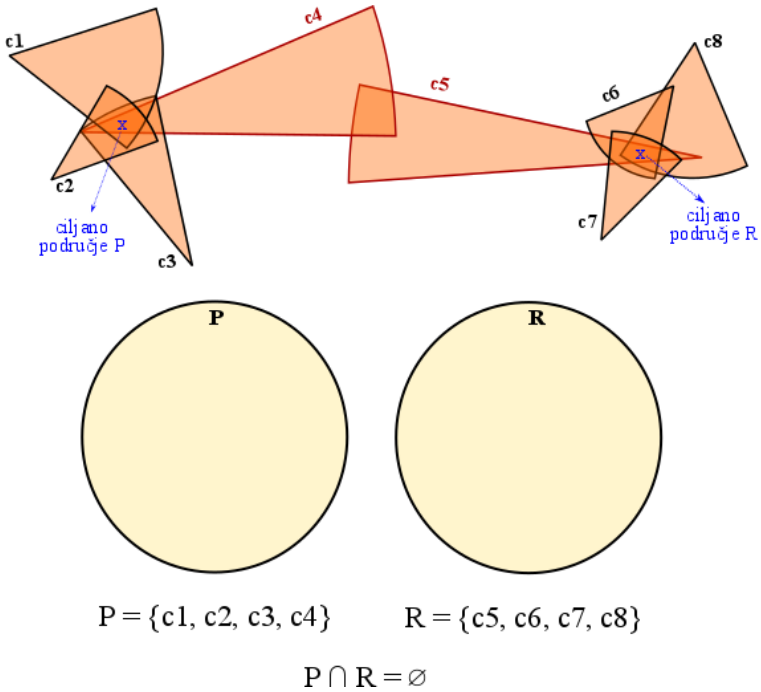
Nakon razmatranja različitih prethodnih slučajeva, može se uobličiti jedinstveni uvjet za ćeliju kontakta s kojim se uspoređuje c_j kod uspoređivanja kontakata s *proizvoljnog* broja ciljanih područja za koje se skupovi ćelija djelomično preklapaju[165]: ćelija kontakta s kojim se uspoređuje c_j mora biti u podskupu ćelija koje nisu u skupovima ćelija koje pokrivaju ista ciljana područja kao i korištena ćelija kontakta koji se uspoređuje c_i.

Kod opisane metode uspoređivanja kontakata u slučajevima kada se skupovi ćelija ciljanih područja *ne preklapaju* ili se *djelomično preklapaju*,iskorišteno je postojanje podskupova ćelija koji se ne preklapaju ili se djelomično preklapaju kako bi se iz rezultata obrade isključili mobilni uređaji korišteni od strane "domaćih osoba" koji predstavljaju "lažno pozitivne" rezultate (prostorno isključivanje uređaja "domaćih osoba").

6.2. Preklapanje područja pokrivenosti ćelija iz skupova ćelija različitih ciljanih područja

U slučajevima kada su ciljana područja zemljopisno dovoljno blizu, moguć je takav raspored ćelija ciljanih područja u kojem se međusobno djelomično preklapaju *područja pokrivenosti* dvije ćelije ili više njih, iako svaka takva pojedina ćelija pokriva samo jedno ciljano područje. Ovakav raspored može se pojaviti i kod djelomičnog preklapanja *skupova* ćelija ciljanih područja i kada se *skupovi* ćelija ciljanih područja ne preklapaju, no u svakoj od tih varijanti može imati utjecaja na kvalitetu rezultata obrade.

[165] Uključen je i slučaj kada se skupovi ćelija *ne preklapaju*.



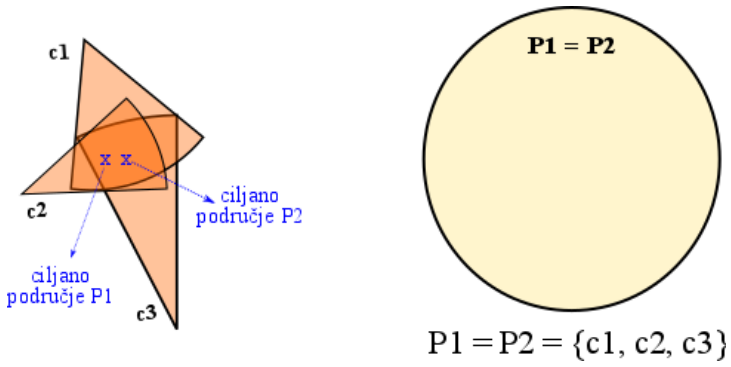
Slika 7: primjer dva ciljana područja sa skupovima ćelija koji se ne preklapaju, ali s ćelijama čija se područja pokrivenosti preklapaju

Na slici 8 prikazan je primjer u kojem se *skupovi* ćelija ciljanih područja *P* i *R ne preklapaju*, ali se preklapaju *područja pokrivenosti* ćelija c4 i c5, od kojih c4 pokriva ciljano područje *P* i ne pokriva ciljano područje *R*, a ćelija c5 pokriva ciljano područje *R* i ne pokriva ciljano područje *P*. Kako se *skupovi* ćelija *P* i *R* međusobno ne preklapaju, primjer je pogodan za uspoređivanje primjenom metode prostornog isključivanja "domaćih osoba", no u rezultatima obrade mogu se naći i mobilni uređaji "domaćih osoba" s (nešto manjeg) područja koje zajednički pokrivaju ćelije c4 i c5. Kada bi se iz rezultata željelo isključiti i ovaj dio mobilnih uređaja "domaćih osoba", moralo bi se iz uspoređivanja isključiti *sve* kontakte s ćelija c4 i c5 jer pomoću dostupnih podataka nije moguće razlučiti koji su mobilni uređaji ostvarili kontakte dok su bili na području preklapanja ćelija c4 i c5, ali bi se tada iz rezultata možda izbacili i interesantni mobilni uređaji zabilježeni i na ciljanom području *P* (ćelija c4) i na ciljanom području *R* (ćelija c5). Osim toga pojavljuje se i problem identificiranja ćelija čija se *područja pokrivenosti* preklapaju: za to je potrebno zasebno vizualno analiziranje područja pokrivenosti svih ćelija ciljanih područja, a ti podaci nisu dostupni korisnicima u zadovoljavajućem obliku i točnosti i na zadovoljavajući način.

Zbog prethodno navedenih razloga, u metodi prostornog isključivanja "domaćih osoba" iz uspoređivanja se *ne isključuju* ćelije čija se *područja pokrivenosti* preklapaju, ali se uzima u obzir da se u rezultatima može naći i dio mobilnih uređaja "domaćih osoba".

6.3. Potpuno preklapanje skupova ćelija ciljanih područja

Postupak prostornog isključivanja uređaja "domaćih osoba" *nije pogodan* u slučajevima kada se skupovi ćelija koje pokrivaju ciljana područja *u potpunosti preklapaju*. To su slučajevi kada su ciljana područja zemljopisno dovoljno blizu da ih pokriva potpuno isti skup ćelija, iako se vremenska razdoblja događaja na ciljanim područjima razlikuju (primjer sa slike 8). Kada bi se u njima primijenila metoda isključivanja podskupova ćelija koje se preklapaju za uspoređivanje ne bi ostalo ništa, zato za smanjenje "lažno pozitivnih" rezultata treba razmotriti druge mogućnosti.



Slika 8: primjer dva ciljana područja sa skupovima ćelija koji se potpuno preklapaju

Kod slučajeva ciljanih područja sa skupovima ćelija koji se *potpuno* preklapaju (zbog čega nije moguće koristiti prostorno isključivanje "domaćih osoba"), potrebno je pribaviti *dodatne* podatke o telekomunikacijskom prometu za *isti skup* ćelija, ali za vremensko razdoblje u kojem interesantni mobilni uređaj *nije bio* na ciljanim područjima (kontrolno vremensko razdoblje) i koje se ne preklapa s ciljanim vremenskim razdobljima[166]. Nakon obilježavanja zapisa u tablici kontakata oznakama ciljanih područja (u ovakvim slučajevima to su skupovi u kojima je isti popis ćelija, ali se odnose na *različita* vremenska razdoblja), provodi se uspoređivanje zapisa iz tablice kontakata: kao pozitivni rezultati uspoređivanja obilježavaju se kontakti s korištenom ćelijom iz skupa ćelija ciljanih područja u ciljanim vremenskim razdobljima, ali samo ako *ne postoji* kontakt mobilnog uređaja iste identifikacijske oznake s korištenom ćelijom iz skupa ćelija ciljanih područja u *kontrolnom* vremenskom razdoblju.

Na taj način iz rezultata se isključuju mobilni uređaji "domaćih osoba" koji su ostvarili kontakt u kontrolnom vremenskom razdoblju, budući da u tom razdoblju interesantni mobilni uređaji nisu bili na ciljanom području (vremensko isključivanje uređaja "domaćih osoba"), no postupak je manje uspješan[167] u odnosu na prostorno isključivanje. Kod metode vremenskog

[166] U protivnom, mobilni uređaj bi u *istom* kontaktu mogao biti na ciljnom području i u ciljanom i u kontrolnom vremenskom razdoblju, a to je u suprotnosti sa zahtjevom da interesantan mobilni uređaj *nije bio* na ciljnom području u *kontrolnom* vremenskom razdoblju.

[167] Kod vremenskog isključivanja mobilnih uređaja "domaćih osoba" ključno je da korisnik ostvari kontakt u kontrolnom vremenskom razdoblju; ako takav kontakt nije ostvaren mobilni uređaj "domaćeg korisnika" ovim

isključivanja dovoljno je postojanje ulaznih podataka za *jedno* ciljano vremensko razdoblje i *jedno* kontrolno vremensko razdoblje, ali korištenje više ciljanih vremenskih razdoblja i šireg kontrolnog vremenskog razdoblja može smanjiti količinu "lažno pozitivnih" rezultata.

U posebnim slučajevima kada potpuno preklapajući skupovi ćelija ciljanog područja pokrivaju nenaseljeno područje (primjerice nenaseljeni dijelovi prometnih pravaca, šumski ili poljski predjeli koji su pokriveni signalom mobilne mreže, isključivo poslovna područja izvan radnog vremena i sl.), može se pokušati izvršiti uspoređivanje i bez prostornog i bez vremenskog isključivanja uređaja "domaćih osoba". Ovakvi slučajevi su prilično rijetki[168], a osim toga obrada daje znatno manje kvalitetne rezultate (više "lažno pozitivnih" rezultata[169]) i zato se gotovo i ne koriste.

7. ZAKLJUČAK

Podaci o kontaktima mobilnih uređaja ostvarenih preko ćelija baznih stanica svojom količinom nerijetko mogu obeshrabriti korisnike i odvratiti ih od pokušaja obrade i dobivanja korisnih rezultata jer to često nalikuje traženju "igle u plastu sijena". Unatoč tome pokazuje se da je moguće uobličiti postupke i metode za učinkovitu obradu podataka i dobivanje iskoristivih rezultata. Vrlo je bitno da korisnici pri tome budu svjesni ograničenja i značenja podataka (onih koji se obrađuju i dobivenih rezultata) i ograničenja u obradi podataka; dio tih ograničenja objašnjen je u opisu postupaka uspoređivanja podataka, no korisno je navesti i druga ograničenja i moguće probleme.

Jedna od prvih odluka koje korisnik treba donijeti prije obrade odnosi se na količinu podataka koji će se pribavljati, uravnotežujući pritom međusobno suprotne zahtjeve. Podaci pribavljeni za veći broj ciljanih područja (kod primjene prostornog isključivanja uređaja "domaćih osoba") ili za šire kontrolno razdoblje (kod primjene vremenskog isključivanja uređaja "domaćih osoba") mogu bitno povećati kvalitetu rezultata obrade (manje "lažno pozitivnih" rezultata). Promatrajući s druge strane, posljedice veće količine ulaznih podataka su veći troškovi pribavljanja podataka, duže vrijeme obrade te veće zadiranje u pravo na zaštitu osobnih podataka[170] korisnika čija je komunikacija zabilježena na ćelijama baznih stanica, a sve to je potrebno smanjiti.

Mogući problem može se pojaviti zbog činjenice da korisnik ima ograničeni utjecaj na popise ćelija koje pokrivaju određena ciljana područja: korisnik u zahtjevu određuje ciljano područje adresom ili zemljopisnom lokacijom, te prima podatke o telekomunikacijskom

---

postupkom se ne može isključiti iz rezultata, pa je u rezultatima načelno više "lažno pozitivnih" u odnosu na metodu prostornog isključivanja uređaja "domaćih osoba".

[168] Poslovanje telekomunikacijskih operatora temelji se na načelima ekonomske isplativosti: uz što manja financijska ulaganja nastoji se signalom mobilne mreže pokriti što više korisnika, a posljedica toga je dobra pokrivenost naseljenog područja i prometnih pravaca, te znatno slabija pokrivenost nenaseljenih i prometno izoliranih područja.

[169] U rezultatima se mogu pojaviti mobilni uređaji koje koriste, npr. osobe koje redovno putuju na posao (prometni pravci), lovci koji obilaze lovište, šumari koji obilaze šumu (šumski predjeli), noćni čuvari (poslovna područja izvan radnog vremena) itd.

[170] Pravo na zaštitu osobnih podataka uređuje Zakon o zaštiti osobnih podataka (Narodne novine 103/03., 118/06., 41/08., 130/11., 106/12.).

prometu sa skupa ćelija koje bi trebale pokrivati traženo ciljano područje. Provjerom dostupnih podataka o pokrivenosti pojedinih ćelija u nekim slučajevima je uočeno da su u ulaznim podacima i datoteke ćelija koje (uzimajući u obzir i pogreške zbog pojednostavljenog prikaza pokrivenosti kružnim isječkom) ipak ne bi mogle pokrivati ciljano područje[171], što može utjecati na kvalitetu rezultata obrade. Problem bi se možda mogao riješiti traženjem podataka s konkretnog skupa ćelija, no korisnicima zbog načina funkcioniranja poslovnih procesa nisu dostupni podaci o pokrivenosti određene zemljopisne lokacije ćelijama u zadovoljavajućem obliku i točnosti, te na zadovoljavajući način. Zato bi bilo korisno uložiti napore u svrhu kvalitetnijeg određivanja skupa ćelija koje pokrivaju zadano zemljopisno područje.

Kod odabira vrste identifikacijskih podataka mobilnih uređaja koji se koriste u postupku uspoređivanja najčešće se odabiru MSISDN brojevi, koji su zapravo pozivni telefonski brojevi, pa postoji mogućnost da se zanemare prednosti koje pruža odabir IMEI brojeva kao vrste identifikacijskih podataka mobilnih uređaja. Naime, neki tehnološki osvješteniji počinitelji kaznenih djela u najmanju ruku naslućuju opasnost koju im stvara korištenje mobilnih uređaja i pokušavaju "zamesti tragove" tako što u različitim "aktivnostima" u svojim mobilnim uređajima koriste različite SIM kartice (tj. različite pozivne brojeve). Kako je svaki mobilni uređaj identificiran jedinstvenim IMEI brojem, korištenjem IMEI brojeva kao identifikatora mobilnih uređaja u postupku uspoređivanja kontakata može se riješiti problem i uspješno identificirati interesantne mobilne uređaje.

Kod korištenja uspoređivanja kontakata zabilježenih na ćelijama baznih stanica može se pojaviti problem "prevelikih očekivanja" jer se često pretpostavlja da će obrada podataka o kontaktima gotovo sigurno rezultirati identitetom nepoznatih počinitelja kaznenih djela, što je prilično netočno. Za kvalitetne rezultate obrade važno je dobro poznavanje okolnosti osnovnih događaja, dobro poznavanje značenja podataka koji se obrađuju, prednosti i mana odabranih postupaka u obradi i problema koji se mogu pojaviti. Prilikom provođenja obrada znatan je broj pretpostavki koje se postavljaju i suprotnih zahtjeva koje je potrebno uravnotežiti. Kada se uza sva ograničenja dođe do iskoristivih rezultata obrade podataka, oni su tek polazna osnova za daljnju operativnu obradu kojom je potrebno utvrditi korisnike identificiranih mobilnih uređaja i njihovu eventualnu ulogu u osnovnom događaju.

Unatoč ograničenjima praksa pokazuje da dobiveni rezultati obrade mogu u značajnom broju slučajeva djelotvorno usmjeriti kriminalističko istraživanje, skratiti utrošeno vrijeme i smanjiti troškove. Zato je korisno i dalje razvijati metode obrade ovakvih podataka, uvažavajući eventualne nove tehničke mogućnosti, kako bi policija i u tom smislu održala tehnološki korak u odnosu na počinitelja kaznenih djela.

[171] Primjerice, slučajevi kada je lokacija bazne stanice nekoliko kilometara udaljena od ciljanog područja, a ćelija užeg snopa signala je okrenuta na suprotnu stranu od ciljanog područja.

LITERATURA

Imei (international mobile equipment identity), http://whatis.techtarget.com/definition/imei-international-mobile-equipment-identity (29. Prosinca 2015.)
Learn about what is on a cell tower: without the cat, http://www.withoutthecat.com (29. Prosinca 2015.)
Mobile telephone, http://www.britannica.com/technology/mobile-telephone (29. Prosinca 2015.)
Mobitel, http://www.enciklopedija.hr/natuknica.aspx?id=41427 (29. Prosinca 2015.)
Msisdn – definition and examples, http://www.msisdn.org (29. Prosinca 2015.)
Uredba o obvezama iz područja nacionalne sigurnosti republike hrvatske za pravne i fizičke osobe u telekomunikacijama. Narodne novine 64/08., 76/13.
Zakon o kaznenom postupku. Narodne novine 145/13., 152/14.
Zakon o policijskim poslovima i ovlastima. Narodne novine 76/09., 92/14.
Zakon o zaštiti osobnih podataka. Narodne novine 103/03., 118/206., 41/08., 130/11., 106/12.

Spomenko Relić

COMPARISON OF MOBILE DEVICES CONTACTS ACHIEVED THROUGH TELECOMMUNICATION BASE STATIONS CELLS

Summary

If an unknown user, usually a perpetrator of a criminal offence, has used a mobile device to make contacts in events defined in terms of space (targeted areas) and time (time periods), comparing the contacts data registered on the telecommunication base stations cells may result in the identification of one or more mobile devices that have been registered in several specific areas. The resulting data may prove useful, as well as cost and time effective, in a criminal investigation.
This paper provides an overview of the current legal basis for obtaining and processing of telecommunication data in Republic of Croatia. It clarifies fundamental technical concepts necessary for understanding the topic and shows the structure and meaning of the processed input data with guidelines for optimizing the selection of input data. Using a symbolic example of the input data for sets of telecommunication base stations cells that cover different targeted areas, the data comparison method, which is suitable for computer processing and is optimized for faster results, has been elaborated. An example of partial overlapping of cell sets for targeted areas with the addition of the method for comparing the data which reduces the amount of "false positive" results and increases the number of possible results has been elaborated separately. The paper also explains the particularities of comparing the contacts in case of complete overlapping of cell sets for targeted areas (the same targeted area in different time periods).

Key words: *telecommunication data, telecommunication base station cells, contact comparison, cell sets overlapping, optimizing.*

STRUČNI RAD

Mladen Vuković[172]

ZNAČAJ I ULOGA MOBILNIH TELEFONA PRILIKOM RASVJETLJAVANJA KRIVIČNIH DJELA

Sažetak

Suzbijanje kriminaliteta predstavlja stalan i veoma aktuelan i problematičan dio sveukupne bezbjednosne problematike i stanja u društvu. Mobilni telefoni, koji svakim danom sve više postaju sredstvo komunikacije među ljudima, koriste i razna lica iz kriminogenih sredina za svoje dogovore, tako da se primjenom odgovarajućih tehničkih sredstava mogu saznati i snimiti sadržaji takvih razgovora, pa i identifikovati sagorornici, tim prije što je poznato da se korisnik mobilnog telefona može locirati skoro na svakom mjestu. Kako su mobilni telefoni nezaobilazan detalj svakodnevnog poslovnog i porodičnog aspekta života svakog čovjeka, razumljivo je da i zloupotreba mobilnih telefona dobija na značaju, kako kvalitativno, tako i kvantitativno. Usred uslovljenosti svakodnevnih životnih aktivnosti posjedovanjem mobilnih telefona, mobilni telefoni postaju sredstvo izvršenja krivičnih djela. Policijski organi moraju da prate tehničko-tehnološka i naučna dostignuća u oblasti mobilne telefonije, a shodno tehničkim mogućnostima operatera mobilne telefonije i osmišljvaju te prilagođavaju metede vlastitog kriminalističkog rada u cilju suzbijanje kriminaliteta. U radu će se prezentirati, analizirati i problematizovati specifičnosti koje se odnose na značaj i ulogu mobilnih telefona prilikom rasvjetljavanja krivičnih djela, ulogu listinga dolaznih i odlaznih poziva i SMS poruka, značaj IMEI broja u operativnom radu policije, specifičnosti vezane za posebnu istražnu radnju nadzor i tehničko snimanje telekomunikacija a koje su prilagođene subjektivnim i objektivnim uslovljavajućim faktorima rada policijskih službenika Ministarstva unutrašnjih poslova Republike Srpske.

Ključne riječi: *mobilni telefon, IMEI, otkrivanje, dokazivanje, posebne istražne radnje.*

1. UVODNA RAZMATRANJA

Efikasnost i uspjeh istrage prvenstveno zavisi od dobro planiranih akivnosti kao kompleksnog i multidisciplinarnog procesa koji posebno dolazi do izražaja kada se radi o primjeni operativno-taktičkih mjera i radnji, te primjenu klasičnih i posebnih metoda u cilju rasvjetljavanja i dokazivanja krivičnih djela. Mobilni telefoni, koji svakim danom sve više postaju sredstvo komunikacije među ljudima, koriste i razna lica iz kriminogenih sredina za svoje dogovore, tako da se primjenom odgovarajućih tehničkih sredstava mogu saznati i snimiti sadržaji takvih razgovora, pa i identifikovati sagorornici, tim prije što je poznato da se

[172] Mladen Vuković, mr., doktorand na Pravnom fakultetu, Univerziteta u Novom Sadu, zaposlen u Ministarstvu unutrašnjih poslova Republike Srpske, Uprava za policijsko obrazovanje, Visoka škola unutrašnjih poslova, Banja Luka, e-mail: mladen_vukovic1983@yahoo.com

korisnik mobilnog telefona može locirati skoro na svakom mjestu. Kako su mobilni telefoni nezaobilazan detalj svakodnevnog poslovnog i porodičnog aspekta života svakog čovjeka, razumljivo je da i zloupotreba mobilnih telefona dobija na značaju, kako kvalitativno, tako i kvantitativno. Usred uslovljenosti svakodnevnih životnih aktivnosti posjedovanjem mobilnih telefona, mobilni telefoni postaju sredstvo izvršenja krivičnih djela. Policijski organi moraju da prate tehničko-tehnološka i naučna dostignuća u oblasti mobilne telefonije, a shodno tehničkim mogućnostima operatera mobilne telefonije i osmišljvaju te prilagođavaju metede vlastitog kriminalističkog rada u cilju suzbijanje kriminaliteta. Sva ova određenja su opšteg karaktera i kao takva se mogu proširivati i sužavati, ali u svakom slučaju treba insistirati da policijski službenici ove radnje preduzimaju kao jedan jedinstven proces koji vodi do otkrivanja krivičnog djela i učinioca. U savremenoj kriminalističkoj praksi, mobilni telefoni se koriste kao sredstvo izvršenja određenih krivičnih djela npr. iznude, ucjene, ugrožavanja sigurnosti, veoma često kao sredstvo međusobne komunikacije između izvršilaca u toku pripreme i izvršenja krivičnog djela, a retko kao objekat napada u krivičnim djelima krađe, drske krađe, uličnih razbojništava. Shodno navedenom u ovom radu će se prezentirati, analizirati i problematizovati specifičnosti koje se odnose na značaj i ulogu mobilnih telefona prilikom rasvjetljavanja krivičnih djela, specifičnosti vezane za primjenu listinga odlaznih i dolaznih poziva, primjenu posebne istražne radnje nadzor i tehničko snimanje telekomunikacija, značaj i ulogu IMEI broja u operativnom radu policije a koje su prilagođene subjektivnim i objektivnim uslovljavajućim faktorima rada policijskih službenika Ministarstva unutrašnjih poslova Republike Srpske.

2. KRIMINALISTIČKI I OPERATIVNI ZNAČAJ IMEI BROJA

IMEI posebno veliku ulogu ima u operativnom radu policije na rasvjetljavanju određenih krivičnih djela u kojima se mobilni telefon pojavljuje kao sredstvo izvršenja krivičnog djela, kao predmet izvršenja krivičnog djela ili u drugim krivičnim djelima (Miladinović, 2008:536). IMEI je skraćenica od engleskih riječi International Mobile Equipment Identity koji bi u slobodnom prevodu mogao da se označi kao jedinstvena međunarodna identifikacija mobilnog telefona. IMEI, u stvari, predstavlja niz od 15 cifri koji sadrže informaciju o porijeklu, modelu i serijskom broju telefona, iz čega proizlazi da IMEI nije serijski broj telefona, mada ima određene karakteristike, usljed čega se tako često (pogrešno) naziva. S kriminalističkog aspekta, najznačajnija karakteristika IMEI-a je što se ne može mijenjati. IMEI omogućava praćenje mobilnog telefona preko mrežnog operatera, te dolaženje do samog mobilnog telefona posrednim putem. Takone, IMEI omogućava i lokalizovanje samog mobilnog telefona. Pored poštovanja svih relevantnih kriminalističko-taktičkih i krivičnoprocesnih pravila a koja se odnose na davanje odgovora na zlatna pitanja kriminalistike, te poštovanja zakonske regulative, posebno je bitan broj kartice koji se nalazio u vrijeme izvršenja krivičnog djela u samom aparatu (sa kog je upućena poruka ili poziv), kao i broj oštećenog (na koji je primljena poruka ili poziv) (Simonović, Pena, 2010: 346). S obzirom na tehničke mogućnosti, u odnosu na broj telefona, najčešće se traže podaci o identifikaciji IMEI koji pripada mobilnom telefonu u kome se nalazio broj koji je telefonu u kome se nalazio broj koji je zloupotrebljen, listing poziva i poruka za taj broj, lokaciju telefona, lokaciju bazne stanice (Banović, 2001: 156). Nakon dobijanja traženih podataka o

listingu, slijedi operativni rad policije na utvrđivanju identiteta korisnika broja telefona koji se nalazi u mobilnom telefonu, kao i na utvrđivanju izvršioca konkretnog krivičnog djela. Sam pronalazak trenutnog korisnika mobilnog telefona ne mora da znači (i najčešće ne znači) da je on izvršilac krivičnog djela, usljed činjenice da izvršilac krivičnog djela, pogotovo kada se radi o ukradenim mobilnim telefonima, najčešće sam otuđeni predmet ne zadržava za sebe, već ga proda, pokloni, zamijeni ili da trećim licima, nakon čega ga oni koriste za vlastite potrebe ili se može desiti da ga i oni preprodaju ili zamijene drugim licima, usljed čega se dešava da se u lancu korisnika mobilnog telefona za relativno kratko vrijeme pronađe više lica. Ukoliko je korisnik broja koji se nalazi u mobilnom telefonu postpejd korisnik, njegovi podaci, ukoliko su traženi naredbom, dostavljaju se uz listing, te se relativno lako utvrđuje sam korisnik. S obzirom na mali broj pretplatnika mobilne telefonije kod nas, male su mogućnosti da se prilikom dostavljanja listinga, dostave i podaci o pretplatniku koji koristi broj sa listinga. Daleko češće se dešava da se listing dostavi bez identifikacije korisnika broja koji se nalazi u mobilnom telefonu. Zbog toga, neophodno je saznati identitet korisnika, kao i pronaći navedeno lice. Postoji više načina da se sazna identitet korisnika broja telefona koji se nalazi u mobilnom telefonu i to: direktno zvanje navedenog broja, pozivanje lica koja su najčešće komunicirala sa spornim brojem, utvrnivanje brojeva fiksne telefonije sa kojima je komunicirao ukoliko se pretpostavlja identitet lica, provjerom preko interneta, na terenu, kroz evidencije (Bošković, 1995:238). Prethodno smo napomenuli da korisnik spornog broja sa listinga koji se nalazi u mobilnom telefonu ne mora da znači da je i izvršilac, usljed čega se mora oprezano postupiti prilikom planiranja verzija i aktivnosti, te na realizaciji planiranih aktivnosti u cilju pronalaska izvršioca i mobilnog telefona. Naime, ukoliko je izvršilac krađe mobilnog telefona svjesno počinio krivično djelo, što je najčešći slučaj, vrlo je vjerovatno da će odmah isti dan, a najkasnije sljedećih dana, htjeti se riješiti navedenog mobilnog telefona, na taj način što će ga prodati, zamijeniti, izvršiti drugo krivično djelo sa njim (iznudu, ucjenu, prijetnju), te ga baciti ili uništiti, dati na poklon ili na poslugu (Kovačević, 2003:135). S obzirom na to, a imajući u vidu tehničke mogućnosti operatera mobilne telefonije koji (najčešće) nisu u mogućnosti da listing dostave isti dan nakon dostavljanja naredbe, odnosno listing se dostavi tek nakon nekoliko dana od dana izvršenja krivičnog djela, rijetke su sitacije kada se mobilni telefon pronane kod izvršioca, već se obično radi o licima koja su kupila, dobila na poslugu ili poklon ili zamijenila mobilni telefon sa izvršiocem ili čak sa drugim licem kom prilikom su i oni sami na taj način dobili u posjed mobilni telefon. Usljed navedenog proizlazi činjenica da u lancu korisnika mobilnog telefona može da bude više lica, što svakako dodatno usložnjava operativni rad na rasvjetljavanju krivičnog djela i pronalasku izvršioca, pogotovo ukoliko se "prekine lanac", odnosno ukoliko jedno lice u lancu ne zna od koga je dobio (kupio) telefon. U ovakvim situacijama, neophodno je hitno podnijeti zahtjev za izdavanje naredbe za listing (Bugarski, 2014:223). Praćenjem lanca korisnika mobilnog telefona unazad, dolazi se do izvršioca konkretnog krivičnog djela. Da bi se listing dobijen na osnovu naredbe koja je izdata na osnovu zahtjeva mogao koristiti u krivičnom postupku, on mora da bude ispravan, odnosno da je izdat na osnovu zakonom utvrnene procedure koja podrazumijeva postojanje osnova sumnje da je izvršeno konkretno krivično djelo, da je zahtjev podnesen od strane tužioca (ili ovlašćenih službenih lica na osnovu saglasnosti tužioca), da je sud cijeneći zahtjev izdao naredbu koja je proslijenena nadležnom operateru, te da je isti postupio u zakonom propisanom roku, te dostavio listing policiji (Simović,

2005:458). Takođe, dostavljeni podaci se, uz izvještaj o realizaciji naredbe, moraju dostaviti sudu u zakonom propisanom roku, inače se navedeni podaci (listing) neće moći koristiti na sudu kao dokaz. Nakon utvrđivanja identiteta korisnika spornog broja telefona sa listinga koji se nalazi u mobilnom telefonu, primarno je da se pronane otuđeni mobilni telefon, te da se isti oduzme. S krivičnoprocesnog aspekta, ispravno je da se, nakon identifikovanja korisnika otuđenog telefona, izda naredba za oduzimanje predmeta, te da se na osnovu te iste naredbe navedeni predmet oduzme. Nakon oduzimanja predmeta, te utvrđivanja istovjetnosti pregledanjem IMEI-a, oduzeti predmet se, uz izvještaj o realizaciji naredbe, u zakonom propisanom roku mora dostaviti sudu koji je izdao naredbu za pretresanje (Lukić, 2005:122). Naravno, licu od kog je oduzet predmet izdaće se potvrda o privremenom oduzimanju predmeta. Moguća je sitacija da se predmet nađe odbačen na odrenenom lokalitetu ili neposredno prije preduzimanja odrenenih operativno-taktičkih mjera i radnji (praćenje, opservacije, lišenje slobode, legitimisanje) i istražnih radnji (pretresanje), kom prilikom se, ukoliko lokacija gdje se nalazi odbačen telefon nije obuhvaćena izdatom naredbom ili ukoliko uopšte ne postoji naredba za pretresanje, treba izvršiti uvinaj na licu mjesta krivičnog djela, odnosno pronalaska predmeta. Kriminalistički je ispravno da se prilikom izuzimanja mobilnog telefona, kao i prilikom izuzimanja mobilnog telefona na osnovu naredbe suda, a uvijek kada isti ne predaje korisnik telefona ili se istoj fizički ili verbalno protivi ili ne priznaje izvršenje krivičnog djela, kao ni bilo kakvu povezanost sa krivičnim djelom ili posjedovanjem mobilnog telefona, da se navedeni telefon izuzme, poštujući određena kriminalističko-taktička i kriminalističko-tehnička pravila, odnosno da se isti obilježi, fiksira, fotografiše, opiše detaljno gdje se nalazio i u kom je stanju, te da se potom izuzme rukavicama, a po potrebi da se sa istog izazvaju i izuzmu eventualni otisci papilarnih linija, koji se trebaju poslati na daktiloskopsko vještačenje (Škulić, 2005:178). Kada su u pitanju lica koja su koristila mobilni telefon, od svih lica koja su koristila mobilni telefon, odnosno od svih lica čija se kartica nalazila u mobilnom telefonu, a ne samo od lica od kog je oduzet telefon, odnosno od lica čija se kartica nalazila u telefonu prilikom oduzimanja, mora se uzeti izjava na okolnosti posjedovanja mobilnog telefona. U kom će se svojstvu uzeti izjava, zavisi od niza okolnosti. Naravno da se uvijek prilikom uzimanja izjave od lica u svojstvu osumnjičnog mora uzeti u obzir mogućnost da je navedeno lice i stvarni izvršilac konkretnog krivičnog djela iz kog potiče mobilni telefon, ali da navodi određene okolnosti koje mu idu u prilog za lakše krivično djelo. Tek kada se utvrde sve okolnosti pod kojima je izvršeno krivično djelo, a lice kod kog je pronađen mobilni telefon ponudi alibi ili na drugi način odagna sumnju da je isti stvarni izvršilac krivičnog djela, treba od istog uzeti izjavu u svojstvu osumnjičenog za prikrivanje krivičnog djela ili, ukoliko se procjeni, uzeti izjavu u svojstvu svjedoka (Miladinović, 2008:538). Prateći lanac korisnika telefona unazad, dolazi se do pravog izvršioca krivičnog djela, naravno ukoliko sva lica znaju od koga su prethodno kupila mobilni telefon, što ne mora uvijek da bude slučaj. Nakon što se done do stvarnog izvršioca krivičnog djela, a ukoliko on nije korisnik mobilnog telefona, što je najčešći slučaj, on može priznati ili negirati krivično djelo. Ukoliko isti prizna krivično djelo uzima se izjava u svojstvu osumnjičenog za konkretno krivično djelo. U izjavi treba navesti i koje je kartice lice koristilo, te sva lica koja su znala da osumnjičeni posjeduje ili da je ukrao navedeni mobilni telefon, te nakon toga i od tih lica uzeti izjavu. Takone, ispravno je uzeti izjavu i od lica koja

saznaju da osumnjičeni koristi navedeni broj telefona, kao i od lica koja su kod njega vidjeli sporni mobilni telefon.

3. PRIBAVLJANJE LISTINGA TELEFONSKOG PRETPLATNIČKOG BROJA

U suzbijanju i sprečavanju kriminaliteta postoji stalna težnja da se izgradi kriminalističko istraživanje i sudsko procesuiranje sa ciljem da se svaki izvršilac krivičnog djela kazni i da mu se onemogući izbjegavanje krivičnog progona. Mjera prikupljanja podataka putem kriminalističko-analitičkog tumačenja i istraživanja listing odlazno-dolaznih poziva sa određenog telefonsko-pretplatničkog broja u velikom broju zemalja u svijetu poznatija je kao ‘’metering’’ (eng. metering, meter chek printer-evidentiranje telefonskih brojeva sa kojih se poziva i brojeva koji se pozivaju, vrijeme i trajanje poziva, SMS poruke ali ne i evidentiranje sadržaja razgovora). Riječ je o radnji koja se u svijetu najčešće primjenjuje na osnovu konkretnih, jasnih i nedvosmislenih zakonskih ovlaštenja, od strane državnih organa (suda, tužilaštva ili službi bezbjednosti), sa ciljem sprečavanja ili suzbijanja najopasnijih oblika kriminala. Pitanje da li listing telefonskog pretplatničkog broja predstavlja posebnu istražnu radnju ili ne, izazvalo je dosta rasprave i polemike u krivično procesnoj praksi u Bosni i Hercegovini. Na početku treba reći da postoje dva različita stanovišta po ovom pitanju. Prvo stanovište je da “listing” predstavlja posebnu istražnu radnju. Zastupnici ovog stanovišta kao argumentaciju navode : prikupljanje podataka o tome ko je koga nazivao u određenom vremenu, ili sa kojeg telefonskog priključka, odnosno prikupljanje popisa teleosnkih brojeva koje je nazivala osumnjičena osoba ili sa kojeg su nazivali osumnjičenu osobu – predstavlja vid posebne istražne radnje nadzora i tehničkog snimanja telekomunikacija. Zbog toga, prikupljanje podataka koji se mogu označiti kao evidentiranje telefonskih brojeva i telefosnkih razgovora osumnjičene osobe, predstavlja nadzor telefonskih razgovora, iako se na osnovu popisa korištenih telefonkih brojeva ne saznaje sadržina telefonskih razgovora (Simović, 2005:567). Drugo stanovište je da listing ne predstavlja posebnu istražnu radnju, a kao argumentacija takvog stava ističe se da se putem listinga ne ostvaruje uvid u sadržinu telefonskih razgovora, pa se prema tome i ne može raditi o nadzoru telekomunikacija u njihovom sadržinskom smislu, odnsono stepen zadiranja u privatnost prilikom uvida u “listing” nije toliki da bi ga okarakterisao kao posebnu istražnu radnju. Analizirajući oba stanovišta može se izvući nekoliko zaključaka: Naime, sasvim sigurno pribavljanje spiska dolaznih i odlaznih poziva osumnjičenog lica predstavlja ograničenje odnosno narušavanje prava na privatnost, ali isto tako, narušavanje prava na privatnost podrazumjevaju i mnoge druge radnje dokazivanja kao sto su pretresanje, naredba banci ili drugom pravnom licu, privremeno oduzimanje pisama telegrama i drugih pošiljki i dr. a ipak se te radnje dokazivanja ne tretiraju kao posebne istražne radnje (Bošković, Skakavac, 2005:368). Naime, pogrešno je konstatovati da je osnov uvođenja posebnih istražnih radnje nadzora i tehničkog snimanja telekomunikacija, prosto zadiranje u privatnost osumnjičenog, jer je zadiranje prava u privatnost moguće i dozvoljeno i sa nekim drugim radnjama dokazivanja koje nemaju karakter posebnih istražnih radnji. Ono što razdvaja i što čini distinkciju između klasičnih radnji dokazivanja kojima se zadire u privatnost i neka druga prava i posebne istražne radnje nadzora i tehničkog snimanja telekomunikacija je stepen zadiranja u to prava, odnosno stepen ograničavanja prava osumnjičenog odnsono drugih lica. Npr. privremenim oduzimanjem

pisama, telegrama i drugih pošiljki, duboko se može ući u privatnost osobe, a ipak ta radnja dokazivanja nema karakter posebne istražne radnje. Kada je u pitanju sam "listing" radi se o spisku dolaznih i odlaznih poziva sa određenog i na određeni telefonski broj, a o čemu preduzeće koje pruža usluge u oblasti telekomunikacija vodi službenu evidenciju. Naime, kada se osoba odluči za prijavljivanje telefonskog broja kod određenog preduzeća koje pruža usluge u oblasti telekomunkacija, ona je svjesna i pristaje da to preduzeće vodi službenu evidenciju o dolaznim i odlaznim pozivima sa tog broja, pa se čak u većini preduzeća u evropi a i kod nekih u BiH uz račun dostavlja i spisak takvih poziva, te taj spisak u stvari čini osnovu izrade računa i njegov integralni dio. Međutim, ta osoba prijavljivanjem telefonskog broja kod određenog preduzeća koje pruža usluge iz oblasti telekomunkacija, nije svjesna niti je pristala da bilo ko sluša njene telefonske razgovore, zbog toga je ulaženje u sadržaj razgovora zaista veliki stepen zadiranja u privatnost osobe, zbog čega je takvo zadiranje u takvu privatnost i obuhvaćeno mjerom nadzora i tehničkog snimanja telekomunikacija kao posebnom istražnom radnjom za koju su propsani posebni uslovi (Sijerčić-Čolić, Simović, 2005: 552). Međutim, kada se traži "listing" suštinski se traži podatak iz službene evidencije preduzeća koje se bavi pružanjem usluga iz oblasti telekomunkacija, te se radi suštinski o privremenom oduzimanju predmeta-dokumentacije, a nikako o posebnoj istražnoj radnji, a naročito kada se ima u vidu da se listing po svojoj prirodi može tražiti samo za već obavljene telefonske razgovore, a nikako za one koji su u toku. Prema tome nema presretanja telefonskih razgovora (real time ili on line nadzor kako je to kod posebne istražne radnje nadzora i tehničkog snimanja telekomunikacija), pa prema tome nema ni nadzora takve komunikacije, a posebno imajući u vidu da se listingom ne saznaje sadržina telefonskih razgovora. Na osnovu navedenog može se zaključiti da listing odlaznih i dolaznih poziva i SMS poruka ne predstavlja posebnu istražnu radnju ali pri pribavljanju istoga moraju biti ispunjeni određeni uslovi. Naredbu za pribavljanje izvještaja odlazno-dolaznih poziva telefonskog pretplatničkog broja izdaje nadležni sud ili tužilaštvo na obrazložen zahtjev pripadnika služni bezbjednosti. Naredba za pribavljanje izvještaja odlazno-dolaznih poziva sa pretplatničkog broja građanina mora da sadrži osnov za sprovođenje ove mjere, odnosno postojanje osnova ili osnovane sumnje. Ukoliko se preduzima u preventivne svrhe (proaktivna i preventivna kriminalistička istražianja) neophodno je izložiti činjenice koje ukazuju na to da neposredno predstoji izvršenje krivičnog djela ili da je njegovo izvršenje već započeto. Kada se koristi poslije izvršenja krivičnog djela (represivna-kriminalistička istraživanja) u naredbu je potrebno unjeti činjenice koje ukazuju na postojanje dovoljnog stepena sumnje da je izvršilac preko pretplatničkog broja za koji se traži izvještaj i identifikacija vlasnika obavljao razgovore u vezi sa izvršenjem krivičnog djela (Mijalković, Manojlović, 2008:153). Da bi listing dobijen na osnovu naredbe koja je izdata na osnovu zahtjeva mogao koristiti u krivičnom postupku, on mora da bude istravan, odnosno izdat na osnovu zakonom utvrđene procedure koja podrazumjeva postojanje osnova sumnje da je izvešeno krivično djelo, da je podnesen od strane tužioca (ili ovlaštenih službenih lica na osnovu saglasnosti tužioca), da je sud cijenjeci zahtjev izdao naredbu koja je proslijeđena nadležnom operateru, te da je ovaj postupio u zakonom propisanom roku od 72 časa, te da je listing dostavio policiji.

4. POSEBNA ISTRAŽNA RADNJA NADZOR I TEHNIČKO SNIMANJE TELEKOMUNIKACIJA

Korišćenje savremenih naučnih i tehnoloških dostignuća u sprečavanju i suzbijanju kriminaliteta, pogotovo u segmentu njegovog otkrivanja i obezbeđenja dokaza, smatra se imperativom u savremenim uslovima. Kada je reč o borbi protiv savremenog kriminaliteta, s pravom je primećeno da organi krivičnog gonjenja mogu imati uspeha u suzbijanju teških krivičnih dela, a naročito organizovanog kriminala, samo uz korišćenje savremenih tehničkih sredstava (Radulović, 2004: 461). Posebne istražne radnje se preduzimaju pre početka krivičnog postupka, s ciljem da se otkrije struktura, oblik i metode delovanja kriminalnih organizacija u cilju pokretanja postupka protiv pripadnika tih organizacija (Lukić, 2005:79). U tom cilju bi, prema shvatanju Evropskog suda za ljudska prava, zakonodavac morao da označi krug lica prema kojima može biti primenjena neka od takvih mera, prirodu krivičnih dela koja pružaju osnov za to, vremenske granice trajanja nadzora i snimanja, uslove za sastavljanje zapisnika o zabeleženoj komunikaciji, načine njihove kontrole, kao i da predvidi razloge za brisanje i uništavanje snimaka. Odredbe o posebnim istražnim radnjama u ZKP RS privremeno ograničavaju ustavna prava i slobode u vezi s krivičnim postupkom i stvarno znače pravno regulisanje posebnih mera za borbu protiv najopasnijih oblika kriminaliteta – terorizma i organizovanog kriminaliteta (Veić, 1996:669). Analizirajući uslove za njihovu primenu, može se zaključiti da se te mere mogu relativno široko primenjivati. Taj zaključak temeljimo najpre na odredbi člana 234 stav 1, po kojoj se posebne istražne radnje mogu odrediti "ako se na drugi način ne mogu pribaviti dokazi ili bi njihovo pribavljanje bilo skopčano sa nesrazmernim teškoćama." Posebna istražna radnja nadzor i tehničko snimanje telekomunikacija se sastoji se u tajnom nadzoru (prisluškivanju) i snimanju razgovora koji se vode sredstvima komunikacije na daljinu, i to njihovim "presretanjem" (detournement, interception) (Banović, 2001:314). Tehničkim putem registrovana komunikacija između nadziranih lica, nakon prepisa u izvornik, može poslužiti, prema slobodnom sudijskom uverenju, kao dokaz o izvršenju određenih krivičnih dela od nadziranih lica. Tom merom obuhvaćen je nadzor i tehničko snimanje svih sredstava za tehničko komuniciranje na daljinu, npr. teleksa, telefaksa, elektronske pošte i sličnih uređaja. U tehničkom pogledu taj nadzor se odnosi na sva tehnička sredstva u bilo kojem obliku (stacioniranom, mobilnom, analognom, digitalnom, tonskom, slikovnom, integrisanom i dr.) koja korisnici upotrebljavaju – bilo preko poštanskih (npr. privatni telefonski priključci, javne govornice i sl.), bilo preko drugih organizacija (npr. telekomunikacije u prometu i sl.), a na koja se proteže ustavnopravna i krivičnopravna zaštita (Krapac, 2002:197). Policijski organi, zaduženi za tehničko provođenje ove posebne radnje, pre samog snimanja dužni su na tehničkom snimku zabeležiti broj sudske naredbe na osnovu koje se postupa, mesto i vreme početka primene mere, podatak da li je registracija menjana, kopirana i u koliko primeraka, kao i vreme završetka primene ove radnje. Sudu se uvek dostavlja izvornik tehničkog snimka, s nužnim podacima za moguću proveru verodostojnosti na taj način prikupljenih saznanja – kako bi se on tokom postupka mogao koristiti kao dokaz, predmet uviđaja ili veštačenja. Pregled pronađenog ili privremeno oduzetog mobilnog telefona ne predstavlja posebnu radnju iz člana 234 stav 2 tačka a), nego pretres pokretne stvari kao "sličnog uređaja za automatsku obradu podataka" (član 115 stav 2).

5. ZAKLJUČNA RAZMATRANJA

Korišćenje savremenih naučnih i tehnoloških dostignuća u sprečavanju i suzbijanju kriminaliteta, pogotovo u segmentu njegovog otkrivanja i obezbeđenja dokaza, smatra se imperativom u savremenim uslovima. Policijski službenici moraju konstantno osmišljavati metode suzbijanja krivičnih djela gdje se kao sredstvo ili predmet izvešenja krivičnog djela koristi mobilni telefon sa posebnim akcentom na krivičnoprocesne aspekte pribavljanja dokaza i dokumentovanja preduzetih mjera i radnji. Navedene mjere i radnje na planu suzbijanja i rasvjetljavanja krivičnih djela, shodno ekspanziji tehničko-tehnoloških dostignuća, pogotovo u oblasti mobilne i kompjuterske tehnologije, neminovno je ne preduzimati bez upotrebe tehničkih potencijala operatera mobilne telefonije, kom prilikom se ostvaruje zajednički cilj i policije i operatera mobilne telefonije. Upotreba IMEI-ja predstavlja jedan od najčešćih i najboljih načina rasvjetljavanja krivičnih djela koja imaju veze sa mobilnim telefonima, odnosno gdje se mobilni telefoni pojavljuju kao predmeti ili kao sredstva izvršenja krivičnih djela. Međutim, jasno je da sam pronalazak otuđenog ili spornog mobilnog telefona najčešće ne dovodi do izvršioca krivičnog djela, usljed čega je neophodno preduzimati i niz drugih operativno-taktičkih mjera i radnji i istražnih radnji na planu otkrivanja izvršioca konkretnog krivičnog djela, kao i potencijalih izvršilaca drugih krivičnih djela. Iz navedenog proizlazi značaj kriminalističkog rada nakon dobijenog listinga na osnovu IMEI-ja kom se mora posvetiti posebna pažnja, odnosno on mora da se zasniva na planskom postupanju po postavljenim verzijama, shodno svim kriminalističkim pravilima operativnog rada. S druge strane, s obzirom na to da listing, najčešće, predstavlja in(d)icijalnu činjenicu na osnovu koje se preduzimaju druge mjere i radnje usmjerene na pronalazak izvršioca, neophodno je da se sve mjere i radnje koje se preduzimaju prilikom operativnog rada izvode, pored kriminalističkih pravila, i u skladu sa zakonskim odredbama, prevashodno u skladu sa krivičnoprocesnim pravilima postupanja, pogotovo što suprotno postupanje, shodno tzv. "pravilima ploda otrovne voćke", može da negira sve rezultate do kojih se dođe tokom istrage ukoliko je početni dokaz (listing) pravno nepodoban, odnosno nije u skladu sa zakonom.

LITERATURA

Bošković M. (1995). *Kriminalistika metodika I*, Beograd, 1995.

Banović B. (2001). *Korišćenje specijalnih sredstava za nadzor komunikacija u prekrivičnom i krivičnom postupku i ljudska prava.* Beograd.

Bošković M., Skakavac Z., (2009). *Organizovani kriminalitet.* Novi Sad.

Bugarski T. (2014). *Dokazne radnje u krivičnom postupku*. Novi Sad.

Kovačević V. (2003). *Metodika istraživanja imovinskih delikata*, Novi Sad.

Krapac D. (2002). *Zakon o krivičnom postupku i drugi izvori hrvatskog procesnog prava.* Zagreb.

Lukić T. (2005). *Otkrivanje i dokazivanje dela organizovanog kriminala u Srbiji*. Novi Sad.

Miladinović A. (2008). *Značaj IMEI-a prilikom rasvjetljavanja krivičnih djela.* Brčko.

Mijalković S., Manojlović D., (2008). *Pribavljanje listing telefonskog pretplatničkog broja građanina-kontroverze u radu nacionalnih Sistema bezbednosti*, Beograd.

Radulović D. (2004). *Specijalne istražne radnje i valjanost dokaza pribavljenih preduzimanjem tih radnji u krivičnom procesnom zakonodavstvu Srbije i Crne Gore i opšteprihvaćeni standardi.* Beograd.

Simonović B., Pena U. (2010). *Kriminalistika*, Istočno Sarajevo.
Simović (2005). *Komentar krivičnog zakona Republike Srpske*, Sarajevo.
Simović M., Sijerčić-Čolić, H., Hadžiomeragić, D., Jurčević, M. (2005) *Komentari zakona o krivičnom/kaznenom postupku u Bosni i Hercegovini*. Vijeće Europe/Europska komisija, Sarajevo.
Škulić M. (2005). *Prikriveni islednik – zakonsko rešenje i neka sporna pitanja.* Beograd.
Veić P. (1996). *Krivičnopravne mogućnosti suzbijanja organizovanog kriminaliteta*, Zagreb.

Mladen Vuković

SIGNIFICANCE AND ROLE OF CELL PHONES IN DETECTING CRIMINAL OFFENSES

Summary

Combating crime is a continuous and ever-present concern in overall security issues and security situation in society. Cell phones, which are more and more used as a means of communication among people, are also used for making arrangements among people stemming from criminal environments, so that by using appropriate technical means we may learn and record content of such conversations and even identify interlocutors since the cell phone user may be located almost anywhere. As cell phones form an essential part of everyday business and family aspect of every person's life, it is only understandable that its abuse is more and more important, both in terms of quality and quantity. Since everyday activities are conditioned by possession of a cell phone, cell phones become the means of perpetrating a crime. Police authorities must pursue scientific advances in cell phone technologies while keeping up with technical possibilities of cell phone operators and finding and adapting methods of their own criminal investigation work aiming at preventing crime. The paper shows, analyzes and presents specific issues referring to the importance and role of cell phones in detecting criminal offenses, role of call and text messages detail records, importance of IMEI number in the operational work of the police, specific issues referring to the special investigation technique of surveillance and technical recording of telecommunications, which are adapted to subjective and objective conditioning factors of the work of police officers of the Republika Srpska.

Key words*: cell phone, IMEI, detection, proving, special investigation techniques.*

PREGLEDNI ZNANSTVENI RAD

Krunoslav Borovec[173]

Iva Balgač[174]

UVOĐENJE POLICIJSKIH KAMERA U RAD SLUŽBE POLICIJSKE OPHODNJE – OTVORENA PITANJA USPJEŠNE IMPLEMENTACIJE I EGZAKTNE PROCJENE UČINKA NA RAD POLICIJE

Sažetak

Razvoj društva općenito, pa i razvoj novih tehnologija, utječe na policijsku službu, taktike i metode njezinog rada na dnevnoj osnovi. Jedna od zadnjih tehnoloških inovacija koja se sve značajnije primjenjuje u radu policijskih organizacija širom svijeta jesu i kamere (engl: Body Worn Cameras – BWC) koje policijski službenici koriste tijekom redovnog obavljanja policijske službe. Policija u Hrvatskoj započela ih je primjenjivati od konca 2015. godine u pet najvećih policijskih uprava, odnosno u gradovima Zagrebu, Splitu, Osijeku, Rijeci i Puli. Na temelju prvih iskustava različitih policijskih organizacija koja su pokazala da korištenje kamera u radu policije može imati i pozitivne i negativne aspekte, zaključeno je kako se ne radi o jednostavnom pitanju, svedenom na tehničke aspekte korištenja nove opreme, već o cijelom nizu važnih tema koje se odnose na uspješnu implementaciju videokamera u policijski rad te na relevantnu, znanstveno utemeljenu procjenu njihovog učinka na policijsku praksu. Stoga je ovaj rad rasprava o važnim temama implementacije: zašto koristiti kamere, kako definirati procedure i taktiku postupanja, na koji način koristiti snimljeni videomaterijal, pitanje treninga za korištenje kamera, ali i pravna pitanja poput zaštite ljudskih prava, povrede privatnosti i drugo. Ovaj rad pruža i raspravu o pitanjima evaluacije, odnosno upućuje na ključna područja koja bi se trebala istraživati u vezi s korištenjem policijskih kamera. Na temelju do sada provedenih istraživanja i onih koja su još u tijeku, kao ključna istraživačka pitanja nameću se: utjecaj kamera na interakciju između policije i građana, utjecaj kamera na ponašanje policijskih službenika, njihovi stavovi o korištenju kamera u svakodnevnom radu, utjecaj kamera na ponašanje građana i njihovi stavovi prema tome, utjecaj kamera na probitak kriminalističkog istraživanja kaznenog djela ili prekršaja, utjecaj kamera na korupciju, policijski integritet i legitimitet, odnosno povećavaju li kamere sigurnost policijskih službenika te smanjuju li pritužbe na njihov rad.

Ključne riječi: *policijske kamere, implementacija, protokol, učinak kamera, aspekti istraživanja.*

[173] Krunoslav Borovec, pomoćnik glavnog ravnatelja policije i načelnik Uprave policije, MUP RH, e-mail: kborovec@mup.hr

[174] Iva Balgač, policijska službenica za međunarodnu policijsku suradnju u Uredu glavnog ravnatelja policije, MUP RH, e-mail: ibalgac@mup.hr

1. UVOD

Iako se temeljna uloga i zadaće policije u smislu očuvanja reda i sprečavanja kriminaliteta već dugi niz godina nije bitno promijenila, policijski rad kroz povijest bio je prožet čestim promjenama i to u odnosu na organizaciju policije, ali i u kontekstu taktika i metoda rada. Na policiju veliki utjecaj ostavlja tehnološki i znanstveni razvoj, međutim ne smije se zanemariti utjecaj promijenjene političke i društvene svijesti građana. Na polju političkih i društvenih promjena na rad policije najsnažniji utjecaj imaju jačanje ljudskih prava, jačanje političkih sloboda i društvene svijesti, te sve veća emancipacija marginaliziranih društvenih skupina stanovništva: manjine, žene, mladi, LGBT osobe i drugi. U skladu s tehnološkim revolucijama i inovacijama policija se sve više oslanja na nove tehnologije, u početku ponajviše na telekomunikaciju i prometnu tehniku, a to prije svega uključuje radio (mogućnost komunikacije na daljinu), ophodna vozila (veća mobilnost i mogućnost brže intervencije), zatim raširenо korištenje različitih znanstvenih metoda u forenzici (učinkovitije identificiranje i praćenje počinitelja te dokazivanje kaznenih djela), djelotvornu primjenu modus operandi sustava (adekvatna reakcija na kriminalni recidivizam), a kasnije na digitalnu tehnologiju, odnosno informatička dostignuća. Posebno novi, trenutno aktualni projektni/poslovni model rada policije, koji je u policijskoj praksi operacionaliziran kao kriminalističko-obavještajni model (*ILP model*) (Kovčo, Borovec, Ljubin Golub, 2013), pod velikim je utjecajem novih tehnoloških dostignuća. Dakle, tehnologija mijenja rad policije na dnevnoj osnovi.

Najnovije tehnologije imaju značajan utjecaj na javne politike u području sigurnosti te procedure i standardne postupke, pa čak i na način kako policijski službenici obavljaju svoje dnevne dužnosti (Ramirez, 2014). Stil rada policije, nove strategije i taktike usvojene od strane rukovodstva mogu diktirati ponašanje policajaca i u pozitivnom i u negativnom smjeru (National Research Council, 1994). Upravo zbog toga, u kontekstu primjene novih tehnologija u svakodnevnom radu policije, važno mjesto imaju i sustavi za audio/videodokumentiranje postupanja policije. Naime, već s razvojem VHS tehnologije policija je počela koristiti videokamere radi fiksiranja i dokumentiranja određenih činjenica važnih za njihov rad, prije svega za dokumentiranje stanja zatečenog na mjestu kaznenog djela ili za dokumentiranje pojedinih dokaznih radnji (ispitivanje okrivljenika, snimanja radnje prepoznavanja osoba i slično), a nakon toga i za snimanje policijskog postupanja, *SWAT* timova i jedinica interventne policije kada postupaju na mjestima na kojima se očekuje značajnije narušavanje javnog reda i mira, odnosno veće policijske intervencije. U korištenju audio-vizualne opreme pojavile su se kamere nošene na tijelu (engl. *Body Worn Cameras*), za koje se još uvijek ne može reći da su standardni dio policijske opreme, već su trenutno u fazi testne primjene. Uvažavajući činjenicu da je u posljednjih nekoliko desetljeća policija značajno povećala korištenje napredne tehnologije, za mnoge policijske rukovoditelje glavni izazov nije donošenje odluke treba li se koristiti određena tehnologija ili ne, već pronaći najbolji omjer korištenja različitih tehnologija ovisno o problemima kriminaliteta, dostupnim sredstvima iz proračuna te drugim čimbenicima (Miller, Toliver, 2014).

Prema Whiteu (2014) nove tehnologije se sve češće koriste kao mehanizam nadzora i promatranja i građana i policije. Opće je poznato da je policiji dopuštena velika diskrecija

kada se bavi s građanima i stoga je važno pitanje, koje ponovno dolazi u fokus interesa zbog intenzivnije uporabe kamera, koliko daleko može policija zadirati u građanske slobode u interesu kontrole kriminala (Bayley, 2002). Početkom 90-ih godina prošlog stoljeća kamere na komandnim pločama automobila pojavile su se kao nova metoda za snimanje događaja između policije i građana u stvarnom vremenu. Kamere za videonadzor – CCTV kamere također su postale vrlo popularne među gradskim vlastima i policijom kao metoda nadzora (prevencija kriminaliteta) i kao alat za kriminalistička istraživanja. Sve veća dostupnost tzv. pametnih telefona značajno je povećala mogućnost snimanja događaja u trenutku njihovog odvijanja, posebice onih između policije i građana. Kao rezultat svega navedenog videosnimke i audiosnimke postale su sveprisutan dio života u 21. stoljeću.

Britanske policijske agencije bile su među prvima koje su počele eksperimentalno uvoditi i testirati učinak policijskih kamera (White, 2014). Harris (2010) navodi kako su prve primjene započele u Plymouthu, Engleska 2005. i 2006. godine, a prva studija primjene kamera u SAD-u provedena je na slučaju policije Rialta, Kalifornija, tijekom 2012. i 2013. godine. Počeci primjene kamera nošenih na tijelu povezuju se s ne tako davnim događajima u SAD-u, Ferguson i Baltimor, tijekom kojih je policija uporabila smrtonosnu silu što je potaklo i policiju ali i građane, udruge za ljudska prava, gradska vijeća pa čak i predsjednika Obamu da snažnije inzistiraju na uvođenju kamera (Lum i sur., 2015, Elliott, 2015). Naime, pokušaji da se rekonstruiraju događaji i reakcija policajaca u tim događajima te utvrdi zakonitost ili nezakonitost njihovog postupanja izazvali su brojne polemike, tako da se očekivalo da će snimke događaja otkloniti sve dvojbe. Upravo zbog toga, kamere su, od pitanja koje je do tada dobivalo malo na važnosti i pažnji, postale visoko postavljene na listi prioriteta i uvrštene u vrh lokalnih politika te su za njih pronađena sva potrebna sredstva (Lum i sur., 2015). To zapravo znači da su se kamere pojavile, odnosno prepoznale kao potencijalno rješenje za pitanje građanskog povjerenja u policiju i policijski legitimitet (Elliott, 2015).

Bez obzira na dostupne modele policijskih kamera, njihova osnovna funkcija je da snime postupanje policijskog službenika, njegovu komunikaciju i drugu interakciju s građanima (Sousa i sur., 2015). U vezi s tim postavljena su i određena očekivanja u odnosu na uvođenje kamera nošenih na tijelu u svakodnevni policijski rad. Prije svega smatra se kako će kamere imati utjecaja, u pozitivnom smislu, na ponašanje i policijskih službenika i građana jer će biti manje pritužbi građana na policijsko postupanje, policijski službenici će manje primjenjivati silu te će biti manje napada na policijske službenike (James, 2014). Također se očekuje kako policijske kamere mogu utjecati na povećanje transparentnosti policije, kako mogu poboljšati policijsku obuku i trening. Pretpostavlja se da će korištenje policijskih kamera uvelike doprinositi sigurnosti policijskih službenika, olakšati situacijsku svijest te osiguravati dokaze za sudske postupke u rasvjetljavanju i rješavanju kaznenih djela. Zagovornici policijskih kamera tvrde kako ova nova tehnologija može promijeniti situaciju te će poboljšati policijsku odgovornost. Snimka policijskog postupanja i onoga što se dogodilo otežava policijskim službenicima poricanje prekomjerne upotrebe sile ili druge nedopuštene radnje, te je također teže osobama koje optužuju policiju za nedopušteno ponašanje to dokazati u slučajevima kada se takvo ponašanje nije dogodilo (Blitz, 2015). Pozitivna očekivanja od uvođenja u policijski rad kamera nošenih na tijelu jednim dijelom bila su zasnovana i na dobrim rezultatima koje su ostvarile kamere instalirane u policijske

automobile (Maghan i sur., 2002, Maxfield i Andresen, 2001). Naime, istraživači (Rosenblatt i sur., 2004) dokumentirali su da kamere u automobilima doprinose učinkovitom radu policije jer:

- povećavaju sigurnost službenika
- podižu razinu policijske, osobne ali i organizacijske odgovornosti
- pružaju bolji uvid u incidente
- jačaju novo zapošljavanje i usavršavanje
- poboljšavaju percepciju zajednice i medija
- jačaju policijsko vodstvo
- poboljšavaju shvaćanje predmeta/slučaja od strane tužiteljstva
- podižu kvalitetu obavljanja policijskih poslova i jačaju profesionalizam
- povećavaju ukupnu sigurnost.

Bez obzira na velika očekivanja, želja za brzom implementacijom kamera u svakodnevno policijsko postupanje izazvala je kritike i skepticizam. Kritičari kamera (prema Blitzu, 2015) naglašavaju kako su kamere prijetnja privatnosti građana. Posebnu prijetnju predstavljaju kada policijski službenici snimaju postupanje u kući ili nekom drugom privatnom prostoru osobe prema kojoj se postupa. Kritičari također naglašavaju kako snimke s kamera nisu u potpunosti objektivne jer snimaju iz određenog kuta, zbog lošeg svjetla moguće je da se neki detalji ne vide, policijske kamere ne snimaju policijskog službenika već samo ono što je ispred njega. Tome treba pridodati kako korištenje kamera predstavlja vrlo važno pitanje privatnosti i povjerenja građana u policiju (Miller, Toliver, 2014). Jedan od problema sa snimkama koje su dokaz u sudskom postupku jest u tome što postoji mogućnost da se snimke uređuju na takav način da daju lažnu sliku o tome što se stvarno dogodilo (Hak, 2004). Stoga se argumenti za i protiv kamera (White, 2014) mogu sistematizirati kao:

<u>Percipirane koristi:</u>

- Kamere povećavaju transparentnost i policijski legitimitet.
- Policijske kamere uljuđuju, odnosno rezultiraju poboljšanim ponašanjem policijskih službenika i građana.
- Policijske kamere ubrzavaju rješavanje pritužbi građana te pružaju dokaze za uhićenje i procesuiranje počinitelja kažnjivih radnji.
- Policijske kamere pružaju dodatni sadržaj i materijal za obuku i trening.
- Policijske kamere pomažu u neposrednom nadzoru jer pružaju uvid u rad policajaca na terenu.

<u>Percipirane zabrinutosti i problemi:</u>

- Kamere narušavaju privatnost građana.
- Kamere uzrokuju narušavanje privatnosti policijskih službenika jer predstavljaju promjenu u radnim uvjetima policijskih službenika i njihovom svakodnevnom postupanju.

- Upotreba kamera zahtijeva dodatnu obuku i izmjenu zakonodavnog okvira.
- Upotreba kamera zahtijeva određene financijske izdatke i logističku podršku. Uvažavajući prednosti i nedostatke kamera moguće je stvoriti uvjete koji drže u ravnoteži ove dvije krajnosti tako da se kamere koriste u okviru vrlo stroge strategije/politike koja će zaštiti javnost od još jednog sustava koji će se koristiti samo za njihovo nadziranje te održati povjerenje javnosti u integritet zaštite njihove privatnosti (Stanley, 2013). Međutim, mora se priznati da je znanje o učincima ove tehnologije tek u stvaranju. Dosadašnja istraživanja su malobrojna te su u njima ispitani tek neki aspekti uvođenja kamera u svakodnevni policijski rad, uglavnom učinak kamera na policijsko ponašanje. Povrh toga, malo je istraživanja u ovom području koja su koristila valjane znanstvene metode (Lum i sur., 2015).

2. ISTRAŽIVANJA UPORABE KAMERA NOŠENIH NA TIJELU U RADU POLICIJE

Prvi pregled provedenih istraživanja vezanih za policijske kamere napravio je White (2014), za potrebe Saveznog ureda Dijagnostičkog centra za pravosudne programe te je utvrđeno kako je do rujna 2013. godine provedeno samo pet evaluacijskih studija uporabe policijskih kamera. Nakon Whitea, Lum i suradnici (2015) utvrdili su postojanje 12 dovršenih empirijskih studija te 30 istraživanja koja se u tijeku. Na temelju dovršenih istraživanja definirani su određeni zaključci:

- Policijski službenici nemaju nužno negativan stav vezan za kamere (Jennings i sur., 2014, Owens i sur., 2014, Ellis i sur., 2015 prema Lum i sur., 2015).
- Kamere mogu smanjiti pritužbe građana na policiju (Ariel i sur., 2015, Farrar, Ariel, 2013, Goodall, 2007, Katz i sur., 2014 prema Lum i sur., 2015).
- Kamere značajno smanjuju incidente u kojima je korištena sila (Ariel i sur, 2015 prema Lum i sur., 2015).
- Policijski službenici koji nose kamere rjeđe će zaustavljati i uhićivati, a češće će izreći upozorenje (Ready, Young, 2015, prema Lum i sur., 2015).

Istraživanje provedeno 2015. godine u SAD-u, vezano za stavove javnosti spram policijskih kamera (Sousa i sur., 2015), pokazalo je da velika većina ispitanika (tri četvrtine i više) potencijalnim koristima smatra:

- kako je vjerojatno da će ponašanje policajaca prema građanima, ali i osumnjičenicima te žrtvama biti s više poštovanja
- kako je vjerojatno da će se smanjiti uporaba prekomjerne sile i druga nedopuštena ponašanja policije
- kako će se smanjiti broj lažnih optužbi na loše policijsko ponašanje
- kako će se povećati transparentnost i
- kako će se poboljšati prikupljanje dokaza.

Rezultati su pokazali i postojanje zabrinutosti kod jednog dijela ispitanika, koji smatraju:

- kako će se kod svjedoka i žrtava povećati bojazan vezano za suradnju s policijom s obzirom na to da se njihova izjava snima
- kako će građani pokazati određenu bojazan vezanu za pristupanje policiji i raspravu o sumnjivim radnjama u svojoj okolini s obzirom na to da se njihova izjava snima
- kako se snimanjem narušava privatnost svake osobe koja je u dosegu kuta snimanja i
- kako se snimkom narušava privatnost osumnjičenika.

Istraživanja koja su provedena ili se još uvijek provode najčešće istražuju pitanja vezana uz utjecaj kamera na kvalitetu interakcije policije i građana (priroda komunikacije/interakcije; prikaz procesne pravde i profesionalizma; nedolično ponašanje ili korupcija). Visoko istraživan je i utjecaj kamera na primjenu sile u toj interakciji, a popularna istraživačka tema je i stav policijskih službenika o kamerama. Jedan dio istraživanja uključuje pitanja vezana za utjecaj kamera na zadovoljstvo građana tijekom susreta s policijom, utjecaj kamera na zadovoljstvo zajednice te percepciju policije i njenog legitimiteta, utjecaj kamera na slobodu odlučivanja policijskih službenika (posebice prilikom uhićenja) te utjecaj kamera na postupanje osumnjičenika u skladu sa zapovijedi. Nekoliko istraživanja uključuje *cost-benefit* analize korištenja kamera te kako kamere mogu utjecati na kriminalističko istraživanje i policijsku proaktivnost (Lum i sur., 2015).

Istraživački projekti vezani uz propitivanje utjecaja kamera na interakciju policije i građana te zadovoljstvo građana s policijom imaju veliko opravdanje, ako uzmemo u obzir da je subjektivan osjećaj sigurnosti i ukupno zadovoljstvo policijom značajno povezano s percepcijom policije (Borovec, 2013) i prirodom kontakta koji se ostvaruje tijekom te interakcije (Schafer i sur., 2003). Kontakti policije i građana koji rezultiraju sukobima i negativnim emocijama imaju znatno snažniji i dugotrajni utjecaj na odnos građana prema policiji nego pozitivni kontakti međusobne suradnje (Dean, 1980; Rosenbaum i sur., 2005; Weitzer i Tuch, 2005). Prema Hindsu (2009) treba uzeti u obzir da je zadovoljstvo javnosti s policijom uvjetovano stavovima ljudi o tome koliko dobro policija radi svoj posao, legitimitetom policije i o primjeni poštenih procedura, a osobno svjedočenje ili posredno saznanje o neprimjerenim policijskim aktivnostima povezanih s negativnom percepcijom policije (Thomas i Hyman, 1977, prema Brown i Benedict; 2002; Weitzer i Tuch, 2005). Skogan (2006) utvrdio je da je utjecaj doživljenog lošeg iskustva s policijom čak četrnaest puta jači od utjecaja jednog pozitivnog iskustva. Istraživači su pokazali da policijski službenici mogu poboljšati svoj legitimitet, ako obavljaju svoje dužnosti na pošten i neutralan način (Mazerolle i sur., 2013; Tyler, Jeffrey 2008).

Ako nošenje kamera tijekom redovne policijske službe može smanjiti negativno policijsko ponašanje i poboljšati odnos prema građanima te učvrstiti njihov legitimitet, opravdano je uvođenjem kamera očekivati značajne koristi za policijsku organizaciju.

Neka od važnih pitanja još uvijek nisu bila obuhvaćena istraživanjima (Lum i sur., 2015) poput utjecaja kamera na zadovoljstvo poslom policijskih službenika i zadržavanje na poslu, odnosno organizacijsku privrženost. Daljnja istraživanja trebala bi istražiti utječu li kamere na vjerojatnost da policijski službenik inicira proaktivan kontakt. Isto tako treba utvrditi kakav

utjecaj sve to ima na kontrolu kriminaliteta i odnos policije i zajednice. Pored toga, treba utvrditi kakav utjecaj imaju kamere na spremnost građana da pozovu policiju, surađuju kao žrtve ili svjedoci, pomognu u istrazi te postupaju u skladu sa zapovijedima i poštuju autoritet. Potrebno je i više znanja o stavovima vezanim za pitanja privatnosti te o tome mogu li kamere olakšati istraživanja kritičnih incidenata; incidenata u koje su uključeni policijski službenici; incidenata u kojima su policijski službenici koristili vatreno oružje ili je netko ubijen; mogu li poboljšati obuku policije te utjecati na promjene u strategijama; utjecati na odgovornost; nadzor, upravljanje ili disciplinski sustav i interne istrage.

U kontekstu istraživanja utjecaja kamera nezaobilazna su i pitanja koja se odnose na tijek i ishod postupaka koje inicira policija, a koji se odnose na događaje u kojima su korištene kamere, odnosno u kojima postoje snimke kao nositelji dokaza (prekršajni, kazneni ili stegovni postupci). U istraživanjima vezanim za utjecaj kamere i njihove snimke na postupke na sudu treba se bazirati na sljedećem:

- utjecaj kamera na ponašanje tužitelja i njihovu praksu
- utjecaj kamera na ponašanje branjenika i obrane te njihovu praksu
- utjecaj kamera na donositelje odluka (sudce i sudska vijeća)
- utjecaj snimki kamera na ishod postupka općeniti, uključujući odbačaje, presude, osude ili žalbe (Lum i sur., 2015).

Jedno od istraživanja koje je provedeno među državnim odvjetnicima (U. S. Department of Justice, 2012) pokazalo je kako je veliki postotak anketiranih (91%) koristio videodokaze snimljene kamerom, kako je postojanje videodokaza (snimke) olakšalo dobivanje osuđujuće presude te priznanje krivnje prethodno odlasku na sud. Većina državnih odvjetnika (81%) izjavila je kako se smanjilo vrijeme provedeno na sudu, iako 41% kako se njihovo vrijeme pripreme povećalo u slučajevima kada je snimka bila dokaz.

3. HRVATSKA ISKUSTVA U PRIMJENI KAMERA NOŠENIH NA TIJELU U RADU POLICIJSKIH SLUŽBENIKA

Pitanje uvođenja kamera nošenih na tijelu u svakodnevni rad policijskih službenika aktualno je i u Republici Hrvatskoj. Naime, 2014. godine hrvatska policija pokrenula je projekt e-policija, u okviru kojeg je predviđeno opremanje policijskih ophodnji kamerama nošenih na tijelu. U oglednoj fazi ovog projekta koja još uvijek traje, policijski službenici u pet najvećih gradova u Republici Hrvatskoj opremljeni su sa 200 kamera te 10 stacionarnih "Sustava za upravljanje policijskim kamerama – e-Kiosk." U ovom projektu uvođenja nove tehnologije u rad policije imalo je cilj:

- Povećati zaštitu policijskih službenika prilikom policijskog postupanja.
- Povećati zaštitu građana prilikom policijskog postupanja.
- Minimalizirati mogućnost korupcije.
- Opremiti policijske službenike ICT opremom i osuvremeniti njihov rad.
- Probitak kriminalističkog istraživanja.

- Automatiziranje radnih procesa u postupanju policijskih službenika.

Neposredno prije prve primjene policijskih kamera napravljene su Izmjene i dopune Zakona o policiji, kako bi se stvorile zakonske pretpostavke snimanja policijskog postupanja kamerama nošenim na tijelu, a uz novu ovlast danu policiji definirana je i obveza prethodne objave/najave snimanja te period čuvanja/pohrane snimljenog materijala.

"Zakon o policijskim poslovima i ovlastima (Narodne novine 76/09. i 92/14.)
članak 3.a:

1) *Policija je ovlaštena, u mjeri u kojoj je to potrebno, kao i radi nadzora zakonitosti postupanja policijskih službenika, zvučno i vizualno ili na drugi način snimiti obavljanje policijskih poslova i primjenu policijskih ovlasti odgovarajućim tehničkim uređajima.*
2) *Policija će snimanje iz stavka 1. ovoga članka na primjeren način objaviti.*
3) *Kada se snimke iz stavka 1. ovoga članka ne koriste u postupcima koji se vode sukladno odredbama posebnih propisa, policija će te snimke uništiti u roku od 90 dana od dana njihovoga nastanka."*

Zagovornici građanskih prava i slobode građana, policijski eksperti i stručnjaci koji su proučavali ovo pitanje uglavnom se slažu da građani moraju znati da ih se snima (Mateescu, Rosenblat, Boyd 2015).

Primarna pitanja vezana za upotrebu i implementaciju kamera (Paddock, 2013; Long, 2013) su sljedeća:

- Tko i što treba biti snimljeno?
- Kada policijski službenici započinju snimati?
- Kada policijski službenici prestaju snimati?
- Postoje li neka izuzeća od snimanja?
- Kako će snimka biti pohranjena?
- Tko ima pristup snimci?
- Kada i kako će snimka biti puštena u javnost?
- Koja pitanja vezana s privatnošću su dio ove tematike?.

Stoga je u odnosu na primarna pitanja tijekom projekta provedena obuka policijskih službenika o tehničkim karekteristikama i rukovanju kamerama, a nakon toga propisane su i procedure koje se odnose na:

- smještaj i pristup e-Kiosku i kamerama
- način zaduživanja kamera
- proceduru korištenja kamera i snimanja policijskog postupanja
- postupanje sa snimljenim materijalom te
- praćenje/nadzor korištenja kamera i edukaciju.

S tim u vezi valja istaknuti kako je smještaj cijelog sustava za upravljanje kamerama određen tako da je moguć kontinuiran i kvalitetan nadzor nad korištenjem te da su u vezi s korištenjem definirane različite razine ovlasti (korištenje, pregledavanje snimki, presnimavanje, uređivanje i drugo) koje su dodijeljene policijskim službenicima ovisno o njihovim radnim mjestima. Posebno je važno osvrnuti se na propisane obveze snimanja te je određeno da su policijski službenici dužni snimati svoje postupanje:

- kada je to naloženo radnim nalogom ili planom posebnog postupanja
- kad se primjenjuju ili se očekuje primjena sredstava prisile
- kada se osobu uhićuje, privodi ili dovodi ili se očekuje takvo postupanje
- kod postupanja koja mogu biti incidentna (s elementima nasilja, u kojima sudjeluje skupina građana itd.)
- kažnjive radnje koje se čine prema policijskom službeniku
- dolazak na mjesto događaja koje treba osigurati
- događaji kod kojih se može očekivati da će uslijediti pritužba građana na postupanje policijskog službenika
- u situacijama kada, po procjeni policijskog službenika, snimljeni materijal može poslužiti kao dokaz u kriminalističkom istraživanju.

Uputom o korištenju kamera određeno je također da snimanje ne smije trajati duže od vremena potrebnog da se ostvari svrha snimanja i da se sve snimke koje su označene kao "incidentni događaj" automatski prebacuju na server i čuvaju u skladu s posebnim propisima, a sve ostale nakon proteka roka od 90 dana od dana snimanja automatski se brišu. Radi lakšeg praćenja, pregledavanja i korištenja snimljenog materijala predmetni materijal se kategorizira te se posebno označavaju snimke koje se odnose na incidentne događaje koje mogu poslužiti kao dokaz u postupku ili snimke koje treba čuvati duže od 90 dana. Uspostavljen je protokol po kojem se osigurava pristup snimljenom materijalu koji ima vrijednost za edukaciju, a posebno situacijski trening, kao što je i preporuka Nacionalnog centra za provedbu politika u provedbi zakona, Međunarodne organizacije šefova policija (IACP *National Law Enforcement Policy Center*, 2005).

Na temelju analize iskustava s primjenom policijskih kamera nošenih na tijelu u ovom projektu, tijekom tri mjeseca (rujan-prosinac 2015.), utvrđeno je kako su policijski službenici snimili 22 283 postupanja pri čemu je 131 snimka (0,6%) okarakterizirana incidentnom.

Policijski službenici kamere su najčešće koristili tijekom službe ophodnje u situacijama koje su se odnosile na:

- narušavanje javnog reda i mira (javna okupljanja, osiguranja nogometnih utakmica)
- kontrole u cestovnom prometu
- upotrebe sredstava prisile
- utvrđivanje identiteta osoba
- uhićenja, dovođenja i privođenja te
- pregleda i pretraga osoba, doma i drugih prostorija.

Prema mišljenju policajaca i njihovih rukovoditelja u korištenju kamera prepoznaje se niz prednosti, ali i određeni nedostaci.

Prednosti koje su prepoznate:

- Građani su obzirniji te se kulturnije ponašaju prema policijskim službenicima.
- Policijski službenici iskazuju veću profesionalnost i kulturu u svom postupanju.
- Snimke pružaju zaštitu policijskim službenicima od neosnovanih i lažnih pritužbi na njihovo postupanje.
- Olakšano je postupanje po pritužbama i predstavkama građana te donošenje ocjene o utemeljenosti takvih predstavki i pritužbi.
- Pomoć u ocjeni zakonitosti postupanja policijskih službenika u primjeni policijski ovlasti.
- Mogućnost korištenja snimki kao dokaza u prekršajnim i kaznenim postupcima.
- Edukacija policijskih službenika kroz prikazivanje dobrih i loših primjera iz prakse, osobito prilikom primjena policijskih ovlasti.

Nedostaci korištenja kamera su sljedeći:

- Mogućnost izazivanja konflikta samo činjenicom da se određeni događaj ili postupanje snima.
- Policijski službenici mogu biti više usmjereni na činjenicu da se postupanje snima nego li na postupanje, odnosno odvraćanje pažnje od postupanja.
- Subjektivan osjećaj nesigurnosti u postupanju svakog policijskog službenika.
- Najčešće su isticani nedostaci tehničke prirode: nemogućnost fiksiranja kamere na odori, a time i centriranja snimke; kratko trajanje baterije; slaba kvaliteta i vidljivost snimke tijekom snimanja noću.

Naposljetku, izuzetno je bilo bitno utvrditi i što policijski službenici, ali i građani misle o novoj tehnologiji:

- Većina policijskih službenika smatra kamere korisnim te kako ih one ne ometaju u svakodnevnom radu.
- Mlađi službenici bolje prihvaćaju kamere kao dodatnu opremu, češće i vještije ih koriste.
- Većina policijskih službenika nije se susrela s tehničkim poteškoćama prilikom korištenja kamera.
- Građani na korištenje kamera gledaju uglavnom pozitivno, a pozitivne reakcije građana zabilježene su osobito kod mlađe populacije.

Na temelju početnih rezultata te s obzirom na pozitivne stavove postignut je široki konsenzus o nastavku projekta uz postojanje svijesti o još brojnim neriješenim pitanjima kvalitetne implementacije i stvarnog utjecaja primjene kamera u svakodnevnom policijskom

radu na policijske službenike, građane te njihovu interakciju. Upravo iz tog razloga pitanje istraživačkih pristupa, nacrta istraživanja te korištenja metodologije istraživanja dolazi u fokus interesa ne samo istraživača već i policijskih praktičara, a posebno donositelja odluka i kreatora javnih politika u području sigurnosti.

4. ISTRAŽIVAČKI PRISTUPI UTJECAJA KAMERA NOŠENIH NA TIJELU

Ubrzana primjena ove vrste tehnologije, bez prethodno prikupljenih visokokvalitetnih informacija o učincima, može dovesti do očekivanih, ali i neočekivanih posljedica koje u konačnici mogu utjecati negativno na rad policije, ali i građane. Potreba za istraživanjima u ovom području je od velike važnost zato što će uvođenje kamera vjerojatno imati snažni utjecaj na interakciju policije i građana, policijsko rukovodstvo i proračun, sigurnost, privatnost ljudi, prijavljivanje od strane građana i njihovu suradnju s policijom te sudsku praksu (Lum i sur., 2015). Znanstvenici mogu pomoći da se istraživanjima i analizama omogući građanima koji imaju javni interes bolje razumijevanje implementacije i uporabe novih policijskih tehnologija, te kako bi se osiguralo da se učinci nošenja kamera na tijelu i drugih tehnologija za nadzor ostvaruju u korist građana (Mateescu, Rosenblat, Boyd, 2015).

U tom kontekstu postaje bitno koja se istraživačka pitanja i vrste istraživanja trebaju provesti i zašto? U svakom slučju, u ovom području potrebna su primijenjena istraživanja kojima se traže znanstveno utemeljeni odgovori na konkretne probleme iz prakse, odnosno razvojna istraživanja kao dio primijenjenih istraživanja (vidi detaljnije u Mejovšek, 2008; Coghlan i Brydon-Miller, 2014), usmjerenih na praćenje i evaluaciju uvođenja i razvoja novih postupaka i tehnologija u policijsku praksu. Na temelju rezultata istraživanja mogu se razvijati pristupi koji su utemeljeni na dokazima, što je danas jedan od ključnih kriterija vrednovanja i razlikovanja učinkovitih projekata ili metoda rada od onih koje ne daju pozitivne i očekivane rezultate.

Jednako važno, kao i stvaranje dokaza o primjeni kamera, jest da istraživanja budu u skladu s potrebama i problemima koji se pojavljuju u interakciji policije i građana te da predvide buduće načine korištenja kamera i neke njihove nedostatke. Bit će potrebna različita istraživanja: ona koja će pružiti dokaze o učincima kamera i evaluacijska istraživanja tijeka implementacije i rezultata primjene. Cilj provedbe/implementacije je uspješno instalirati i testirati tehnologiju, potom trenirati osoblje da koriste tehnologiju uspješno u svojim svakodnevnim aktivnostima (Stolting i Kurz, 2005). Zato su potrebna istraživanja kako bismo bili sigurni da ovaj proces ne ide u krivom smjeru.

Nikako se ne smiju zanemariti pravne analize i etička pitanja vezana za privatnost, uređenje i objavu snimki te pohrane tih podataka. Naposljetku, potrebna su i empirijska istraživanja vezana za utjecaj kamera na sudske, kaznene ili prekršajne postupke, interne policijske istrage te postupke vezane uz provjere po predstavkama i pritužbama građana u vezi s radom policije. U konačnici nužne su i *cost benefit* analize (Farrell, Bowers i Johnson, 2005) s obzirom na to da je uvođenje novih tehnologija u rad policije uvijek povezano s znatnim financijskim ulaganjima.

Dakle, važna tema jest "Koja istraživačka pitanja trebaju biti istražena?" i u tom smislu postavljena pitanja trebaju predstavljati znanstveni problem koji je moguće empirijski provjeriti. Neki od važnih znanstvenih problema jesu:

- utjecaj policijskih kamera na ponašanje policijskog službenika
- stavovi policijskih službenika o kamerama
- utjecaj kamera na ponašanje građana
- stavovi građana i zajednice o kamerama
- utjecaj kamera na policijsku učinkovitost, osobnu i organizacijsku
- utjecaj kamera na kriminalistička istraživanja te unutarnje istrage
- utjecaj kamera na policijsku organizaciju, zadovoljstvo poslom i organizacijsku privrženost
- istraživanje učestalosti korištenja kamera i čimbenika koji su s time povezani te
- utjecaj kamera na policijski integritet i legitimitet.

Upravo se pitanja policijskog integriteta (Klockars i sur., 2000) i policijskog legitimiteta (Tyler, 2004) danas nameću kao ključna za svaku modernu, demokratsku policijsku organizaciju, orijentiranu prema potrebama građana i zajednica.

Buduće istraživačke studije kamera nošenih na tijelu trebale bi imati složeni kvazieksperimentalni nacrt, dakle zadovoljiti stroge kriterije, uključivati i eksperimentalne i kontrolne skupine ispitanika te mjerenje (istraživanje) provedeno u više vremenskih točaka, pod pretpostavkom odabira slučajnog reprezentativnog uzorka ispitanika (Vogt, Gardner i Haeffele, 2012). U tom smislu istraživanja provedena na manjim prigodnim uzorcima ne bi dala dovoljno relevantne dokaze na kojima bi se moglo uvoditi novu tehnologiju u policijsku praksu. S obzirom na činjenicu da je posrijedi primjena nove tehnologije u radu policije, pa samim time i promjena taktike postupanja, u istraživanju je uz eksperimentalnu skupinu ispitanika (oni koji koriste kamere) potrebna i kontrolna skupina (oni koji kamere ne koriste), kako bismo na temelju razlika njihovih rezultata mogli zaključivati o stvarnom utjecaju kamera na policijski rad. Posebnu pažnju treba posvetiti i uzorkovanju jer prema karakteristikama eksperimentalna i kontrolna skupina moraju odgovarati jedna drugoj, moraju biti uparene prema svojim svojstvima i karakteristikama zajednica kojima služe, stoga je najbolje da se svakom ispitaniku u eksperimentalnoj skupini odredi njegov par (npr. policijski službenik sličnih karakteristika – dob, spol, stručna sprema, staž u policiji, sklonost disciplinskim prijestupima, rezultati rada i drugo) u kontrolnoj skupini. Time bi se smanjio utjecaj različitih ometajućih činitelja koji se, pored primjene kamera, mogu također reflektirati na rezultate istraživanja. Mjerenje u više vremenskih točaka (prije primjene kamera u radu policije i u određenim intervalima tijekom primjene) nužno je kako bismo mogli zaključivati o promjenama koje su se dogodile zbog uvođenja kamera te kako bismo mogli odgovoriti na pitanje "Imaju li kamere trajno pozitivan utjecaj na policijsku praksu, ili se pozitivni efekti s vremenom smanjuju?". Naime, nije nepoznato da nove taktike i metode s vremenom mogu izgubiti pozitivni utjecaj kojeg su u početku imale.

Osim podataka koje je moguće prikupiti anketiranjem građana i policajaca, buduća istraživanja trebaju koristiti i podatke koje redovito prikuplja policija (npr. prigovori na rad policije, izvješća o uporabi sile, pokazatelji o rezultatima rada i drugo) i materijale snimljene kamerama te sadržaje prikupljene intervjuiranjem policijskih rukovoditelja i ključnih ljudi u zajednici. Kada su u pitanju podaci koje policija generira kroz svoj redovni rad, treba se fokusirati na pritužbe građana (primjerice, broj pritužbi, narav i težina pritužbi, ishod, uključujući i potencijalne disciplinske mjere), izvješća o uporabi sredstava prisile (npr. broj slučajeva uporabe sredstava prisile, narav i ozbiljnost slučajeva uporabe sredstava prisile), uključujući i opravdanu i neopravdanu uporabu sredstava prisile, statističke podatke o kaznenim djelima i prekršajima počinjenim na štetu policijskih službenika (npr. broj, težina, rezultati), disciplinske podatke o policijskim službenicima (npr. broj stegovnih postupaka, težina optužbi, rezultati). Metodologija za analizu podataka treba biti i kvantitativna i kvalitativna.

Sve spomenuto smatra se nužnim, ako se želi izgraditi policijska praksa utemeljena na dokazima, generirati nova znanja za policiju i akademsku zajednicu, uz istovremeno nastojanje da se poboljša odnos policije i zajednice.

5. ZAKLJUČAK I PREPORUKE

Intenzivan razvoj novih tehnologija ima značajan utjecaj i na unapređenje policijske prakse. U vrijeme "pametnih telefona" koje građani nerijetko koriste i za snimanje policijskog postupanja, važno je i da policija ima službenu snimku određenog događaja, stoga se treba suočiti s mogućim pozitivnim, ali i negativnim aspektima korištenja policijskih kamera nošenih na tijelu.

Trenutno, dok smo još uvijek na početku u vezi s primjenom kamera, glavni problem njihovog korištenja jest nedostatak operativnih standarda te protokola i procedura. Već se i sada zna da kamere imaju i pozitivan i negativan aspekt, stoga policije koje razmišljaju o uvođenju policijskih kamera mogu imati koristi u mnogim različitim područjima, ali samo ako se implementacija provede valjano, po principu policijske prakse utemeljene na dokazima te ako je odgovarajuća politika i obuka policijskih službenika važna komponenta implementacije ove nove tehnologije.

Ako će se kamere koristiti, politika njihovog korištenja i procedure trebaju biti donesene prije implementacije. One se odnose na pravna pitanja koja su šira od zaštite privatnosti i ljudskih sloboda. Procedure bi trebale sadržavati odredbe kada se kamere koriste, odnosno kada bi trebale biti upaljene ili ugašene kako bi svi građani imali jednak tretman. Također, parametri za dobrovoljno, obvezno i zabranjeno korištenje kamere trebaju biti jasno postavljeni, a snimka kamere trebala bi se smatrati javnom snimkom.

Adekvatna obuka o politici korištenja, proceduri i opremi je prijeko potrebna. Obuka se treba odnositi ne samo na tehničko korištenje kamera, već i na proceduralnu pravdu, etička pitanja, pohranu, korištenje te uporabu snimljenog materijala. Upravo povezano s etičkim i pravnim pitanjima te s obzirom na nužnu transparentnost u policijskom postupanju, snimanje

treba biti ograničeno na policijske službenike u odori i "obojana" vozila kako bi građani znali što mogu očekivati te bi policijski službenici, kada je to moguće, trebali obavijestiti građane da snimaju intervenciju. Drugim riječima, to znači da se kamere nošene na tijelu ne bi smjele koristiti za prikriveno prikupljanje informacija. Policijski službenik jasno treba najaviti da se postupanje snima prilikom ulaska u dom osobe, osim u slučaju hitnih intervencija, a snimke se ne bi trebale pohranjivati duže od vremena koje je potrebno da se ostvari svrha zbog koje je snimka nastala. Snimke mogu biti korištene samo za interne i vanjske istrage nedopuštenog ponašanja te u slučajevima kada postoji osnovana sumnja da snimka sadrži dokaz kaznenog djela ili prekršaja. Pod određenim uvjetima snimke se mogu koristiti i kao edukativni materijal. Snimljene osobe trebale bi imati pristup snimci, moći je kopirati tijekom vremena njenog čuvanja, a snimke mogu biti objavljene javno uz pristanak snimljene strane ili bez pristanka ako su propisno uređene – zamagljeni dijelovi ili izmijenjeni glas.

Uza sva spomenuta pitanja policijski rukovoditelji trebaju u obzir uzeti i mnoga praktična strateška pitanja uključujući značajne financijske troškove uvođenja ovog sustava i pohranjivanja nastalih snimki, a o načinu korištenja snimljenog materijala potrebno je postići dogovor i s drugim dionicima, prije svega, kaznenim pravosuđem.

Uvođenje kamera u svakodnevni policijski rad treba graditi na konceptu prakse utemeljene na dokazima zbog čega je potrebno blisko surađivati s istraživačima te razviti striktan plan evaluacije, implementacije i učinka uvođenja ove tehnologije. Ne smije se zaboraviti da je sustav kamera veliki potencijal za policijsku obuku, kako u akademskom smislu, tako i u smislu procjene i evaluacije policijskih procedura.

Jedna od mogućih posljedica nedosljednosti u implementaciji nove tehnologije s kojima bi se policijske organizacije mogle susresti jest neprihvaćanje kamera od strane policijskih službenika jer, ako policijski službenici smatraju kako se kamere koriste isključivo sa svrhom nadzora njihova ponašanja, mogli bi pružiti otpor spram njihova korištenja. Međutim, velika većina policajaca je posvećena svom poslu i sposobni su profesionalci koji služe svojoj zajednici na častan način, stoga na kamere treba gledati kao na sredstvo da se takav rad bolje dokumentira i vrednuje. Izražena zabrinutost zbog narušavanja odnosa s javnošću ne bi nas trebala pokolebati.

LITERATURA

Bayley, D.H. (2002). Law enforcement and the rule of law: Is there a tradeoff? *Criminology and Public Policy.* Vol. 2, No. 1:133-154.

Blitz, M. J. (2015). *Police Body-Worn Cameras: Evidentiary Benefits and Privacy Threats*. Washingon, DC: American Constitution Society.

Borovec, K. (2013). *Strategija policije u zajednici i njezin utjecaj na strah od kriminala, percepciju kriminaliteta i javnog nereda u Hrvatskoj*. Doktorski rad. Sveučilište u Zagrebu, Edukacijsko rehabilitacijski fakultet.

Brown, B., Benedict, W.,R. (2002). Perceptions of the Police Past findings, metodological issues, conceptual issues and policy implication. *An International Journal of Police Strategies & Managment 25/3,* <http://www.emeraldinsight.com/1363-951X.htrn>. Pristupljeno 13. 1. 2011.

Coghlan, D., Brydon-Miller, M. (2014). *The Sage Encyclopedia of Action Research*. Thousand Oaks, CA: Sage.
Dean, D. (1980). Citizen ratings of the police: The difference contact makes. *Law and Policy Quarterly.* Vol. 2, No. 4:445-471.
Elliott,J. (2015). *Body Worn Cameras.* A Step Toward Trust and Legitimacy for campus Police. University Honors Theses. Paper 145.
Farrell, G., Bowers, K. J. and Johnson, S. D. (2005). *Cost benefit analysis for crime science: making cost-benefit analysis useful through a portfolio of outcomes.* U: Tilley and Smith (ur.). Crime Science: New Approaches to Preventing and Detecting Crime. Willan Press.
Hak, J. W. (2004). *Forensic Video Analysis and the Law.* Effective Use of Video in Law Enforcement for Managers and Prosecutors. Pristupljeno 2. 2. 2016. na http://ric-zai-inc.com/Publications/cops-w0404-pub.pdf
Harris, D. A. (2010). Picture This: Body Worn Video Devices ('Head Cams') as Tools for Ensuring Fourth Amendment Compliance by Police. *Legal Studies Research Paper Series*. Pittsburgh: University of Pittsburgh School of Law.
Hinds, L. (2009). Public satisfaction with police: The influence of general attitudes and police-citizen encounters. *International Journal of Police Science & Management* 11/1: 54 - 66.
IACP National Law Enforcement Policy Center (2005). *Mobile Video Recording Equipment.* Virginia, Aleksandria: International Association of Chifes of Police.
James, N. (2014). Can Body Worn Cameras Serve as a Deterrent to Police Misconduct? Pristupljeno 7. 2. 2016. na https://www.fas.org/sgp/crs/misc/IN10142.pdf
Klockars, C. B., Kutnjak Ivkovich, S., Harver, W. E., Haberfeld, M.R. (2000). *The Measurement of Police Integrity.* US Department of Justice, Office of Justice Programs, National Institute of Justice.
Kovčo Vukadin, I., Borovec, K., Ljubin Golub, T. (2013). Policing in Croatia: The Main Challenges on the Path to Democratic Policing. U: Meško, G., Fielda, C., B., Lobnikar, B., Sotlar, A. (ur.), *Handbook on Policing in Central and Eastern Europe*. New York, Heidelberg, Dordrecht, London: Springer (31-57).
Long, C. (2013). NYPD ordered to start using officer-worn cameras, *THE ASSOCIATED PRESS.* Pristupljeno 7. 2. 2016. na http://www.policeone.com/ police-products/body-cameras/articles/6386513-NYPD-ordered-to-start-using-officer-worncameras/.
Lorraine, M., Antrobus, E., Bennett, S., Tyler, T.R. (2013). Shaping Citizen Perceptions of Police Legitimacy: A Randomized Field Trial of Procedural Justice. *Criminology* 51, no. 1: 33–63.
Lum, C., Koper, C. S., Merola, L.M., Scherer, A., Reioux, A. (2015). *Existing and Ongoing Body Worn Camera Research: Knowledge gaps and opportunities*. Fairfax. VA: Center for Evidence-Based Crime Policy, George Mason University.
Maghan, J., O'Reilly, G. W. and Ho Shon, P. C. (2002). Technology, policing and implications of in-car video. *Police Quarterly.* Vol. 5, No. 1:25-42.
Mateescu, A., Rosenblat A., Boyd, D. (2015). *Police Body-Worn Cameras.* Data & Society Research Institute, Working Paper2.
Maxfield, M. G. and Andresen, W. C. (2001). *Evaluation of New Jersey state police in-car mobile video recording system.* Trenton, NJ: Office of the Attorney General, Department of Law and Public Safety.
Mejovšek, M. (2008). *Metode znanstvenog istraživanja u društvenim i humanističkim znanostima.* Jastrebarsko: Naklada Slap.
Miller, L, Toliver, J. (2014). *Implemeting a Body-Worn Camera Program: Recommendations and Lessons Learned.* Washnington, DC: Office of Community Oriented Policing Services.

National Research Council. (2004). *Fairness and effectiveness in policing: The evidence.* Washington, D.C: National Academies Press.
Paddock, B. (2013). NYPD cops in stop-and - friskiest precincts to wear body cams after judge's ruling, *NEW YORK DAILY NEWS*, pristupljeno 7. 2. 2016. na http://www.nydailynews.com/new-york/nypd-cops-wear-body- cams.
Ramirez, E. P. (2014). *A Report on Body Worn Cameras.* Los Angeles: Manning & Kass.
Rosenbaum, D. P., Schuck, A. M., Costello, S. K., Hawkins, D. F. and Ring, M. K. (2005). Attitudes toward the police: The effects of direct and vicarious experience. *Police Quarterly*, Vol. 8, No. 3:343-365.
Rosenblatt, D. N., Cromartine, E. C., Firman, J. (2004). *The Impact of Video Evidence on Modern Policing. Research and Best Practices from the IACP study on In-Car Cameras.* Washington D.C. U. S. Department of Justice, Office of Community Oriented Policing Services.
Schafer, A., S., Huebner, B., M., Bynum, T., S. (2003). Citizen Perceptions of Police Services: Race, Neighborhood Context, and Community Policing. *Police Quarterly* 6/4: 440-468.
Skogan, W., G. (2006). „Asymetry in The Impact of Encounters with Police". *Policing and society* 16/ 2: 99-126.
Sousa, W. H., Miethe, T. D., Sakiyama, M. (2015). Body Worn Cameras on Police: Results from a National Survey of Public Attitudes. *Research in Brief.* Center for Crime and Justice Policy.
Stanley, J. (2013). Police Body-Mounted Cameras: With Right Policies in Place, a Win for All. Pristupljeno 7. 2. 2016. na https://www.aclu.org/files/assets/police_body-mounted_cameras.pdf .
Stolting, S., Kurz, D. (2005). *Acquisition of New Technology, A Guide for Newly Appointed Police Leaders*. Virginia, Aleksandria: International Association of Chifes of Police.
Tyler, T. R., Jeffrey F. (2008). Legitimacy and cooperation: Why do people help the police fight crime in their communities? *Ohio State Journal of Criminal Law*: 231-275.
Tylor, T. R. (2004). Enhancing Police Legitimacy. *The Annals oft he American Academy of Political and Social Science,* vol. 593, no.1:84-99.
U. S. Department of Justice (2012). A Primer on Body-worn cameras for Law Enforcement. National Institute of Justice, pristupljeno 7. 2. 2016. na https://www.justnet.org/pdf/00-Body-Worn-Cameras-508.pdf
Vogt, W. P., Gardner, D. C., Haeffele, L. M. (2012). *When to Use What Research Design.* New York: Guilford.
Weitzer, R., Tuch, S., A. (2005). Determinants of Public Satisfaction with the Police, *Police Quarterly* 8/3: 279-296.
White, M. D. (2014). *Police Officer Body-Worn Cameras: Assessing the Evidence*. Washington, DC: Office of Community Oriented Policing Services.
Zakon o policijskim poslovima i ovlastima. Narodne novine 76/09. i 92/14.

Krunoslav Borovec

Iva Balgač

THE INTRODUCTION OF POLICE CAMERAS IN THE WORK OF POLICE PATROLS - ISSUES RELATED TO SUCCESSFUL IMPLEMENTATION AND EXACT ASSESSMENT OF THE IMPACT ON POLICE WORK

Summary

The development of society in general, including the development of new technologies, affects the police service, its tactics and work methods on a daily basis. One of the latest technological innovations that is being increasingly used in the work of police organizations around the world are Body Worn Cameras (BWCs) that police officers use in the activities they conduct every day. The Croatian police started to use BWCs at the end of 2015, in the five largest police departments in the country, i.e. in the cities of Zagreb, Split, Osijek, Rijeka and Pula. Based on the first experiences of different police departments which have shown that the use of cameras in police work can have both positive and negative impacts, it was concluded that it is not a simple matter, it doesn't include only the technical aspects of the use of new equipment, but a whole range of important topics related to the successful implementation of BWCs in police work and the relevant, scientifically based assessment of their impact on police practices. Therefore, this paper presents a discussion of the important issues of implementation, such as: why use cameras?, how to define procedures and tactics of conduct?, how to use video footage?, the question of training tutorials to use the camera, but also legal issues such as the protection of human rights, invasion of privacy and more. In addition, this paper provides a discussion of issues of evaluation, and indicates the key areas that should be investigated in connection with the use of police cameras. Based on past and ongoing research, the key research questions are as follows: the impact of cameras on the interaction between police and citizens, the impact of cameras on the behavior of police officers, their views on the use of cameras in their daily work, the influence of cameras on the behavior of citizens and their attitudes towards this matter, the impact of cameras to support criminal investigation of crimes or offenses, the impact of cameras on corruption, police integrity and legitimacy, i.e. if cameras increase the security of police officers and reduce the number of complaints related to their work.

Key words: *Body Worn Cameras (BWCs), Implementation, Protocol of Use, Impact of Cameras, Research Aspects.*

STRUČNI RAD

Zlatko Kovač[175]
Nikola Protrka[176]

RAČUNALNA ANALIZA LJUDSKOG GLASA I GOVORA

Sažetak

U članku se govori o analizi ljudskog glasa (govora) baziranoj na dugotrajnom prosječnom spektru govora (Long-Term Average Spectrum – LTAS), sa aspekta forenzičke analize potrebne kod spornog i nespornog uzorka računalne forenzike odnosno vještačenja. Korištena su dva računalna programa, koji rade u sprezi – WaveSurfer i Catalina Forensic Audio Toolbox. Pri tom prvi program analizira audio zapis i rezultate sprema u obliku tekstualnih datoteka, a drugi program učitava te datoteke, statistički ih obrađuje i grafički prikazuje rezultate kroz niz dijagrama. Ukratko su opisana oba računalna programa, sa svojim mogućnostima i radnim prozorima. Kroz analizu jednog glasa (vokala a) prikazani su osnovni parametri ljudskog glasa (osnovna frekvencija, formanti i dugotrajni prosječni spektar). Zatim je provedena analiza dvaju različitih glasova (govor dviju ženskih osoba sličnih tonalnih karakteristika) i rezultati su komparirani kroz prikaz odnosnih dijagrama. Na kraju je provedena analiza glasa istog govornika, gdje mu je analizirana jedna i druga polovina tijeka govornog zapisa. Relevantni dijagrami su uspoređeni, kako bi se utvrdilo podudaranje krivulja na grafikonima ili utvrdilo moguće odstupanje (kao mjera variabiliteta u glasu i govoru iste osobe). Za navedene analize i komparacije, autori su postavili audio datoteke na internet adresu koje svaki zainteresirani čitatelj može preuzeti i naknadno analizirati.

Ključne riječi: *vještačenje, govor, glas, analiza, LTAS.*

1. UVOD

Ovim člankom prikazan je segment računalne audioforenzike ljudskog glasa i govora, baziran na dugotrajnom prosječnom spektru govora (LTAS). Prikazana dva softverska alata, *WaveSurfer* nastao na Kraljevskom institutu u Švedskoj[177] i *Catalina Forensic Audio Toolbox*[178] proizvođača Forensic Media Services., Ltd. iz Denvera, SAD, mogu koristiti audioekspertu – vještaku, u sprezi s mnoštvom drugih tehnologija, tehnika i koncepcija. Pošto su ovdje korišteni nekomercijalni programi, slobodno dostupni na internetu, korisno je ukazati na još jedan sličan program, također dostupan na internetu, a po namjeni sličan navedenima

[175] Zlatko Kovač, voditelj programa specijalizacije, e-mail: zkovac@mup.hr
[176] Nikola Protrka, predavač na Visokoj policijskoj školi u Zagrebu, e-mail: nprotrka@fkz.hr
[177] Royal Institute of Technology (KTH), Department of Speech, Music and Hearing, Stockholm, http://www.speech.kth.se/wavesurfer/ - datum pristupa 19. 2. 2016.
[178] Forensic Media Services., Ltd. Denver, CO, USA, http://www.forensicav.ro/software.htm - datum pristupa 19. 2. 2016.

pod nazivom *Praat*[179], program širokih mogućnosti u području govorne analize i sinteze, nastao na Sveučilištu u Amsterdamu.

U smislu šireg razmatranja problematike forenzike govora, stručnjaci se danas koriste i slušnom metodom i spektrometrijskom metodom, a postoje i zagovornici potpune automatizacije analize govora, gdje bi računalo i softver davali odgovore oko identiteta glasa i govora.

Također se mnogo koriste rezultati iz druge, paralelne grane istraživanja glasa (engl. *Speaker Recognition* ili *Speaker Verification*) koja se razvijala za komercijalne svrhe – identifikaciju i autorizaciju osoba na temelju njihova glasa kao lozinke za ulaze u objekte (npr. banke, trezore, vojne objekte itd.) ili pristup različitim računima u elektroničkim transakcijama. Budući da se u ovim automatiziranim sustavima radi o potpuno strojnom procesu identifikacije, rezultat se izračunava pomoću statističkih algoritama i izražava kroz vjerojatnost poklapanja određenih parametara ispitivanog glasa s parametrima referentnih glasova iz glasovne baze.

2. OPIS RAČUNALNIH PROGRAMA WAVESURFER I CATALINA FORENSIC AUDIO TOOLBOX

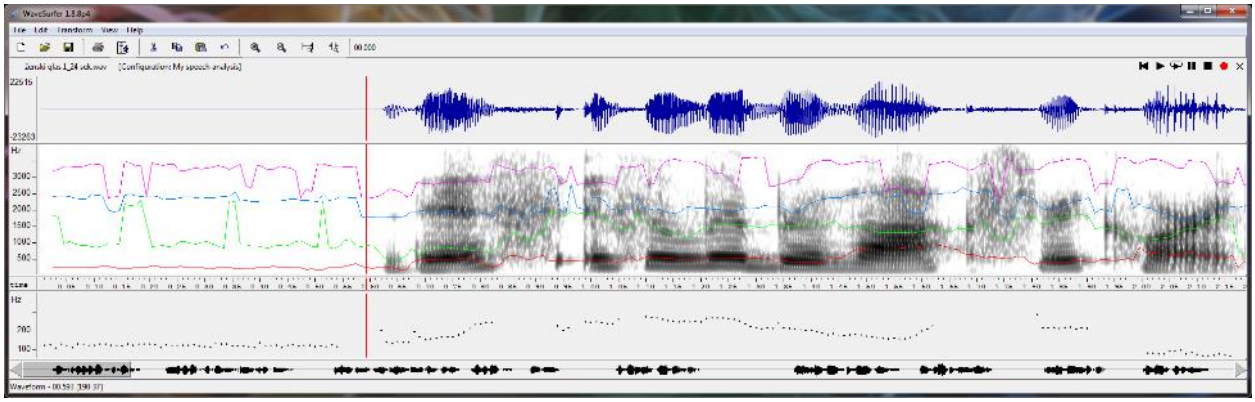
Metoda analize ljudskog glasa i govora temeljena na dugotrajnom prosječnom spektru govornog signala (engl. Long-Term Average Spectrum – dalje u tekstu LTAS) je postupak kojim se dobiva prosječna vrijednost uzastopnih trenutačnih spektralnih analiza, koje se izračunavaju duž čitavog audiozapisa koji se analizira. Svaka trenutačna spektralna slika, koja se dobiva diskretnom Fourierovom transformacijom, odraz je fonetske karakteristike zvuka u danom trenutku. LTAS sumira ova trenutačna zvučna stanja preko cijelog ispitnog uzorka. LTAS ovisi o zajedničkom utjecaju analiziranog govora, okolnog šuma, šuma elektroničkih uređaja i frekvencijskoj karakteristici prijenosnog lanca.

Za audioanalize danas postoji mnoštvo aplikacija, kako komercijalnih tako i slobodnih, dostupnih putem interneta. Važno je istaći da ovaj program svoje rezultate sprema u obliku tekstualnih datoteka. Ove datoteke učitava drugi program, *Catalina Forensic Audio Toolbox* (također slobodno dostupan na internetu), statistički ih obrađuje i rezultate prikazuje u obliku višestrukih dijagrama.

Audiozapis mora biti jednokanalni (mono), u *wav* zapisu i PCM formatu, uzorkovan frekvencijom 8 kHz, i rezolucije 16 bita. Ako je audiozapis u nekom drugom formatu, on se prije svega mora konvertirati u ovaj navedeni format. Ovo je potrebno zbog kompatibilnosti s *Catalina Forensic Audio Toolboxom,* koji će, u tom slučaju, najtočnije izvesti statističku obradu primljenih tekstualnih podataka izvezenih iz *WaveSurfera* i onda ih prikazati u obliku dijagrama. Nadalje, u svrhu kompatibilnosti ova dva programa, potrebno je prilagoditi i određene postavke u programu *WaveSurfer,* koje su navedene u *Catalina Forensic Audio Toolbox* korisničkom priručniku.

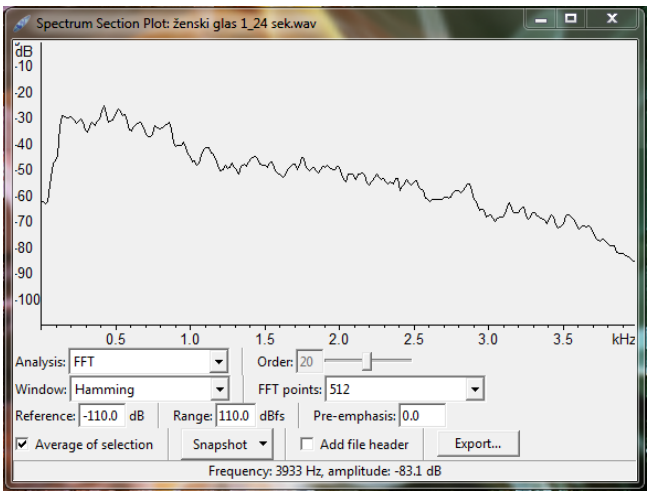
[179] University of Amsterdam, Phonetic Sciences, http://www.fon.hum.uva.nl/praat/ datum pristupa 19. 2. 2016.

WaveSurfer program ima više inicijalnih konfiguracija, koje se, na početku upotrebe ovog alata, odabiru ovisno o poslovima koje primarno treba obaviti, kao npr. razne vrste transkripcije audiozapisa, analiza spektrograma, analiza govora, vremenska analiza audiosignala ili konfiguracija za demonstraciju mogućnosti aplikacije. Moguće je, također, postaviti razne parametre programa po svojoj volji i spremiti takve postavke kao svoju konfiguraciju za buduću uporabu. Na slici 1 prikazana je jedna od konfiguracija – za analizu govora (Speech analysis), s učitanim audiozapisom.



Slika 1: Radni prozor programa WaveSurfer

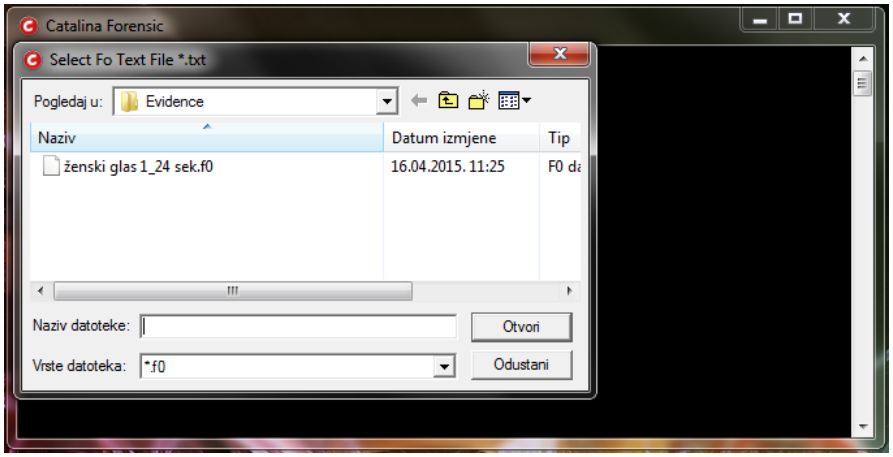
U gornjem redu radne površine aplikacije prikazan je početni dio analiziranog audiozapisa u vremenskoj domeni. Ukupni audiozapis prikazan je u donjem redu, a sivo označeni vremenski segment zapisa uvećan je u gornjem redu. Drugi red radne površine prikazuje spektrogram (u nijansama sivog) i četiri formanta prikazanih u boji (F1 – crveno, F2 – zeleno, F3 – plavo i F4 – ljubičasto). Treći red prikazuje osnovnu frekvenciju analiziranog glasa F0 (visina glasa, engl. *pitch*). Iz gore prikazanog prozora *WaveSurfera* može se otvoriti prozor za prikaz dugotrajnog prosječnog spektra – LTAS (slika 2).



Slika 2: WaveSurfer – LTAS

Kako je već navedeno, *WaveSurfer* stvara tekstualne datoteke rezultata svoje zvučne analize. Program kreira tri tekstualne datoteke oblika: *naziv_datoteke.fo* (za osnovnu frekvenciju

glasa), *naziv_datoteke.frm* (za formante F1, F2, F3 i F4) i *naziv_datoteke.lts* (za dugotrajni prosječni spektar, LTAS). Prve dvije datoteke formiraju se iz osnovnog prozora *WaveSurfera* prikazano na slici 1, a treća datoteka formira se iz LTAS prozora vidljivo na slici 2, pritiskom na izbornik *Export…* Sve tri datoteke treba spremiti u direktorij *Evidence* programa *Catalina Forensic Audio Toolbox* i nakon toga pokrenuti program *Catalina Forensic Audio Toolbox*. Program je, zapravo, statistički softver za grafički prikaz podataka danih u tabelarnom obliku u tekstualnim datotekama koje generira *WaveSurfer* (slika 3).



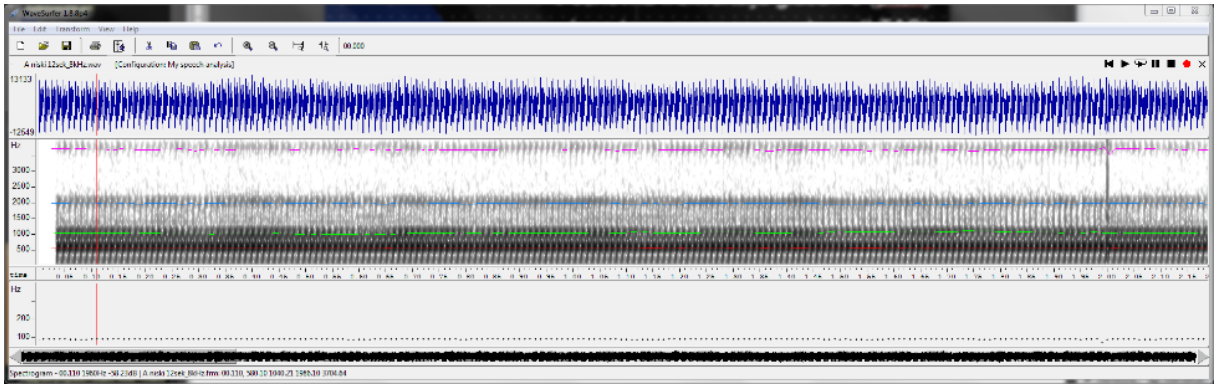
Slika 3: Početni prozor programa Catalina Forensic Audio Toolbox

Program, odmah po učitanju, traži da se učita prva od tri formirane datoteke s ekstenzijom *.fo*. Nakon što se unese *fo* datoteka, program dalje radi automatski – sam pronalazi i učitava ostale dvije datoteke istog imena ali ekstenzija *.frm* i *.lts* iz direktorija *Evidence*. Nakon obrade, *Catalina Forensic Audio Toolbox* stvara osam slika s dijagrama. Slike su u *.tif* formatu i spremaju se u direktorij *Plots* programa.

3. OSNOVNI PARAMETRI LJUDSKOG GLASA I GOVORA

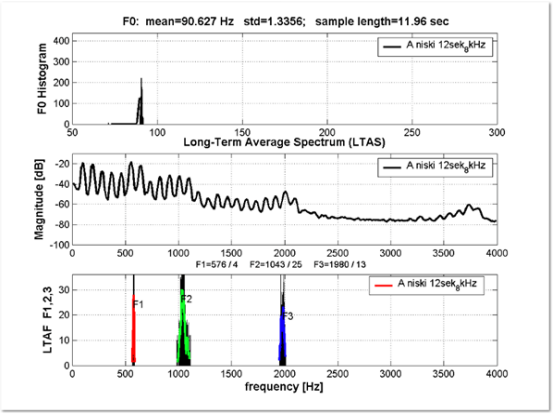
Uporaba dijagrama za analizu audiozapisa pojedinih govornika bit će prikazana u nastavku, a prije toga, prikazat će se osnovni parametri ljudskog glasa – osnovna frekvencija glasa F0 (visina glasa), frekvencije formanata F1-F4 i dugotrajni prosječni spektar LTAS kroz primjer analize vokala *a*. Vokal je izabran, zato što vokali nose energiju glasa i imaju jasno određenu osnovnu frekvenciju F0 (što je u stvari frekvencija titranja glasnica, bez utjecaja ostalog vokalnog trakta) i jasno određene formante F1, F2, F3, F4 (naglašena frekvencijska područja glasa, kao rezultat rezonantnih karakteristika vokalnog trakta).
Sve korištene zvučne datoteke iz ovog članka postavljene su na internetskoj adresi http://1drv.ms/1I3kHUS i slobodne su za preuzimanje sa *Cloud* sustava *Microsoft OneDrive*.
Audiodatoteka glasa *a - A niski 12sek_8kHz.wav* je trajanja 12 sekundi, jer za analizu dugotrajnog prosječnog spektra (LTAS) *Catalina Forensic Audio Toolbox* zahtijeva duljinu

audiozapisa veću od 10 sekundi. Nakon učitavanja zvučne datoteke *A niski 12sek_8kHz.wav*[180] u *WaveSurfer*, program daje rezultat prikazan na slici 4.



Slika 4: Rezultat analize audiozapisa vokala a

Iz donjeg dijela slike može se iščitati osnovna frekvencija F0 vokala *a* od približno 100 Hz. Sredina slike daje formante: F1 ≈ 500 Hz, F2 ≈ 1000 Hz, F3 ≈ 2000 Hz i F4 ≈ 3700 Hz. Formant F4 neće se uzimati u obzir jer *Catalina Forensic Audio Toolbox* uzima i obrađuje samo 3 formanta (F1, F2, i F3) što je u praksi najčešće dovoljno za analizu govora. Iz slike se vidi kako su osnovna frekvencija i formanti, u ovom slučaju, vremenski gotovo nepromjenjivi – ravne vodoravne linije duž vremenske osi. To, međutim, kako će se kasnije vidjeti, nije slučaj za govor. Prikazani rezultati samo su gruba orijentacija o vrijednosti parametara analiziranog glasa – točne vrijednosti dat će program *Catalina Forensic Audio Toolbox*.
Kako je prije rečeno, sada treba unutar *WaveSurfera*, formirati 3 tekstualne datoteke podataka (*niski 12sek_8kHz.fo, niski 12sek_8kHz.frm i niski 12sek_8kHz.lts*) koje će *Catalina Forensic Audio Toolbox* statistički obraditi i prikazati dijagramima. Detalji ovog postupka navedeni su u korisničkom priručniku i ovdje se neće pobliže objašnjavati. Formirane datoteke spremaju se u direktorij *Evidence* programa *Catalina Forensic Audio Toolbox*. Potom se aktivira program, učita se prva datoteka (*niski 12sek_8kHz.fo*) i dalje, nakon obrade, rezultati se u grafičkom obliku spremaju u direktorij *Plots* kao slike u .tif formatu – vidi sliku 5.



Slika 5: Dijagrami programa Catalina Forensic Audio Toolbox glasa a

[180] Internetska adresa Microsoft OneDrive http://1drv.ms/1I3kHUS (datoteka *A niski 12sek_8kHz.wav*), datum pristupa 19. 2. 2016.

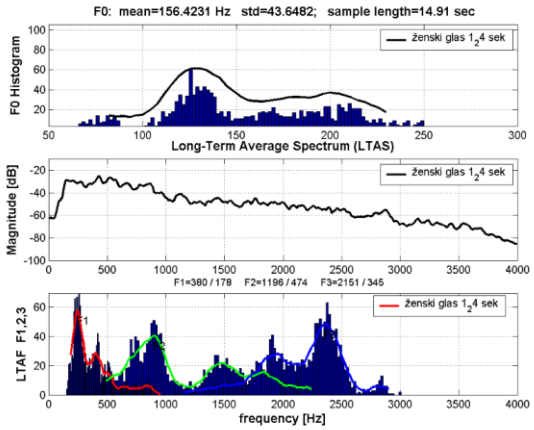
Ovdje su, sada, uz iscrtane grafove, točno ispisane srednja vrijednost osnovne frekvencije vokala *a* F0 u hercima s pripadajućom standardnom devijacijom (F0=90,627 Hz, std=1,3356) i srednje vrijednosti formanata F1, F2 i F3 u hercima s pripadajućim standardnim devijacijama (F1=576/4, F2=1043/25, F3=1980/13). Prikazan je i dijagram dugotrajnog prosječnog spektra (LTAS), na kojem se vide energetska nadvišenja na frekvencijama oko 500, 1000, 2000 i 3700 herca, što odgovara formantima.

Dijagrami sa slike 5 osnovni su rezultati audioanalize uz pomoć ova dva programa. U nastavku će biti pokazana šira primjena ovih alata u analizi dužeg govora ispitanika. Rezultantni dijagrami prikazat će se na osam slika koje su produkt statističke obrade ulaznih podataka uz pomoć programa *Catalina Forensic Audio Toolbox*.

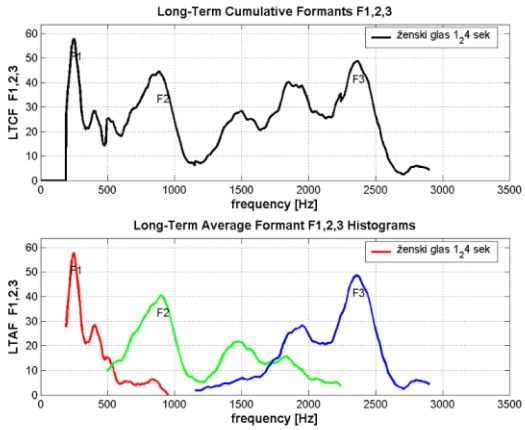
4. ANALIZA GLASA JEDNOG GOVORNIKA

Već je rečeno kako *Catalina Forensic Audio Toolbox* stvara ukupno osam slika s dijagramima. Pojašnjenja toga što se stvara na pojedinoj slici su sljedeća:
1. slika – 3 dijagrama; F0 histogram, LTAS i LTAF (Long-Term Average Formants) histogram formanata F1, F2 i F3
2. slika – 2 dijagrama; kumulativni histogram formanata i pojedinačni histogram formanata F1, F2 i F3
3. slika – ukupni formantni prostor F1-F2
4. slika – ukupni formantni prostor F2-F3
5. slika – formantni prostor F1-F2 vokala a, e, i, o (za engleski jezik)
6. slika – formantni prostor F2-F3 vokala a, e, i, o (za engleski jezik)
7. slika – 2 dijagrama; Long-Term Average Spectrum-Fast Fourier Transform (LTAS-FFT) dijagram i LTAS histogram izvedeni su programomom Catalina Forensic Audio Toolbox. LTAS-FFT dijagram identičan je dijagramu LTAS kojeg je iscrtao WaveSurfer.
8. slika – 3 dijagrama; LTAS-FFT, Long-Term Cumulative Formants F1, F2, F3 i Long-Term Average Formant F1, F2, F3 Histograms također su izvedeni programom Catalina Forensic Audio Toolbox i identični su dijagramima s podacima iz WaveSurfera.
Svi dijagrami bit će prikazani kao rezultat analize audiozapisa govora jedne ženske osobe – *ženski glas 1_24 sek.wav* i gore već navedenim slijedom.[181] Ovu datoteku ćemo u opisu slika imenovati Datoteka 1. Postupak rada s programima upravo je opisan, pa sada slijede samo rezultati – Catalina dijagrami prikazani na osam slika – od slike 6 do slike 13.

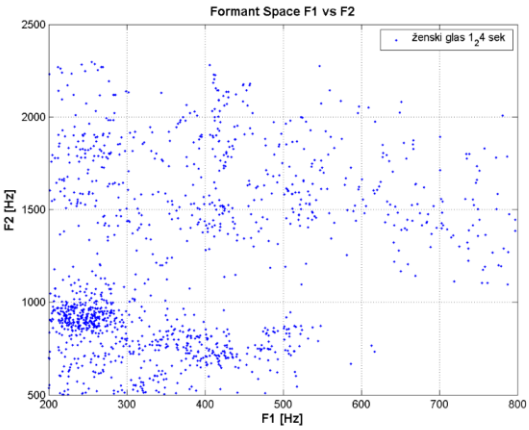
[181] Internetska adresa Microsoft OneDrive http://1drv.ms/1I3kHUS (datoteka *ženski glas 1_24 sek.wav*), Datoteka 1, datum pristupa 19. 2. 2016.



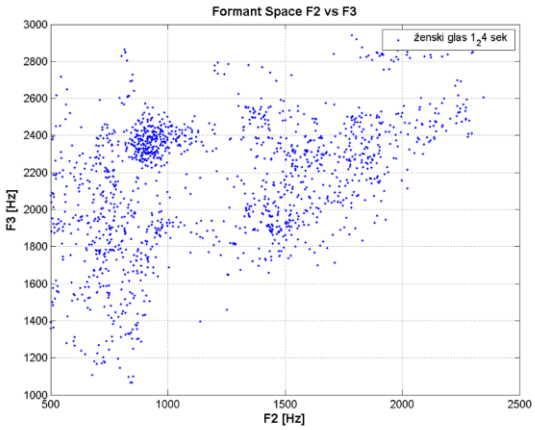
Slika 6: Datoteka 1 - dijagram 1



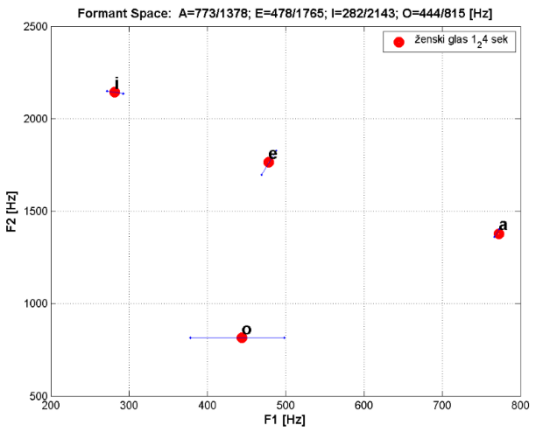
Slika 7: Datoteka 1 - dijagram 2



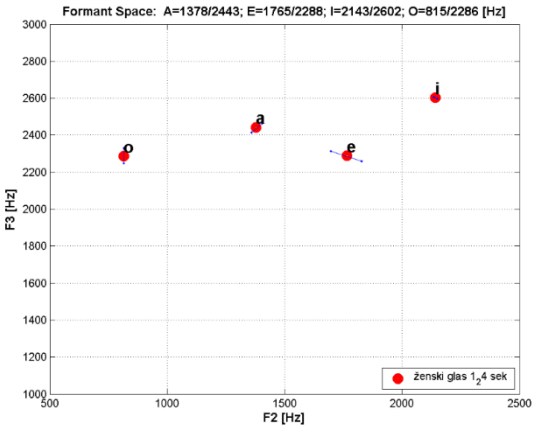
Slika 8: Datoteka 1 - dijagram 3



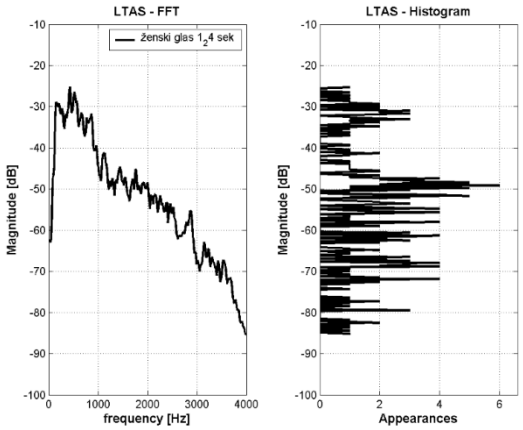
Slika 9: Datoteka 1 - dijagram 4



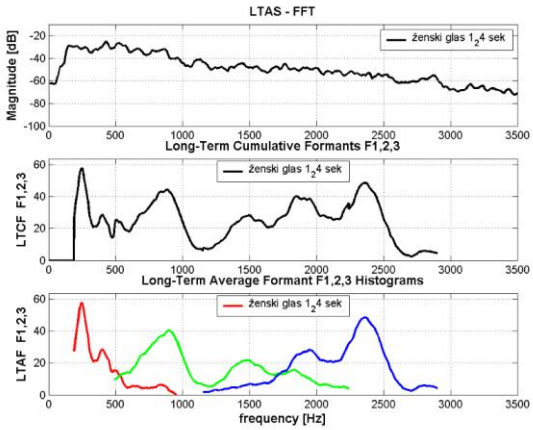
Slika 10: Datoteka 1 - dijagram 5



Slika 11: Datoteka 1 - dijagram 6



Slika 12: Datoteka 1 - dijagram 7



Slika 13: Datoteka 1 - dijagram 8

Komentari prikazanih dijagrama nam pojašnjavaju:
- Histogram LTAF na slici 7 – dolje jednak je onom na slici 6 – dolje, na kojem su prikazane samo vanjske konture histograma (bez ispuna ispod grafa).
- Histogram LTCF na slici 7 – gore grafički je zbroj pojedinačnih dijagrama F1, F2 i F3 sa donjeg grafa i čini jednu konturu (kumulativni ili zbrojeni formanti).
- Slike 8 i 9 prikazuju ukupni formantni prostor F1-F2 odnosno F2-F3.

Svaka točkica na dijagramu predstavlja jednu detektiranu frekvenciju formanata F1, F2 i F3 u kratkom vremenskom intervalu analize. Prozor analize pomiče se, zatim, na novi vremenski interval i tu se očitavaju formanti za sljedeću točkicu u grafu i tako dalje, do kraja audiozapisa.

Zanimljivo je uočiti vezu rezultata sa slike 8 i 9 i grafova na slici 7. Naime, najveća gustoća točkica na slici 8 je za formante F1 ≈ 250 Hz i F2 ≈ 900 Hz. Kad se, sada pogleda slika 7, vide se pikovi (najveći broj pojavljivanja) upravo na tim frekvencijama. Isto vrijedi i za sliku 9 – najveća gustoća točkica je za F2 ≈ 900 Hz i F3 ≈ 2300 Hz, što odgovara pikovima na slici 7.

- Slike 10 i 11 prikazuju položaj vokala *a, e, i, o* u formantnim prostorima F1-F2 i F2-F3.

Naime, statistički su određene granice frekvencija formanata u hercima, za pojedine vokale engleskog jezika. Vrijednosti su prikazane u tablici na slici 14 (*Catalina Forensic Audio Toolbox* User's Manual).

601	850	1100	1600	2200	2800	← vowel [a]
401	600	1500	2000	2100	2800	← vowel [e]
220	400	2000	2400	2400	2900	← vowel [i]
370	600	700	1200	2200	2600	← vowel [o]
↑	↑	↑	↑	↑	↑	
low	high	low	high	low	high	
limits		limits		limits		
for F1		for F2		for F3		

Slika 14: Frekvencije formanata vokala u engleskom jeziku

Vrijednosti sa slike 14 nalaze se u datoteci *formants.txt* direktorija Catalina, u kojem je instalirana aplikacija. Datoteka je promjenjiva i u nju se mogu upisati vrijednosti i za druge jezike ili vrijednosti za neka specifična istraživanja određenih skupina govornika – ispitanika. Na slikama 10 i 11 zatamnjeni kružići prikazuju prosječne vrijednosti formanata pojedinih vokala u cijelom audiozapisu, a u skladu s granicama iz tablice na slici 14. Male točkice oko kružića, povezane linijom, srednje su vrijednosti formanata određenog vokala, izračunate za prvu i za drugu polovicu trajanja ukupnog audiozapisa. Duljina linije ukazuje na varijabilnost vokala (a time i govora) iste osobe (ispitanika).

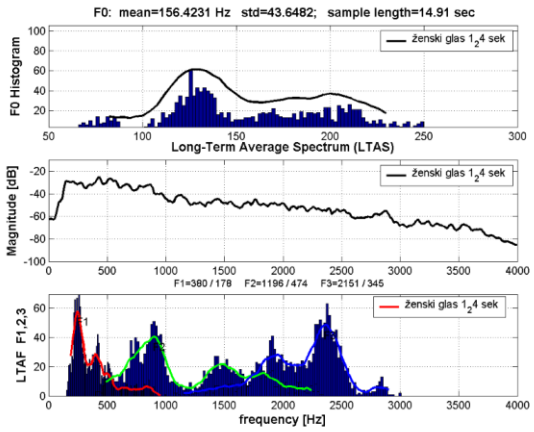
- Dijagrami na slikama 12 i 13 dobiveni su metodom brze Fourierove transformacije (FFT) unutar samog programa *Catalina Forensic Audio Toolbox*. Vidi se kako su ovi dijagrami identični onima izvedenim programom *WaveSurfer*.

LTAS histogram na slici 12 prikazuje relativnu učestalost pojavljivanja (Appearances) određene energije govora (analogno glasnoći govora) za pojedinu frekvenciju govornog spektra (lijevi dijagram na slici 12, LTAS – FFT).

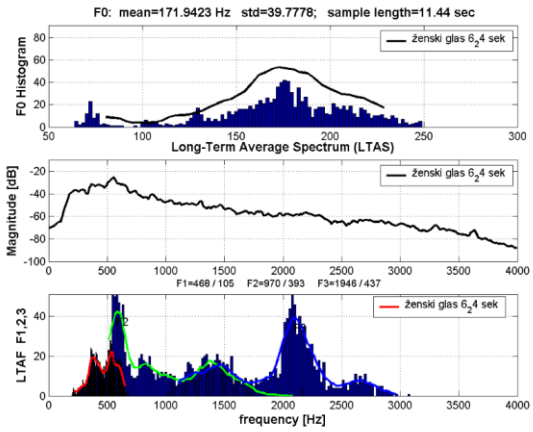
5. KOMPARACIJA GLASOVA DVOJE GOVORNIKA

Pravi smisao forenzike ljudskog glasa ili govora dolazi u postupcima komparacije rezultata dviju analiza, gdje se, jednostavnom vizualnom usporedbom grafova, može zaključiti radi li se o glasovima jedne osobe na obje snimke, ili se radi o glasovima različitih osoba. Za demonstraciju će se usporediti govor dviju ženskih osoba, ženski glas 1, na audiozapisu *ženski glas 1_24 sek.wav* i ženski glas 2, na audiozapisu *ženski glas 6_24 sek.wav*. Datoteku *ženski glas 6_24 sek.wav* u opisu slika ćemo imenovati kao Datoteka 2. [182]
Kako bi se komparacija, odnosno usporedba otežala, izabrani su slični ženski glasovi po boji, intenzitetu govora i govornoj dinamici (preporuča se poslušati navedene audiodatoteke radi slušne usporedbe). Rezultati za ženski glas 1 već su gore navedeni i objašnjeni, a za ženski glas 2 treba izvesti identični, već opisani postupak analize. Ponovno će se formirati osam slika s dijagramima za ženski glas 2 i ove će se slike međusobno usporediti. Rezultati su prikazani na slikama 15 – 22.

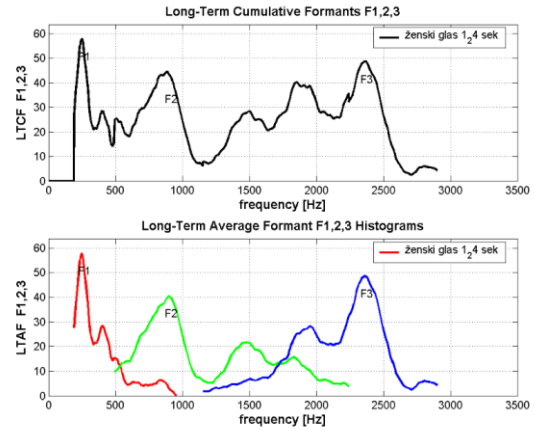
[182] Internetska adresa Microsoft OneDrive http://1drv.ms/1I3kHUS (datoteka *ženski glas 6_24 sek.wav*), Datoteka 2, datum pristupa 19. 2. 2016.



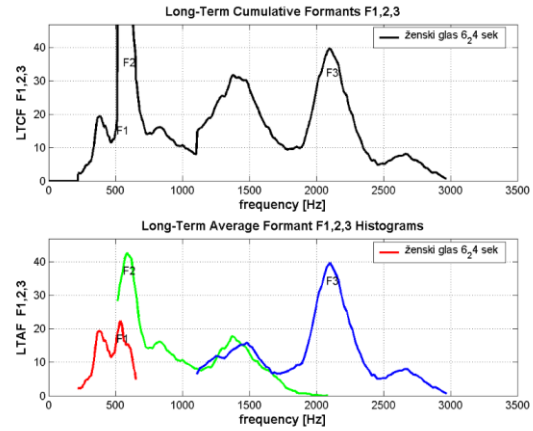
Slika 6: Datoteka 1 - dijagram 1



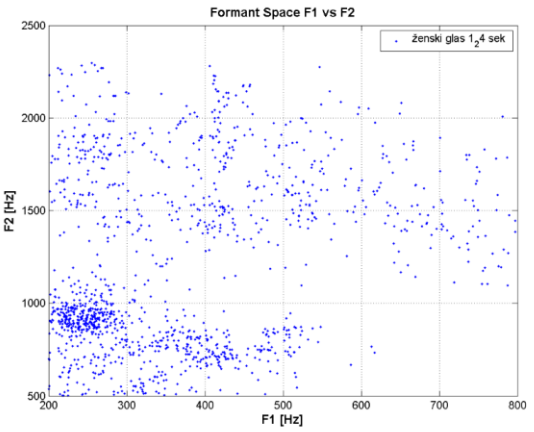
Slika 15: Datoteka 2 - dijagram 1



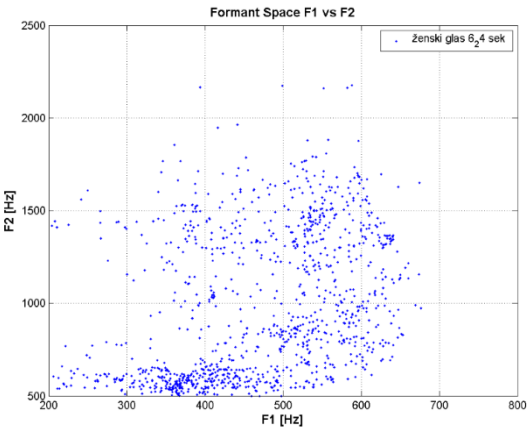
Slika 7: Datoteka 1 - dijagram 2



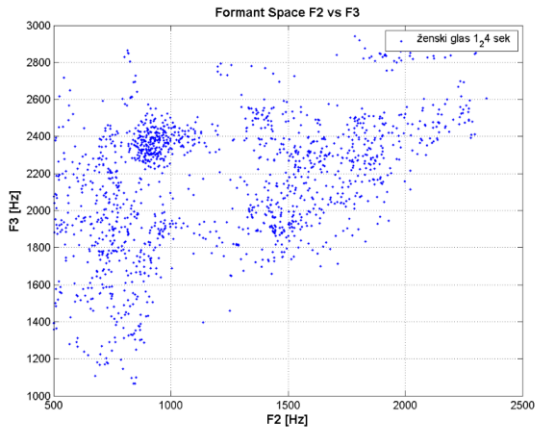
Slika 16: Datoteka 2 - dijagram 2



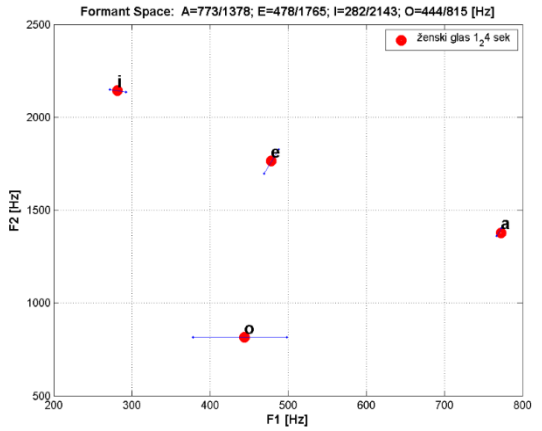
Slika 8: Datoteka 1 - dijagram 3



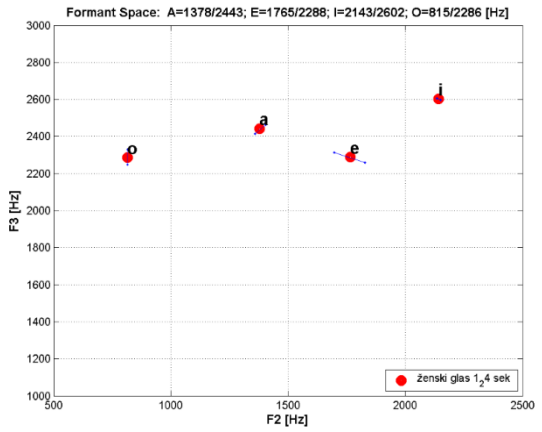
Slika 17: Datoteka 2 - dijagram 3



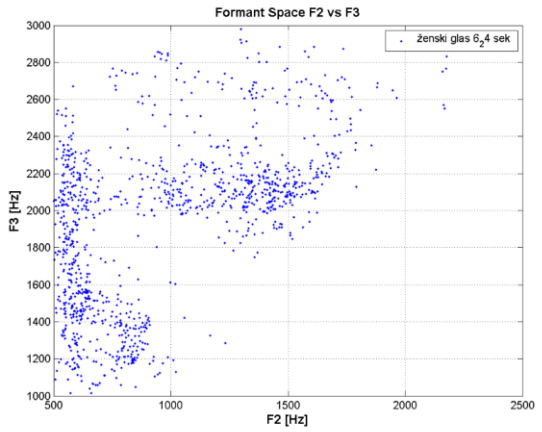
Slika 9: Datoteka 1 - dijagram 4



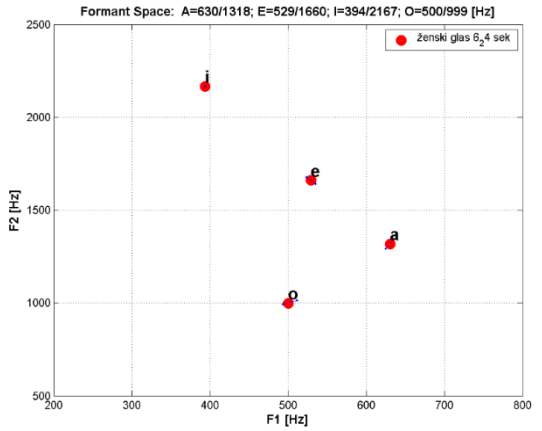
Slika 10: Datoteka 1 - dijagram 5



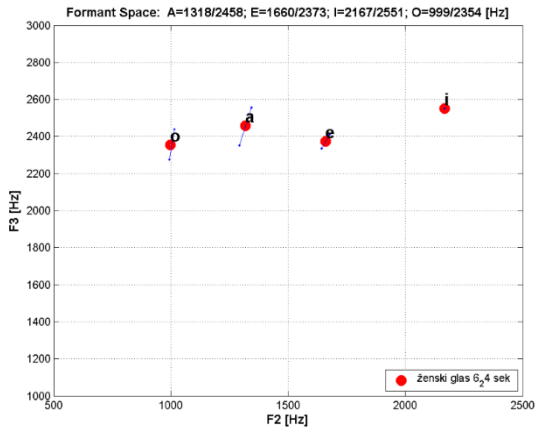
Slika 11: Datoteka 1 - dijagram 6



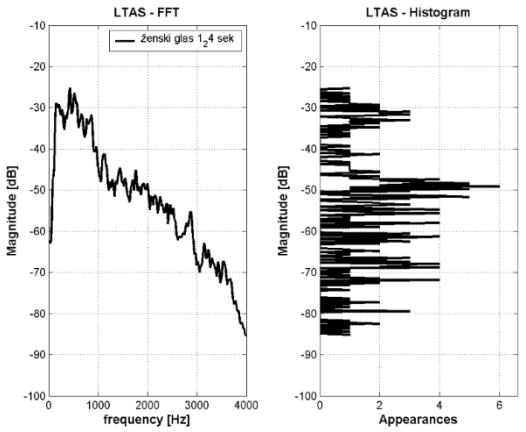
Slika 18: Datoteka 2 - dijagram 4



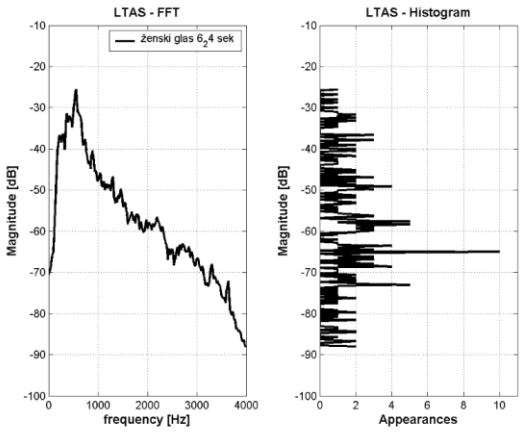
Slika 19: Datoteka 2 - dijagram 5



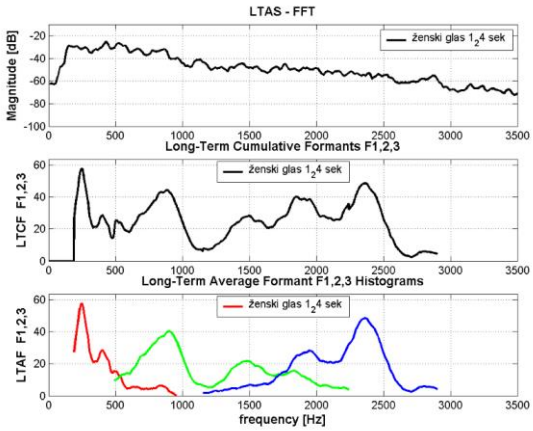
Slika 20: Datoteka 2 - dijagram 6



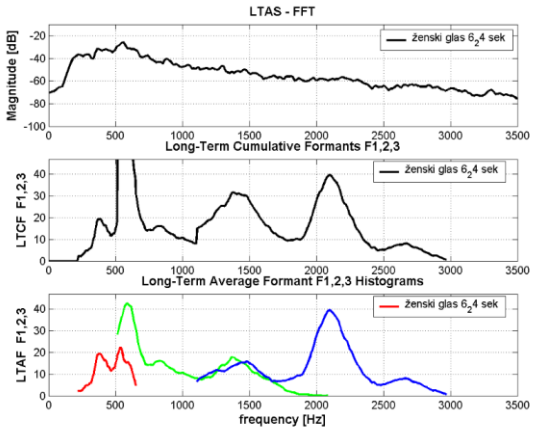
Slika 12: Datoteka 1 - dijagram 7



Slika 21: Datoteka 2 - dijagram 7



Slika 13: Datoteka 1 - dijagram 8



Slika 22: Datoteka 2 - dijagram 8

Usporedbu istovjetnih prikaza dijagrama Datoteke 1 i Datoteke 2 ne treba posebno komentirati. Izgledi i tijekovi grafova, te položaji vokala u formantnim prostorima, bitno se razlikuju, što upućuje na zaključak kako se radi o glasovima dviju različitih (ženskih) osoba.

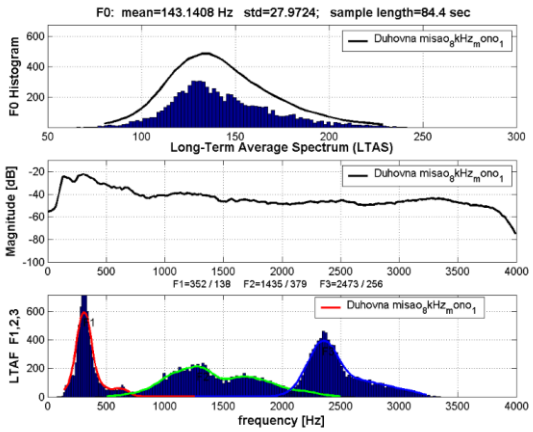
6. KOMPARACIJA GLASOVA ISTOG GOVORNIKA

U počecima audioforenzike, spektrogram nekog glasa nazivao se i *voiceprint*, po uzoru na forenziku papilarnih linija – *fingerprint*. Daljnjim proučavanjem ljudskog glasa i govora, došlo se, međutim, do spoznaje kako je ljudski glas sve samo ne tako stalan kao otisak prsta, daleko podložniji kojekakvim promjenama, pa ga se, strogo uzevši, ne može smatrati nikakvim postojanim "otiskom glasa". Jedan glas, riječ ili rečenica izgovoreni uzastopno, kod iste osobe, nisu potpuno jednaki po svojim zvučnim karakteristikama. Stoga, kod komparacije glasova u nekoj ekspertizi, uvijek se mora imati na umu i postojanje varijabiliteta unutar istog glasa.

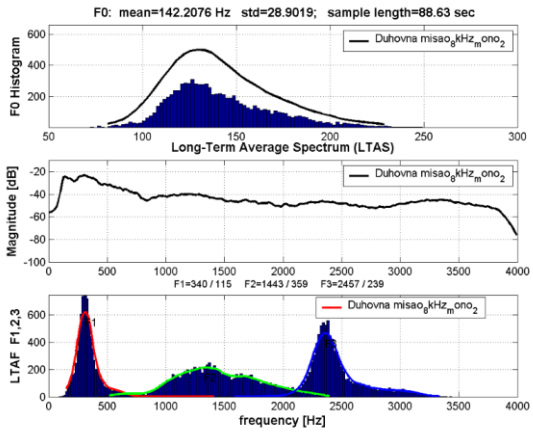
Kako izgledaju rezultati komparacije glasa istog govornika prikazat će se na sljedećem primjeru. Koristit će se audiozapis jedne radioemisije – Duhovna misao – govor muške osobe u trajanju od 4 minute i 10 sekundi. Audiozapis će se podijeliti na dva jednaka dijela –

datoteku *Duhovna misao_8kHz_mono_1.wav*, trajanja 2:04 min. i datoteku *Duhovna misao_8kHz_mono_2.wav*, trajanja 2:06 min. Datoteku *Duhovna misao_8kHz_mono_1.wav* u opisu slika ćemo imenovati Datoteka 3, a datoteku *Duhovna misao_8kHz_mono_2.wav* u opisu slika ćemo imenovati kao Datoteka 4. [183]

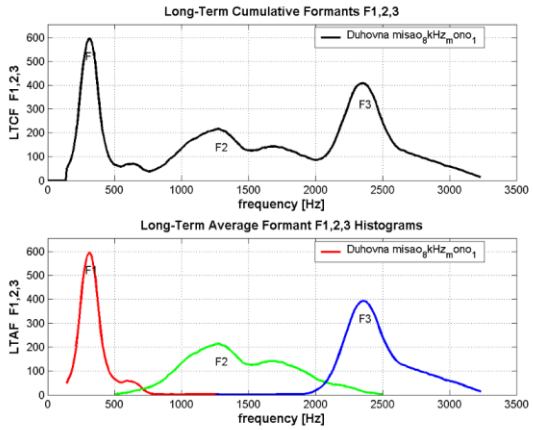
Na obje datoteke primijenit će se isti, gore već opisani postupak analize, a zatim će se pripadajući dijagrami usporediti. Rezultati su prikazani na slikama od 23 do 38.



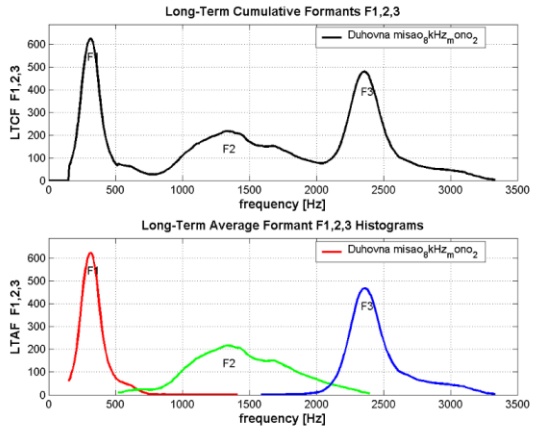
Slika 23: Datoteka 3 - dijagram 1



Slika 24: Datoteka 4 - dijagram 1

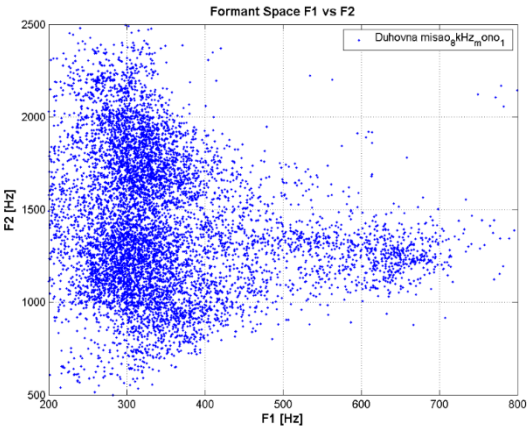


Slika 25: Datoteka 3 - dijagram 2

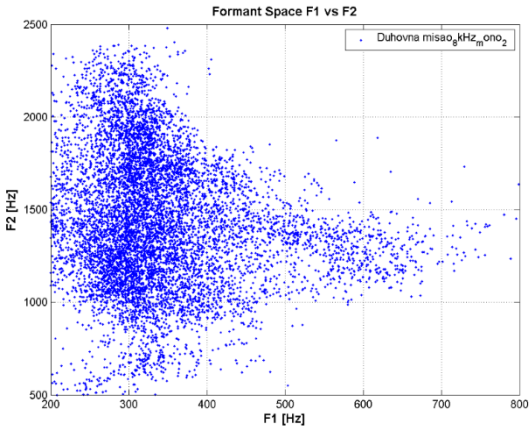


Slika 26: Datoteka 4 - dijagram 2

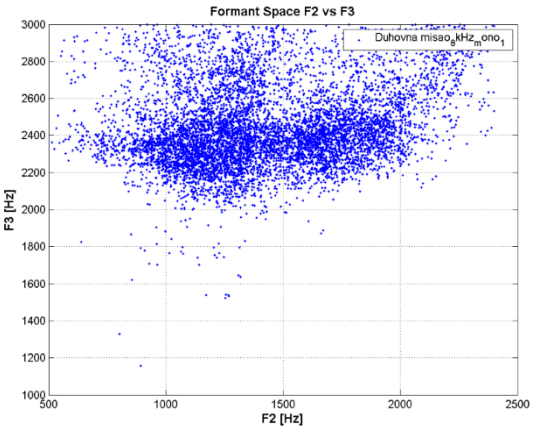
[183] Internetska adresa Microsoft OneDrive http://1drv.ms/1I3kHUS *Duhovna misao_8kHz_mono_1.wav* - Datoteka 3, *Duhovna misao_8kHz_mono_2.wav* - Datoteka 4, datum pristupa 19. 2. 2016.



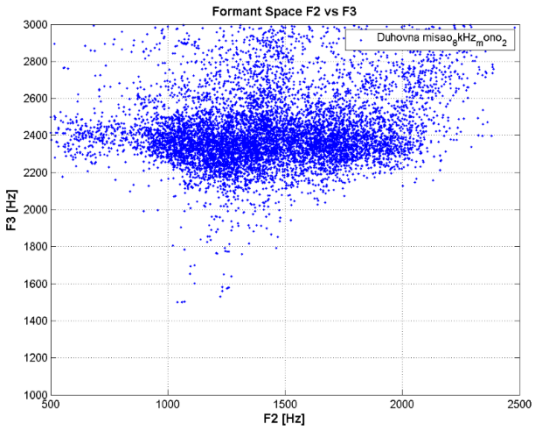
Slika 27: Datoteka 3 - dijagram 3



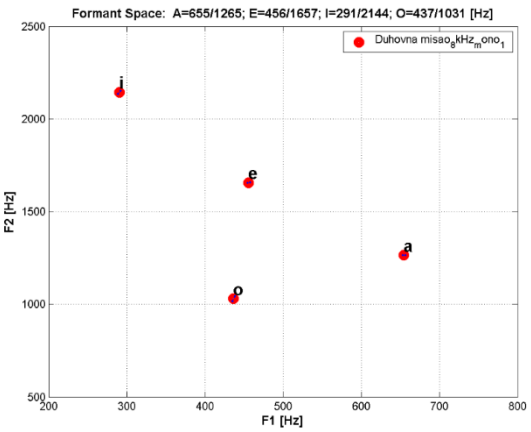
Slika 28: Datoteka 4 - dijagram 3



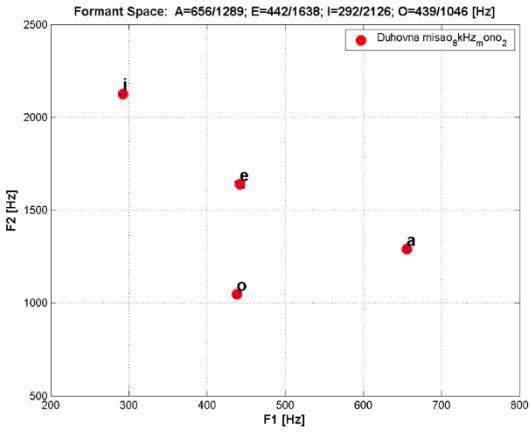
Slika 29: Datoteka 3 - dijagram 4



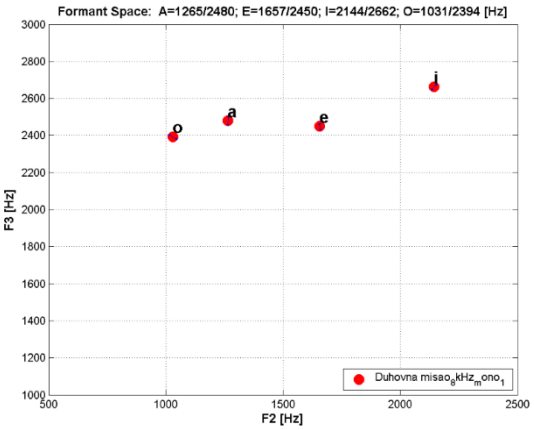
Slika 30: Datoteka 4 - dijagram 4



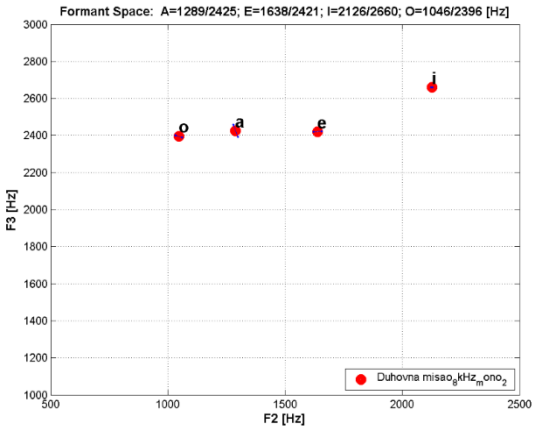
Slika 31: Datoteka 3 - dijagram 5



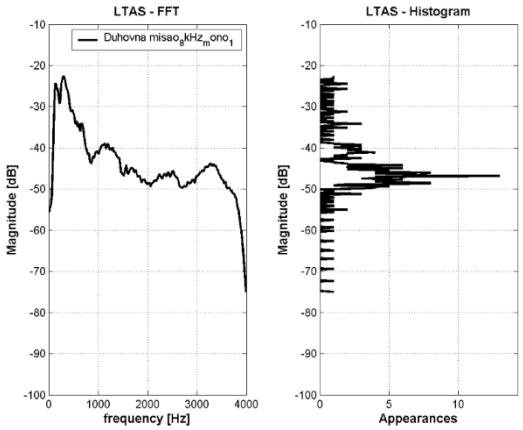
Slika 32: Datoteka 4 - dijagram 5



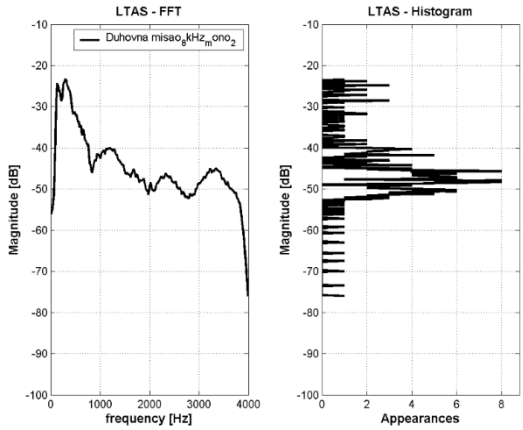
Slika 33: Datoteka 3 - dijagram 6



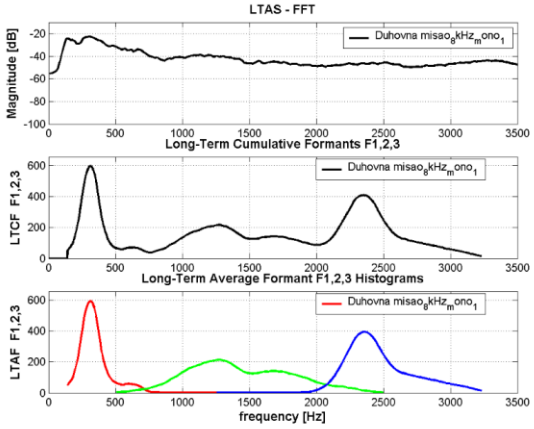
Slika 34: Datoteka 4 - dijagram 6



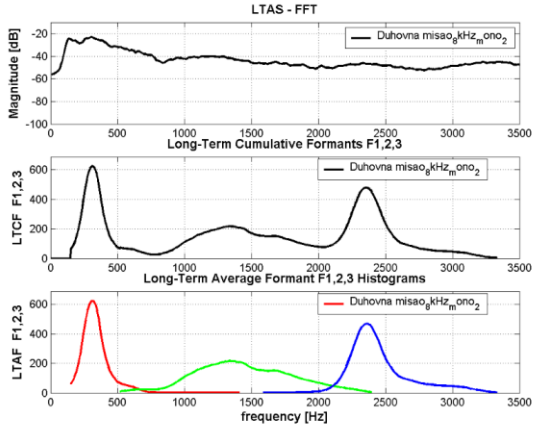
Slika 35: Datoteka 3 - dijagram 7



Slika 36: Datoteka 4 - dijagram 7



Slika 37: Datoteka 3 - dijagram 8



Slika 38: Datoteka 4 - dijagram 8

Međusobno pripadajući dijagrami pokazuju izvrsno poklapanje, što ukazuje na to kako je varijabilitet ovog glasa (govornika) minimalan.

7. ZAKLJUČAK

Iz prikazanog postupka analize govora, temeljene na dugotrajnom prosječnom spektru (LTAS), vidi se kako su rezultati prikazani kroz mnoštvo dijagrama. Ovim načinom omogućena je jednostavna komparacija dvaju ispitivanih zvučnih zapisa – relevantni dijagrami jednostavno se stavljaju jedan pored drugog, te se ocjenjuju tokovi krivulja, pronalaze vrhovi (maksimalne vrijednosti) na tim dijagramima, s pripadajućim frekvencijama i magnitudama. Lagano se uočavaju podudarnosti i/ili odstupanja, što može vidjeti i osoba koja nije ekspert u audioforenzici. Jednostavnom vizualnom usporedbom ocjenjuje se pripadaju li dva uzorka govora istoj osobi ili različitim osobama. Sadržaji govora dvaju audiozapisa ne moraju biti jednaki, jer LTAS postupak, u duljem vremenskom intervalu, usrednjuje frekvencijsku karakteristiku govornika. Međutim, ovi zapisi morali bi biti snimljeni s približno jednakim elektroničko prijenosnim karakteristikama kako bi se utjecaj varijabli na kvalitetu snimke što više smanjio.

Koliko je područje vještačenja i analize glasa i govora kompleksno i, kao dokaz na sudu, još uvijek nepouzdano ili samo u određenom stupnju pouzdano, govori i sudska praksa u svijetu. Identifikaciju osobe po glasu neki sudovi u SAD-u i drugim državama u svijetu prihvaćaju kao dokaz, neki uopće ne prihvaćaju, a neki prihvaćaju djelomično i uvjetovano, s određenim stupnjem dokazne snage. No, bez obzira na sudstvo, policija ovom forenzičnom disciplinom dobiva moćno oruđe u svojem svakodnevnom operativnom radu.

LITERATURA

Forensic Media Services, Ltd. Denver, CO, USA. http://www.forensicav.ro/software.htm (pristupljeno 19. 2. 2016.)

Royal Institute of Technology (KTH), Department of Speech, Music and Hearing, Stockholm. http://www.speech.kth.se/wavesurfer/ (pristupljeno 19. 2. 2016.)

University of Amsterdam, Phonetic Sciences. http://www.fon.hum.uva.nl/praat/ - (pristupljeno 19. 2. 2016.)

Zlatko Kovač
Nikola Protrka

COMPUTER ANALYSIS OF THE HUMAN VOICE AND SPEECH

Summary

This article discusses the analysis of the human voice and speech based on the long-term average spectrum of speech (Long-Term Average Spectrum - LTAS), in terms of forensic analysis needed at the disputed and undisputed pattern of computer forensics and expertise. Two computer programs working in conjunction have been used: WaveSurfer and Catalina Forensic Audio Toolbox. The first program analyses the audio track and the results stored in the form of text files, and the second program loads these files, processes them statistically and displays graphically the results through a series of diagrams. Authors briefly describe both of the computer programs, their capabilities and working windows through analysis of a voice ('a' vocal), the basic parameters of the human voice (fundamental frequency, formant and long-term average spectrum). Then an analysis of two different voices (speech of two female persons of similar tonal characteristics) has been made and the results compared through presentation of relevant diagrams. Finally, an analysis has been performed involving a voice of the same speaker, where both the first and second half of the voice record have been analysed. The relevant charts are also compared to determine matching curves on graphs or determine possible deviation (as a variability measure in voice and speech of the same person). For the above analysis and comparison, the authors have uploaded the audio files on the Internet and provided link to any interested reader for download and further analysis.

Key words: *expert analysis, speech, voice analysis, LTAS.*

STRUČNI RAD

Goran Guska[184]
Goran Blagojević[185]

SAVREMENI METODI I SREDSTVA U SUPROTSTAVLJANJU ZLOUPOTREBI PLATNIH KARTICA

Sažetak

Zahvaljujući naglom razvoju tehničko-tehnoloških dostignuća, plaćanje metalnim novcem, odnosno papirnim novčanicama odavno postaje zastarjeli način plaćanja koga svakodnevno sve više zamjenjuju savremeni instrumenti bezgotovinskog plaćanja i novčanih transakcija. Jedan od takvih instrumenata jeste platna kartica koja kao način bezgotovinskog plaćanja u razvijenim zemljama predstavlja jedno od najpopularnijih sredstava plaćanja. Uporedo sa pojavom i sve većom primjenom platnih kartica, javljaju se i prvi slučajevi njihove zloupotrebe, što predstavlja jedan od savremenih načina sticanja protivpravne imovinske koristi. Naime, nagli razvoj elektronskog bankarstva, odnosno kartičnog sistema poslovanja doveo je do povećanja broja korisnika ove vrste bankarskih usluga, što je s druge strane stvorilo ogromnu mogućnost za razne vrste zloupotreba platnih kartica. Upravo u ovom radu govorićemo uopšteno o platnim karticama sa posebnim osvrtom na njihovu zloupotrebu. Takođe, biće riječi o pravnom i kriminalističkom aspektu ove pojave, a uz uvažavnje rezultata sprovedenog anketnog istraživanja, pokušaćemo ponuditi rješenja u cilju suzbijanja ovakve vrste zloupotreba.

Ključne riječi: *platna kartica, zloupotreba, protivpravna imovinska korist.*

1. UVOD

Razvoj modernog društva u tehničko-tehnološkom smislu je svakako uticao i na unaprjeđenje načina plaćanja gdje se obim plaćanja metalnim i papirnim novcem smanjuje a svakodnevno ga sve više zamjenjuju savremeni instrumenti bezgotovinskog plaćanja i novčanih transakcija. Jedan od takvih načina bezgotovinskog plaćanja je platna kartica koja se u komercijalnoj upotrebi počinje pojavljivati početkom druge polovine prošlog stoljeća.

Platne kartice su se pojavile u Sjedinjenim Američkim Državama tokom 1920-te godine, kada su pojedine firme poput naftnih kompanija i lanaca hotela počele da ih izdaju svojim potrošačima. Ovakve kartice mogle su da se koriste samo u objektima kompanija koja ih je izdala i njihova upotreba se značajno povećala nakon Drugog svjetskog rata. Prvu univerzalnu karticu koja je mogla da se koristi u raznovrsnim prodajnim ili uslužnim objektima izdao je Diners Club 1950. godine. Ideja o platnim karticama potekla je od američkog biznismena

[184] Goran Guska MA, Visoka škola unutrašnjih poslova Banja Luka, Uprava za policijsko obrazovanje, MUP Republike Srpske, e-mail:goranguska@gmail.com
[185] Goran Blagojević mr., Visoka škola unutrašnjih poslova Banja Luka, Uprava za policijsko obrazovanje, MUP Republike Srpske, e-mail: blagojevicgoran@yahoo.com

Frenka Maknamare koji na jednoj poslovnoj večeri u restoranu uvidjevši da je zaboravio da ponese novčanik, ostavio svoju vizit kartu, a zatim sutradan došao i platio račun. Ova nezgodna situacija podstakla ga je na razmišljanje koliko poslovnih ljudi se našlo u sličnoj situaciji, iz čega se izrodila ideja o kartičnom poslovanju. Tako je osnovan Diners Club (eng. *to dine-večerati*) koji je prvi izdao istoimenu platnu karticu (Ivanović, 2011:4). Kada govorimo o platnim karticama i njihovoj upotrebi, ovdje podrazumijevamo dakle rasprostranjenost i elektronskog bankarstva, jer bez ovog načina funkcionisanja, platne kartice bi praktično bile beskorisne. Početkom osamdesetih godina prošloga vijeka kartice su postale uobičajeno sredstvo plaćanja roba i usluga i dostigle su razmjere masovne primjene. U bankama i organizacijama koje su se bavile kartičnim poslovanjem, za potrebe kartičnog poslovanja, razvijena je tehnološka i računarska infrastruktura koja je opsluživala ovako masovno sredstvo plaćanja. Bankomati su funkcionisali na bazi kartica, a uvodile su ih banke sa ciljem da smanje troškove šalterskog poslovanja, da stave na raspolaganje korisnicima mogućnost da 24 časa dnevno mogu da podižu novac i da pomoću njih produže vrijeme odležavanja novca na računima korisnika. U opticaju se nalazio veliki broj različitih kartica. Svaka banka je izdavala ili pokušavala da izdaje svoju karticu, ali se nekoliko svjetski poznatih sistema izdvojilo i počelo naglo da se širi i nameće kao standard. To je stvorilo potrebu za definisanjem svjetskog standarda, kako bi se omogućilo da se kartice jedne banke koriste na bankomatima drugih banaka.

Razvojem kreditnih kartica, banke su tokom vremena svojim klijentima nudile sve više različitih mogućnosti i usluga korištenja platnih kartica gdje banka praktično ispunjava želju svome komitentu na način da mu daje razne finansijske pogodnosti u cilju njegovog pridobijanja. Neke od pogodnosti za korisnika kreditnih kartica sastoje se u tome što iznos novca mogu da uplaćuju obročno, odnosno u određenim anuitetima, ratama i sl. plaćajući za to određenu proviziju, korištenje novca iako ga realno klijent ne posjeduje, dozvoljena prekoračenja, (tzv. minusi), internet bankarstvo i plaćanje usluga, ali prije svega, treba napomenuti da je najbitnije to što njezin korisnik ima mogućnost da raspolaže novcem i da mu novac bude dostupan u svakom trenutku dana i noći putem bankomata. Platna kartica i sve olakšice koje ona pruža postaju svakim danom sve prisutniji u životima običnog čovjeka. Međutim, ovaj način plaćanja roba i usluga postaje metom raznih vrsta zloupotreba. Tokom posljednjih godina, velika dostupnost i korištenje kreditnih kartica utiču da prevare u vezi sa njima postaju sve značajnije (Berg, 2007:325). Zbog ovakve tendencije, pojavu zloupotrebe platnih kartica treba sveobuhvatno sagledati i razumjeti pa pokušati dati odgovor kao reakciju na ublažavanje ove pojave i njenih posljedica. Upravo aktuelnost razvoja primjene platnih kartica u modernom društvu te negativne pojave koje takav razvoj prate motivisale su nas da ovim uratkom pokušamo dati odgovore na neka od aktuelnih pitanja u vezi sa platnim karticama I njihovim zloupotrebama. Značaj istraživanja se ogleda u bližem razumijevanju mogućnosti koje banka i njeni klijenti imaju elektronskim načinom poslovanja i uopšte prednostima elektronskog marketinga i upotrebe platnih kartica u finansijskom saobraćaju. Takođe, sam značaj istraživanja ogleda se i u problematici koja mora biti sagledana i sa kriminalističko-pravne strane. Naime, u tom smislu potrebno je obratiti pažnju na zloupotrebe platnih kartica i prevare kada je u pitanju ovaj način manipulisanja sa novcem. Savremeno funkcionisanje bankarskog sistema praktično uslovljavaju opstanak finansijske institucije,

(mislimo na banku), da ostvaruje svoje rezultate na tržištu, naročito u savremenoj današnjici, odnosno 21. vijeku, koristeći različita, odnosno sva tehnička dostignuća kojim bi sebi olakšali posao, ali istovremeno potrebno je zaštiti korisnika, odnosno građanina usluga platnih kartica, te obezbijediti mu sigurnost u domenu raspolaganja sopstvenim novcem.

Osnovna hipoteza ovoga rada jeste da veliki broj stanovništva koristi platne kartice kao sredstvo bezgotovinskog načina plaćanja. Posebna hipoteza ovog rada jeste da veliki broj želi da koristi platne kartice i da korisnici platnih kartica žele da saznaju koji je najbezbjedniji način korištenja ove vrste plaćanja. Druga posebna hipoteza ovog rada jeste da se građani plaše zloupotrebe i prevara u oblasti platnih kartica.

U ovom radu kao metod istraživanja koristiće se empirijski metod, odnosno metod ispitivanja, kojim ćemo ispitati 50 ispitanika na način da se podjednako obuhvati srazmjerno mogućnostima i prilici broj uposlenika bankarskih službenika, građana odnosno korisnika bankarskih usluga, različiti po strukturi pola, starosti, obrazovanja a kao odgovarajući instrument istraživanja koristićemo anketni upitnik koji se sastoji od deset pitanja otvorenog tipa, u okviru kojih ispitanici imaju po nekoliko mogućih opcija odgovora i odlučuju se za jednu od njih, za koju smatraju da je najprihvatljivija.

2. VRSTE PLATNIH KARTICA

U zavisnosti od izgleda, namjene i drugih karakteristika, postoji više vrsta platnih kartica. Tako u zavisnosti od izgleda postoje glatke i embosione (utisnute) platne kartice. Prema zapisu na platnoj kartici, imamo platne kartice sa magnetnim zapisom i platne kartice sa čipom. U odnosu na primjenu, platne kartice mogu biti: međunarodno validne platne kartice, nacionalne i korporativne platne kartice.

U odnosu na rok dospijevanja transakcije na naplatu, platne kartice se dijele na: kreditne i debitne platne kartice (Ivanović, 2011:5). Takođe treba napomenuti da su platne kartice proizvodi u vlasništvu izdavaoca kartice (banke odnosno neke druge finansijske institucije), dok su korisnici platnih kartica klijenti kojima se one izdaju radi korišćenja pod uslovima i na način koji je propisan opštim pravilima izdavaoca i u skladu s odredbama ugovora koji zaključuju izdavaoc i korisnik platne kartice. Platnu karticu može koristiti samo ono lice čije se ime nalazi na samoj kartici i ovo pravo nije prenosivo.

Kreditne kartice su kartice kojima se njihovim vlasnicima automatski odobravaju zajmovi, što omogućuje vlasnicima kartice da kupi robu ili uslugu od preduzeća bez gotovine ili čeka (Miller, VanHoose, 1997:63). Bitno je spomenuti da ovakav oblik finansijskog funkcionisanja u načinima korištenja kartičnih usluga i pogodnosti, zapravo je zastupljen odavno, a to se naročito odnosi na zemlje koje su u tehničko – tehnološkim inovacijama naprednije od nas. Danas se sve češće koriste za elektronsku trgovinu preko Interneta. Kreditne platne kartice su one kod kojih postoji mogućnost da se račun klijenta zadužuje mjesečno, tako što se dug dijeli na rate. Ovdje korisnik kreditne kartice može da troši sredstva do visine odobrenog limita, koji izdavalac kreditne platne kartice definiše prije toga. Shodno poslovnoj politici izdavaoca

kartice, rate se plaćaju na sam dan dospijeća, a na osnovu izvršenog obračuna i pregleda svih transakcija pojedinačno (Kresoja, Kirkov, 2009:499).

Kada je riječ o klijentu banke kome je banka izdala kreditnu karticu, odnosno korisniku ove kartice, potrebno je spomenuti da taj klijent posjeduje račun koji se praktično razlikuje od računa kojeg zovemo tekući. To znači da kreditna kartica jeste zapravo vezana za tekući račun prilikom naplate anuiteta, odnosno rate kredita, ali fizički to su ustvari dva različita računa što predstavlja inače račun po kreditnoj kartici i račun po kartici tekućeg računa (npr. preko kojeg računa klijent prima platu u banci). Fizičko lice koje posjeduje kreditne kartice, o stanju zaduženja po osnovu kredita može da se informiše na različite načine i u različitim vremenskim periodima, u zavisnosti od paketa, odnosno usluge koju koristi u banci.

Kao podvrsta ili kao druga kategorija kreditnih kartica postoje i tzv. „revolving“ kartice. Sam proces izdavanja ovih kartica predstavlja u pogledu prava, dužnosti i obaveza kako klijenta, tako i banke, mnogo odgovorniji proces i nosi sa sobom dodatno plaćanje koje može da se odnosi na plaćanje članarine,troškova održavanja računa i kamate na korišćeni kredit, koji se najčešće javlja u varijantama revolving kredita. Iako je naša zemlja, kao i zemlje u regionu u tranziciji, pojava prisutnosti kreditnih kartica je praktično preplavila stanovništvo u smislu korištenja ovih kartica. Upravo finansijski stručnjaci upozoravaju da se ovakve kartice racionalno troše jer postoji bojazan da će usljed nekontrolisane finansijske nediscipline, građani zapasti u dužničko ropstvo jer neće imati odakle vratiti ono što su po osnovu kredita potrošili.

Debitna kartica je takva vrsta platne kartice koja funkcioniše po principu jednostavnijeg korištenja. Ukoliko na tekućem računu građanina, odnosno klijenta banke, odnosno korisnika debitne kartice, postoji dovoljno sredstava, transakcija, bilo da se radi o kupovini ili plaćanju nekih usluga će biti odobrena. U suprotnom, ukoliko na tekućem računu nema sredstava, transakcija neće biti odobrena, ukoliko se ne radi o određenim platnim karticama koje dozvoljavaju korištenje sredstava u iznosu od jedne, dvije ili tri plate korisnika da uđe u dozvoljeni minus. Kamate, depoziti i ostali troškovi nisu uobičajeni za debitne kartice, osim na godišnjem nivou gdje se plaća godišnja članarina. Za trgovce međutim ne predstavlja neku posebnu razliku da li kupac posjeduje kreditnu ili debitnu karticu jer će trgovac svoju uslugu naplatiti momentalno (Barać i sur, 2007:130). Debitne kartice omogućavaju korisniku, odnosno komitentu banke, platne operacije u iznosu sredstava na depozitnom (deviznom) računu, bilo kao rentabilniji supstitut čekova i/ili identifikaciona kartica na elektronskim terminalima i blagajnama (Živković i sur., 2008:414). Vlasnik ove kartice posle kupovine nema period slobodnog kredita. To znači da komitent putem daljinskih komunikacionih veza povlači svoj novac sa svog tekućeg računa kod banke, bez potrebe da fizički dođe u banku. Debitne kartice mogu se koristiti u trgovinskim radnjama koje su snabdjevene POS terminalima ili bankarskim automatima (ATM).

Kada govorimo o podjeli kartica u smislu izmirenja obaveza koje su nastale korištenjem kartica, a koje obaveze banka potražuje od svoga klijenta, tj. korisnika kartice možemo reći da

postoje sistematizovane kartice među kojima izdvajamo: pay before ili pre paid kartice, debitne kartice i kreditne kartice čije plaćanje se vrši odloženo.

Kartice koje se nadopunjuju su one koje praktično imaju već određenu (dopunjenu) vrijednost sredstava koju je klijent uplatio da bi je kasnije koristio. Ovakve kartice su veoma popularne među populacijom koja realno ne može da posjeduje, odnosno da im banka izda druge neke kartice, iz različitih razloga (nezaposlenost, neredovna primanja i sl.). Ove kartice veoma su omiljene među studentima i mlađim osobama. One mogu da budu jednokratne ili mogu, kako je prethodno navedeno da budu limitirane na određeni period pod uslovom dopunjavanja sredstava na ovim karticama, ili čak držanja određenog minimalnog iznosa na kartici radi njenog negašenja. Najpoznatije kartice ove vrste su: poklon kartice (najčešće jednokratne upotrebe), kartice koje služe za uplate primanja ali su u vlasništvu poslodavca, kartice koje su namijenjene omladini i tinejdžerima, kartice koje izdaju mega marketi, kartice koje se koriste za plaćanje preko interneta, kartice za javni saobraćaj i studentske kartice.

3. ZLOUPOTREBA PLATNIH KARTICA

Krivično djelo falsifikovanje kreditnih kartica i kartica za bezgotovinsko plaćanje inkriminisano je u članu 276. Krivičnog Zakona Republike Srpske[186] a glasi:

1.Ko napravi lažnu kreditnu ili karticu za bezgotovinsko plaćanje ili ko preinači takvu pravu karticu u namjeri da je upotrijebi kao pravu ili ko takvu lažnu karticu upotrijebi kao pravu, kazniće se novčanom kaznom ili zatvorom do jedne godine.

2.Ako je učinilac djela iz stava 1. ovog člana upotrijebom kartice pribavio imovinsku korist, kazniće se novčanom kaznom i zatvorom do tri godine.

3.Ako je učinilac djela iz stava 1. ovog člana pribavio imovinsku korist u iznosu koji prelazi 10.000 KM, kazniće se zatvorom od jedne do osam godina, a ako taj iznos prelazi 50.000 KM, kazniće se zatvorom od dvije do deset godina.[187]

Ovo krivično djelo inkriminisano je u sljedećim oblicima: pravljenju lažne platne kartice u namjeri da se upotrebi kao prava; preinačenju prave platne kartice u namjeri da se upotrebi kao prava; upotrebi lažne, odnosno preinačene platne kartice kao prave; neovlašćenoj upotrebi tuđe platne kartice; neovlašćenoj upotrebi povjerljivih podataka koji jedinstveno uređuju tu karticu u platnom prometu; nabavljanju lažne platne kartice u namjeri da se upotrebi kao prava; pribavljanju podataka u namjeri da se iskoriste za pravljenje lažne platne kartice (Ivanović, 2011:7). U narednom tekstu definisaćemo neke od njih.

Prvi oblik krivičnog djela falsifikovanje i zloupotreba platnih kartica postoji onda kada je riječ o pravljenju lažne platne kartice ili preinačavanju prave platne kartice u namjeri da se ona

[186]Službeni glasnik Republike Srpske, broj 49, od 25. juna 2003. godine.
[187]Krivični zakon Republike Srpske., preuzeto sa:
http://www.tuzilastvobih.gov.ba/files/docs/zakoni/Krivicni_zakon_lat_RS_49_03.pdf
(Pristup:07.02.2016.godine).

upotrebi kao prava, odnosno upotrebi lažne odnosno preinačene platne kartice. Pravljenje lažne platne kartice znači proizvodnju jedne materije ili stvari koja posjeduje određena svojstva prave platne kartice na osnovu kojih se može upotrebiti kao prava platna kartica. Nije nepohodno da napravljena lažna platna kartica u svakom pogledu imitira pravu, već je potrebno da posjeduje određene elemente originalne platne kartice koji omogućavaju njenu upotebu kao prave. Naime, nepohodno je da lažna platna kartica ima magnetnu traku sa podacima koji su prethodno prekopirani sa originalne platne kartice, ali nije nepohodno da lažna platna kartica po svom spoljašnjem izgledu bude vjerna imitacija originala. Pravljenje lažne platne kartice po svojoj prirodi sadrži u sebi imitaciju, tj. pravljenje lažne platne kartice predstavlja izradu lažne platne kartice sa određenim elementima prave platne kartice, koji omogućavaju njenu upotrebu kao prave (Ivanović, 2011:7-8) Za postojanje krivičnog djela bez značaja je u kojoj je količini izvršeno pravljenje lažnih platnih kartica. Krivično djelo je izvršeno pravljenjem samo jedne lažne platne kartice u namjeri da se upotrebi kao prava. Prema tome, ako je napravljeno više lažnih platnih kartica, u tom slučaju neće postojati sticaj, već jedno krivično djelo.

Preinačenje prave platne kartice smatra se promjena prirode, izgleda i sadržaja određene stvari, odnosno pravljenje od jedne stvari nečega što ona nije po svojoj prirodi ili namjeni. S tim u vezi pod preinačenjem prave platne kartice podrazumijeva se prepravljanje prave platne kartice tako da ona dobije drugačiji izgled od onog koji stvarno ima, a u namjeri da se upotrebi kao nepreinačena prava platna kartica. Ovo se uglavnom vrši na taj način što se slip na kome se nalazi potpis vlasnika platne kartice briše i prepravlja drugim potpisom, kako bi se prava platna kartica mogla koristiti za plaćanje na POS terminaliima od strane osobe koja nije pravi korisnik te kartice. Prema tome. preinačavanjem prave platne kartice mijenjaju se određeni zaštititni elementi koji omogućavaju njeno nesmetano korišćenje od strane osoba koje nisu pravi korisnici te platne kartice.

Upotreba lažne, odnosno preinačene platne kartice se ogleda radnji ovog krivičnog djela koju predstavlja svaka upotreba lažne ili preinačene platne kartice kao prave, što se najčešće ostvaruje kupovinom robe plaćanjem usluga, duga, dažbina, podizanjem novca sa bankomata i slično. Za postojanje ovog krivičnog djela je bez značaja da li je lažna platna kartica prethodno falsifikovana, odnosno preinačena od strane nekog drugog lica, ili pak od strane lica koje tu lažnu ili preinačenu platnu karticu upotrebljava kao pravu.

Nabavljanje lažne platne kartice treba shvatiti kao svaku djelatnost kojom se stiče lažna platna kartica. Prema tome, za postojanje krivičnog djela je bez značaja o kakvoj se djelatnosti radi, već je važno samo da se tom djelatnošću ostvaruje posjedovanje lažne platne kartice. S tim u vezi nabavljanje lažne platne kartice može se ostvariti kupovinom, trampom, primanjem na poklon, oduzimanjem i slično. Za postojanje djela bitno je da još prilikom pribavljanja postoji namjera da se takava lažna platna kartica upotrebi kao prava. Treba napomenuti da je sasvim irelevantno da li je lažna platna kartica pribavljena direktno od lica koje je tu lažnu platnu karticu napravilo ili od nekog drugog lica. Krivično djelo je izvršeno samim pribavljanjem takve lažne platne kartice u pomenutoj namjeri.

Pribavljanje podataka za pravljenje lažne platne kartice ogleda se u djelatnostima kojima se stiče magnetni sadržaj prave platne kartice. S tim u vezi pribavljanje podataka za pravljenje lažne platne kartice može se ostvariti skimovanjem (kopiranjem), kupovinom, trampom ili primanjem na poklon magnetnog sadržaja platne kartice i slično. Takođe, kao i u prethodnom slučaju za postojanje djela bitno je da se pribavljanje pomenutih podataka vrši sa namjerom da se isti iskoriste za pravljenje lažne platne kartice.

4. ZLOUPOTREBE KOD KORIŠTENJA BANKOMATA

Bankomat – ATM (*automated teller machine*) pruža usluge klijentima na principima savremene tehnologije i elektronike. Moglo bi se reći da je to neka vrsta automatske banke sa širokom ponudom usluga. Neke od najčešće dostupnih usluga koje se nude korisniku su podizanje gotovog novca u svako doba dana, provjera stanja na računu korisnika, plaćanje računa i uplate na račun, polaganje depozita, usluge noćnog trezora, mjenjački poslovi, kupovina karata za parking ili javni prijevoz te kupovina dopuna za mobilne telefone.
Za korištenje bilo koje od usluga putem bankomata potrebno je imati platnu karticu i odgovarajući PIN kod (*personal identification number*) koji je zapravo lozinka koju poznaje jedino korisnik kartice a služi kao autentikacija korisnika prilikom korištenja usluga putem bankomata. Zloupotrebe platnih kartica kod usluga na bankomatima suštinski se odnose upravo na nezakonito pribavljanje podataka koji su poznati jedino korisniku da bi tako dobijeni podaci kasnije bili zloupotrijebljeni radi ostvarivanja protivpravne imovinske koristi na štetu korisnika kartice.

Jedan od načina nezakonitog pribavljanja podataka je pomoću uređaja koji se postavlja na čitač (otvor za primanje platne kartice) na bankomatu. To je lažni čitač platne kartice (Skimer) u koji je ugrađen aparat za čitanje magnetne linije i skladištenje podataka (u lokalnoj memoriji), ili aparat koji služi za prosljeđivanje podataka (npr. na radiofrekvenciji, putem poruke). Originalni čitač kartice pored postavljenog lažnog čitača u stanju je da povuče i učita podatke sa platne kartice, to znači da se transakcija može izvršiti na ATM. Aparat za kopiranje podataka može biti izrađen na više načina, od dobre kopije, koja može da obavi sve do onih koji se lako mogu primijetiti. Lažni aparat (Skimer) je obično iste boje kao i originalni čitač kartice, kako to ne bi pobudilo sumnju korisnika ove bankarske usluge na dotičnom ATM.

Drugi način se odnosi na postavljanje prednje strane lažnog bankomata na dio bankomata koji je dostupan samo klijentima-korisnicima ove bankarske usluge gdje se lijepi kompletna prednja strana. Lažna prednja strana se u cjelosti može postaviti na ATM, i na njoj se formira otvor za izdavanje novčanica, otvor za ubacivanje depozita i otvor za (prijem) učitavanje platne kartice. Otvor za učitavanje platne kartice je tako izrađen, da može da utvrdi i skladišti podatke sa magnetne linije platne kartice (u lokalnoj memoriji), ili da prosljeđuje podatke (npr. komunikacija preko radiofrekvencije). Na lažnoj prednjoj stranici obično se postavljaju i naljepnice, koje banka koristi u cilju informisanja korisnika ATM-a i da im skrene pažnju. Boja lažne prednje strane obično je identična sa originalnom bojom ATM-a.

Jedan od starijih i dobro poznatih načina nezakonitog pribavljanja podataka se vrši pomoću „ wire tapping“ metode kada se na komunikacionu liniju priključuje manji čitač, koji ima ulogu da očitava, utvrđuje i prosljeđuje podatke od bankomata i šalje ih primaocu. Podaci koji se šalju od bankomata su između ostalih i podaci sa magnetne linije, koji se kasnije koriste za nezakonite transakcije.

Nezakonito pribavljanje PIN koda se može vršiti sa lažnom PIN tastaturom gdje se na PIN tastaturu bankomata obično lijepljenjem postavlja lažna PIN tastatura, koja od strane korisnika usluge na ATM ukucani PIN kod, mehanički prosljeđuje PIN tastaturi bankomata, ali u međuvremenu utvrđuje i skladišti (u lokalnoj memoriji), ili prosljeđuje (npr. komunikacijom preko radiofrekvencije) ukucani kod. Lažna PIN tastatura je uglavnom ofarbana u boju bankomata, boje tastatura i natpisi raznih funkcija se podudaraju s pravom tastaturom ili se koristi čak originalna tastatura za određeni tip bankomata.
Nadalje, prisutan je metod kad se PIN kod pribavlja sa kamerom koja se prethodno ugrađuje u bankomat ili u njegovoj blizini.Na pogodnom mjestu bankomata ugrađuje se mikrokamera, koja kroz otvor snima ukucavanje PIN koda od strane korisnika. U konstrukciju se ugrađuje aparat za skladištenje (u lokalnu memoriju), ili aparat za prosljeđivanje PIN koda do izvršioca ovog kriminalnog djelovanja.Takođe, moguće je u blizini bankomata postaviti skrivenu (kamufliranu) mikrokameru (npr. skrivena u signalizatoru za dim ili držaču za brošure na samom bankomatu, fiksiranu na plafon iznad ATM i slično), čiji otvori za snimanje su usmjereni na PIN tastaturu.

Neka od zloupotreba se može izvršiti manipulacijom čitača kartica za kontrolisanje pristupa u predvorje filijale (tzv. lobbi ATM – to je samostojeći bankomat koji se postavlja u dvadesetčetveročasovnim zonama ili predprostorijama na ulasku u filijalu banke) u koji se ugrađuje skimer za kopiranje, koji učitava sve podatke sa magnetne linije platne kartice i skladišti (u lokalnu memoriju) ili prosljeđuje (npr. komunikacijom preko radiofrekvencije) informacije izvršiocu ovog kriminalnog djelovanja. Izvršioci ovih krivičnih djela obično kradu čitač kartice za kontrolu pristupa i ugrađuju svoj pripremljen skimer za pribavljanje podataka. Unaprijeđena verzija je kada se pored skimera postavi i tastatura za unos PIN koda. Aparat za pribavljanje podataka je tako izrađen da nakon provlačenja kartice traži od korisnika i PIN kod, koji može da skladišti ili da ga proslijedi. Aparat za kopiranje se može izraditi na više načina, od dobre kopije, koja može da obmane, sve do onih koji se lako mogu primijetiti. Postavljanu spravu izvršioci obično zalijepe ili unutrašnjost izlivaju vještačkom smolom, tako kopija savršeno biva prilagođena originalnom aparatu za kontrolu pristupa u predvorje filijale (lobbi ATM).

Libanska petlja je stara i dobro poznata metoda za vršenje prevara na ATM tako što se (u otvor za prijem platne kartice postavi savijena traka načinjena od rentgenskog filma koja je takvog oblika da kartica ne moze da izađe iz bankomata odnosno ostane zaglavljena u međuprostoru između čitača kartice i otvora), a zatim se pravom korisniku platne kartice približi lice koje navodno želi da pomogne i savjetuje korisnika da još jednom unese PIN kod, naravno samo radi toga da on sazna ove podatke, nakon čega se ništa ne dešava i kriminalac sačeka da korisnik ode sa lica mjesta, a nakon toga izvlači platnu karticu iz bankomata uz

pomoć naprijed navedene trake i uz PIN kod koji je saznao, praktično mu je omogućeno da počisti račun na istom ili pak na drugom bankomatu.

Jedna od mogućih metoda kriminalnog pribavljanja podataka sa platnih kartica je sprega kriminalaca kao eksternih faktora sa licima koja opslužuju, servisiraju i održavaju bankomate. Uloga ovih lica je da kriminalcima omoguće pristup računaru bankomata, gdje se u logovima čuvaju podaci sa magnetne piste obavljenih transakcija. Zloupotreba se sastoji u tome da se preko nekih od ulaznih portova na računaru ukradu brojevi kartica koji se nalaze na računaru, a drugi poznati oblik je instaliranje zlonamjernog programa-virusa koji će u određenom trenutku dovesti do nekontrolisane isplate novca inicirane ubacivanjem platne kartice koja na magnetnoj pisti ima potreban zapis za to.

Postavljanje potpuno, odnosno u cjelini lažnog bankomata, koji je po izgledu potpuno funkcionalan i postavlja se obično na prometnom mjestu poput velikih tržnih centara i to uz već postojeće prave bankomate. Prilikom vršenja transakcija, odnosno nakon unosa platne kartice i PIN koda bankomat prikazuje na ekranu odnosno monitoru, da nije moguće izvršiti transakciju, i vrati platnu karticu korisniku, ali su prije toga, korumpirani podaci sa piste i PIN kod, što kasnije služi za zloupotrebe i prevare sa platnim karticama na pravim bankomatima. U ovim slučajevima svi podaci se skladište u samom lažnom bankomatu, koji ima komunikaciju sa izvršiocima ovih kriminalnih radnji.

5. SUPROTSTAVLJANJE ZLOUPOTREBI KORIŠTENJA PLATNIH KARTICA

Politika suprotstavljanja kriminalitetu sadržinski obuhvata dva osnovna oblika reakcije države i društva na kriminalitet a čine ih prevencija – sprečavanje kriminaliteta i represija – suzbijanje kriminaliteta.(Jovičić, 2011: 207-216).

Zadatak kriminalistike u pogledu suprotstavljanja ovako savremenom i specifičnom obliku kriminaliteta, jeste da ove dvije značajne komponente poveže, uporedi i da time ukaže na najcjelishodnija rješenja za praktično antikriminalno ponašanje u društvu. U tom pravcu je neophodno stalno praćenje zahtjeva i potreba društva na planu suprotstavljanja kriminalitetu u ovoj oblasti, a pri tome treba imati u vidu da je prevencija, iako vrlo često nedovoljna, uvijek najracionalnije i najhumanije rješenje, ukoliko je uspješna. Cilj i zadatak preventivnog djelovanja ukazuje na to da je ono u odnosu na represivna – postdelikatna postupanja: svrsishodnije, humanije i cjelishodnije.

Prevencija kriminaliteta u oblasti kartičarstva nalazi svoju opravdanost i u činjenici što je sadašnja edukacija i na njoj zasnovana praksa mnogo bliže represivnom, odnosno postdeliktnom nego preventivnom postupanju, iako je uspjeh i efikasnost u suprotstavljanju ovom kriminalitetu moguće postići samo intenzivnom i stalnom koordinacijom ove dvije metode, što za sada nije slučaj. Preventivne mjere zaštite su nesumnjivo u skladu i sa demokratskim razvojem društva, što ima za cilj postupnije angažovanje svih društvenih činilaca u suprotstavljanju kriminalitetu, kao i humaniji odnos prema čovjeku uopšte.

Preventivne mjere treba da imaju za cilj sprečavanje kriminaliteta, kroz preduzimanje niza mjera na zaštiti poslovanja u sferi korišćenja platne kartice kao sredstva i načina bezgotovinskog plaćanja robe i usluga.

Mjere prevencije u oblasti kartičarstva se ogledaju kroz sljedeće oblike:

- Normativno regulisanje ovog načina poslovanja, što se ogleda u donošenju odgovarajućih pravila i procedura za poslovanje s platnim karticama.
- Fizičko-tehničku zaštitu, gdje je potrebno uvođenje novih standarda i tehničko-tehnoloških dostignuća u ovoj oblasti.
- Preventivni rad pri obavljanju redovnih poslova i zadataka u korišćenju platnih kartica.
- Otklanjanje uzroka koji utiču na kriminalitet, odnosno aktivnosti na otklanjanju preddeliktnih stanja.
- Edukacija i razvijanje bezbjednosne kulture kod klijenata-korisnika platnih kartica kod zaposlenih u bankama i drugim finansijskim institucijama koje izdaju platne kartice, kao i kod trgovaca, ugostiteljskih radnika i svih drugih gde se platne kartice koriste. (Kresoja, Kirkov, 2008: 510-512)

Sveobuhvatna politika zaštite poslovanja uz korišćenje platnih kartica treba da se zasniva ne na eliminaciji rizika, već na upravljanju rizikom. To praktično znači dobro razumijevanje prirode i ozbiljnosti različitih tipova rizika u poslovanju s platnim karticama, određivanje rizika koji se može smatrati prihvatljivim u situaciji u kojoj se posluje u sistemu funkcionisanja platnom karticom, dovođenje postojećeg rizika na nivo koji se može smatrati prihvatljivim ili bar opravdanim.

Jedna od najvažnijih preventivnih mjera protiv zloupotrebe jeste stalna edukacija kako korisnika tako i trgovaca koji posjeduju POS terminale o bezbjednom korišćenju platnih kartica. Tu se prvenstveno podrazumijeva dobro poznavanje uputstava i odredaba ugovora koji su i pisani na osnovu dosadašnjih iskustava u korišćenju kartica, kako od strane finansijskih ustanova i korisnika tako i od strane preventive prema mogućim zloupotrebama.
Drugi vid je uvođenje kartica sa čipom, čime se višestruko povećava nivo zaštite platnih kartica od falsifikovanja, kao i obavezno unošenje PIN koda pri korišćenju platne kartice čime se smanjuje mogućnost zloupotrebe prilikom krađe ili gubljenja kartice.

Treći vid je mogućnost da sam korisnik kartice prilikom sklapanja ugovora o korišćenju platne kartice obavezno zahtijeva uključivanje SMS servisa, odnosno da mu prilikom svake promjene na računu stigne SMS poruka. Na ovaj način korisnik ukoliko primi SMS za transakciju koju nije lično učinio može istog momenta da kontaktira autorizacioni centar i da spriječi njenu dalju zloupotrebu nalogom da se kartica blokira.
Četvrti vid je obavezno postavljanje softvera za RISK monitoring koji će vršiti praćenje transakcija platnim karticama uz dnevno izvještavanje o sumnjivim transakcijama kao i o pokušajima zloupotreba.

Posljednje i najskuplje rješenje, ali koje je ujedno i najbolja zaštita finansijskih institucija i njihovih korisnika, jeste nadzor i kontrola transakcija u realnom vremenu – RISK monitoring online.(Nellie, 2013:129-135) Risk monitoring online koristi jedna od banka u našem okruženju koja je ujedno i procesor unutar kuće za platne kartice. Sistem je postavljen tako što je RISK monitoring praktično izmješten iz procesing centra i organizovan u tri odjeljenja. Prvo odjeljenje se bavi samo karticama izdanja te banke odnosno preko RISK monitoringa – računara na kojima se prate transakcije odnosno na kojima na osnovu postavljenih parametara na monitoru računara "iskaču" sumnjive transakcije. Drugo odjeljenje se bavi praćenjem prihvatne mreže bankomata i POS terminala te banke uz stalno nadgledanje izvršenih transakcija.Konačno, treće odjeljenje se bavi isključivo već učinjenim zloupotrebama, kao upravljanjem video zapisima, kao i saradnjom sa policijom i pravosudnim organima u cilju rasvjetljavanja krivičnih djela iz ove oblasti.

6. ANALIZA REZULTATA EMPIRIJSKOG ISTRAŽIVANJA

Anketnim upitnikom metodom slučajnog izbora obuhvaćen je uzorak od 50 ispitanika gdje je pomenutom metodom obuhvaćen uzorak od 12 službenika iz 4 komercijalne banke u gradu Banja Luka, a banke koje su bile obuhvaćene istraživanjem su najreferentnije u smislu ponude i potražnje u ovom dijelu bankarskog poslovanja i zakona tržišta u ovom sektoru koji je i bio predmet istraživanja. Kada je riječ o korisnicima usluga banaka oni su takođe izabrani metodom slučajnog uzorka i vođeno je računa da bude korektna zastupljenost komiteneta, odnosno klijenata banke. Analogno tome građani koji su zatečeni u vrijeme anketiranja u bankama su predstavljeni brojčano kako slijedi: 13 ispitanika koji su korisnici usluga Nove Banke Banjaluka, 10 ispitanika NLB Banke, 9 Unicredit Banke i 6 ispitanika Raiffeisen Banke. Ukupan broj anketiranih ispitanika klijenata banaka je 38. Anketni list je sadržao deset pitanja sa ponuđenim odgovorima.

Prvo pitanje je formulisano na sljedeći način: „ Da li ste upoznati sa primjenom platnih kartica u sistemu bankarstva?“Prema prikupljenim podacima uočeno je to da veliki broj ispitanika zapravo koristi usluge platnih kartica odnosno koristi usluge kartičarstva. U ovom smislu potrebno je reći da je broj građana koji su dali pozitivan odgovor najveći i iznosi 38 ,odnosno 76%, onih koji su se izjasnili kao djelimično upoznati je 9 odnosno 18% dok su se oni koji su dali negativan odgovor pojavili u procentu 6% odnosno tri ispitanika.

Analizom odgovora na drugo pitanje anketnog upitnika „ Da li koristite usluge platnih kartica i elektronskog bankarstva?“ došli smo do rezultata da najveći broj ispitanika anketnog upitnika i to njih 46% koriste usluge platnih kartica, dok njih 38% se izjasnilo da koristi ove usluge samo za podizanje gotovog novca. 12% ispitanika koristi ovaj način finansijskog funkcionisanja u smislu plaćanja računa a samo 4% ispitanika ne koristi platne kartice i usluge elektronskog bankarstva. Dakle, u svemu navedenom je vidljivo da 96% od ukupno ispitanih lica zapravo koriste usluge platnih kartica i elektronskog bankarstva što potpuno potvrđuje ponovo opštu hipotezu ovoga rada.

Treće pitanje anketnog upitnika glasilo je : „Smatrate li da je vaš novac bezbjedan u sistemu kartičnog poslovanja?“ i baziralo se na drugu posebnu hipotezu ovoga rada. Kako bi se na nju

podsjetili, spomenućemo da se ona odnosi na pretpostavku da se građani u najvećoj mjeri plaše zloupotrebe i prevara u oblasti platnih kartica. Upravo odgovorom na ovo treće pitanje utvrdili smo da je najveći broj ispitanika 42% izjavio da su takvog stava i mišljenja da strahuju od mogućnosti zloupotrebe i prevare u pogledu svoga novca kada je u pitanju sistem platnih kartica. Nešto malo manji broj procentualno izraženih ispitanka i to njih 36% su stava da potpuno smatraju kako je njihov novac bezbjedan u segmentu ovog načina finansijskog funkcionisanja. Ispitanici i to njih 22% su mišljenja da ovaj način bezbjednosti njihovog novca nije zadovoljavajući. Na osnovu odgovora na treće pitanje, možemo konstatovati da su u potpunosti potvrđene hipoteze i to druga posebna hipoteza koja se odnosi na strah građana od zloupotrebe i prevare u ovom pogledu poslovanja, ali i opšta generalna hipoteza koja govori o pretpostavci da veliki broj stanovništva koristi platne kartice kao sredstvo bezgotovinskog načina plaćanja.

Četvrtim pitanjem anketnog upitnika (Kakva su vaša iskustva u pogledu korištenja platnih kartica?) praktično je željeno postići kontrolno pitanje u smislu korektnosti odgovora ispitanika, kako bi se moglo utvrditi da isti nisu zamoreni pitanjima ili da na ponudjene odgovore ne odgovaraju automatski ili mahinalno. Odgovori koji su bili pozitivni su zastupljeni procentualno sa 96% a negativni samo 4%. Može se zaključiti da ovakav način poslovanja sa bankama odgovora građanima i da je generalno prihvaćen.
„Smatrate li da građani vjeruju u bezbjednost elektronskog bankarstva i upotrebi platnih kartica?“ bilo je peto pitanje gdje se 48% ispitanika izjasnilo da građani imaju povjerenja, 44% da sve više imaju povjerenja i 8% da uopšte nemaju povjerenja. Ovo pitanje daje posredan odgovor kakav je stav većeg dijela korisnika ovih bankarskih usluga. U ovom smislu jako je bitno je spomenuti činjenicu da ispitanici smatraju da građani vjeruju u sam sistem kartičnog poslovanja, odnosno platnih kartica, kao i u samu bezbjednost njihovog novca kojim raspolažu u ovom smislu.

Pitanje broj šest je glasilo:“ Da li se plašite zloupotrebe vaše platne kartice?“.Pozitivan odgovor dalo je 72% ispitanika, negativan odgovor 18% a 10% odnosi se na odgovore da je neopredjeljen. Kada je u pitanju šesto pitanje anketnog upitnika, ono se prevashodno odnosilo na drugu posebnu hipotezu ovoga rada a koja se odnosi na pretpostavku da se najveći broj građana plaši zloupotrebe u oblasti platnih kartica. Naime, u svemu ovome jasno se može zaključiti da to praktično i jeste činjenica a čemu doprinose različiti razlozi, bilo to neinformisanost, neobrazovanje, pa čak i inertnost kako pravosudnih organa tako i banaka. Dakle, evidentna je ova bojazan.

Pitanje broj sedam se odnosilo na to da ispitanici ocjene od čega zavisi bezbjednost platne kartice. Analizom odgovora uočeno je da je najveći broj ispitanika, 40%, mišljenja da bezbjednost njihove platne kartice zavisi od zaštite PIN kodom. Takođe, znatan broj ispitanika je mišljenja da od samog, odnosno ličnog rukovanja sa platnim karticama praktično zavisi bezbjednost od zloupotrebe a takvih ispitanika je bilo 28%. Uputstva banke kao odgovor ponudilo je 18% ispitanika a informisanost 14% . U tom smislu možemo zaključiti da je kod građana izražena želja za informisanosti i želja za uputstvima banaka u pogledu zaštite platnih kartica. Dakle, u ovom smislu građani nisu nezainteresovani i inertni, već

postoji potreba za spoznajom većeg stepena samozaštite kako se ne bi i sami građani viktimizirali i time doprinijeli da postanu žrtve krađe i zloupotrebe.

Pitanje broj osam je glasilo:“ Od čega strahujete kada su u pitanju zloupotrebe platnih kartica?“. Dobijeni rezultati prikazuju da se građani zapravo najviše boje zloupotrebe kada je riječ o krađi u vezi sa platnom karticom i to u procentu 36%. Krađa putem Interneta je odgovor koji je ponudilo 30% ispitanika. Bojazan od gubitka kartice odgovor je zabilježen u procentu 14% a odgovor u kojem građani strahuju od zloupotrebe u vezi sa PIN kodom je prisutan kod 20% ispitanika. Da su građani edukovani u smislu upotrebe i korištenja platnih kartica govori nam i podatak da se kod građana pojavljuje i strah zloupotrebe platnih kartica i kada je kupovina putem interneta u pitanju. U tom smislu, uočljivo je da građani koriste internet gdje se putem određenih sajtova opredjeljuju za kupovinu određenih proizvoda.

Pitanje broj devet je postavljeno tako da nudi pozitivan ili negativan odgovor na prisutnost platne kartice u društvu a rezultati gdje 62% ispitanika tvrdi da ona nije dovoljno prisutna u društvu govori da se u budućnosti od strane građana očekuje njeno veće prisustvo.

Posljednje deseto pitanje je postavljeno na sljedeći način:“ Da li biste radije koristili platne kartice ili gotov novac?“. Odgovori koji su dobijeni su da je 32% ispitanika opredjeljeno za gotov novac a 68% za platne kartice. Dakle, jasno je da su se građani opredijelili za evolutivne promjene u pogledu inovacija u tehničko-tehnološkom smislu, a naročito kada se radi o novcu i posebnim olakšicama u pogledu raspolaganja sa novcem, a što i sam sistem korištenja platnih kartica to i dozvoljava. Zapravo ovim poslednjim odgovorom, odnosno njegovom analizom, zaokružili bi jedno cijelo poglavlje koje ovom radu praktično i daje pečat opravdanosti u pogledu naučno-stručnog istraživanja gdje se izvodi zaključak da je ova tema još nedovoljno istražena, odnosno da osavremenjavanjem tehničko-tehničkih dostignuća postoji velika mogućnost zloupotreba i prevara u ovoj oblasti, te da se različitim načinima, metodama i saradnjom različitih organa cjelokupnog sistema, treba ukazati “običnom” građaninu na najbolje mogućnosti samozaštite.

7. ZAKLJUČAK

U smislu rasprostranjenosti i rastućeg trenda upotrebe platnih kartica, nužno se javlja i mogućnost njenih zloupotreba pa nije teško izvesti zaključak da je i kriminalitet koji se ogleda u prevarama i zloupotrebama s platnim karticama, u trendu ubrzanog razvoja, što ozbiljno upozorava. Ova vrsta kriminaliteta sve više dobija na masovnosti a sada već predstavlja ozbiljno stanje koje od svih faktora u društvu zahtjeva sveobuhvatan pristup izučavanju ove problematike. Sa kriminalističkog aspekta potrebno je obratiti pažnju na pitanja:šta je sve potrebno da se zaštiti u poslovanju sa platnim karticama,od koga ili od čega kartičarstvo treba zaštiti, zašto i kojim sredstvima je ovaj vid bezgotovinskog načina plaćanja potrebno zaštititi. Takođe se da zaključiti da je za izvršenje krivičnog djela falsifikovanje i zloupotreba platnih kartica neophodno poznavanje najprije tehnike i tehnologije korišćenja platnih kartica, što nam govori da je ovaj oblik privrednog kriminaliteta, kriminalitet profesionalaca i specijalista. U vršenju ovog krivičnog djela, takođe je neophodna zloupotreba savremenih tehničko-tehnoloških dostignuća, te stoga možemo reći da se ovaj oblik

privrednog kriminaliteta odlikuje karakateristikama visokotehnološkog kriminaliteta. Naime, za falsifikovanje i zloupotrebe platnih kartica kriminalci se koriste savremenim metodama zasnovanim na naučnim dostignućima i najnovijim pronalascima u oblasti elektronskog bankarstva, što umnogome otežava otkrivanje, razjašnjavanje i dokazivanje ovog vida kriminalnog ispoljavanja.

Za bezbjedno i uspješno funkcionisanje platnih kartica neophodni su savremeni tehnički uređaji za uspješno obavljanje novčanih transakcija (ATM, POS, kompjuteri, video i nadzor od zloupotreba i dr.), kvalitetna organizacija i dobro obučeni kadrovi banaka, kao i kvalitetno sačinjeni programi za bezbjedan rad i funkcionisanje svih u sistemu ovog načina poslovno-tehničkog funkcionisanja, novčanih transakcija i bezgotovinskog načina plaćanja, evidentiranje podataka i dobro razrađen monitoring sistem, kao i drugi vidovi preventivne zaštite.

Efikasno suzbijanje i prevencija kriminala zloupotreba i falsifikovanja platnih kartica zahtjeva moderan zakonodavni okvir, dobru organizaciju, obučenost i opremljenost organa otkrivanja i gonjenja ove vrste krivičnih djela.

Takođe, na smanjenje rizika od viktimizacije koja se odnosi na zloupotrebu u oblasti platnih kartica uveliko i gotovo u potpunosti može da doprinese sam njezin korisnik, odnosno vlasnik. U tom smislu možemo zapravo reći da se veći dio tereta koji se odnosi na mogućnosti zloupotrebe platnih kartica zapravo odnosi na ponašanje njenog korisnika odnosno vlasnika. Obzirom da je širok spektar načina i mogućnosti zloupotrebe platnih kartica, kao savjeti i preporuke u cilju izbjegavanja situacije viktimiziranosti može se reći sljedeće: platnu karticu je potrebno čuvati na ili u mjestu gdje samo korisnik ima pristup, PIN kod koji ja zapisan trebao bi biti odvojen od kartice, kartica mora da bude u neprestanom posjedu i pod kontrolom korisnika, preporučljiva je promjena PIN koda koji je dobijen od banke, koverat sa PIN kodom čuvati u tajnosti, stari PIN kod koji se nalazi na koverti učiniti neupotrebljivim, biti oprezan kod korištenja bankomata (sumnjiva lica u blizini ili sumnjiv izgled bankomata treba da utiču da se odustane od transakcije).

Kada se govori o zloupotrebama platnih kartica u otkrivanju, rasvjetljavanju i dokazivanju ovih krivičnih djela, kao i njihovih izvršilaca trebalo bi da budu uključeni svi raspoloživi subjekti u cilju uspješnog pokretanja, vođenja i okončanja krivičnog postupka krivičnih djela iz oblasti kartičarstva i kartičnog poslovanja. Veoma je bitna saradnja policijskih službenika i nadležnog tužilaštva, kao i nadležnih sudova zajedno sa bankama, te u tom smislu potrebna je harmonizacija ovih odnosa.

LITERATURA

Barać, S., Stakić, B., Hadžić, M., Ivaniš, M.(2007). *Praktikum za bankarstvo*. Beograd: Univerzitet Singidunum, 130.
Ivanović R. A.(2011). Falsifikovanje i zloupotreba platnih kartica, *Perjanik., Časopis za teoriju i praksu u oblasti kriminalistike, bezbijednosti, kriminologije i prava*, 4.
Jovičić, D.(2011). *Javna bezbjednost*. Banja Luka: Fakultet za bezbjednost i zaštitu, 207-216.
Kresoja,M., Kirkov, Z. (2008). Primjena savremenih metoda i sredstava u suprotstavljanju kriminalitetu u oblasti zloupotrebe platnih kartica, *Internacionalna asocijacija kriminalista, Zbornik radova*, 510-512.
Kresoja, M., Kirkov, Z. (2009). *Primjena savremenih metoda i sredstava u suprotstavljanju kriminalitetu u oblasti zloupotrebe platnih kartica*. Novi Sad, 499.
Miller, R. L., VanHoose, D. D.(1997), *Moderni novac i bankarstvo*. Zagreb: Mate, 63.
Nellie, L. (2013). Credit and Banking. *Journal of Money vol.45*, 129-135.
Službeni glasnik Republike Srpske, broj 49, od 25. juna 2003. godine.
Živković, A., Stanković, R., Krstić, B.(2008). *Bankarsko poslovanje i platni promet*. Beograd: Centar za izdavačku djelatnost Ekonomskog fakulteta u Beogradu, 414.
Berg, B. (2007). *Criminal investigation*. New York: The McGraw-Hill Companies, 327.

Internet
http://www.tuzilastvobih.gov.ba/files/docs/zakoni/Krivicni_zakon_lat_RS_49_03.pdf(Pristup: 07.02.2016.godine).

Goran Guska
Goran Blagojević

MODERN METHODS AND RESOURCES IN COMBATING PAYMENT CARDS ABUSE

Summary

Rapid advancements in technical and technological achievements have rendered payment in coins and notes obsolete giving rise to contemporary non-cash payment instruments and money transactions.
One of these instruments is the payment card which represents one of the most popular means of payment in developed countries. The emergence and growing use of payment cards resulted in first cases of their abuse, which is one of the modern methods of gaining illegal profit. The rapid development of electronic banking and credit card payment system has led to increased numbers of users of this type of banking services, which, on the other hand, has created infinite possibilities of diverse types of payment card abuses.
The paper discusses payment cards in general with special reference of their abuse. Also to be discussed are legal and criminal aspects of this phenomenon. With the results of the survey research conducted, we will try to offer some solutions for combating this kind of abuse.

Key words: *payment card, abuse, gain of illegal profit.*

STRUČNI RAD

Igor Špoljarić[188]
Ante Orlović[189]
Gordan Mršić[190]

IMPLEMENTACIJA VISOKE TEHNOLOGIJE U FORENZIČNO-KRIMINALISTIČKIM ISTRAŽIVANJIMA – SKENIRAJUĆI ELEKTRONSKI MIKROSKOP (STANJE I PERSPEKTIVE)

Sažetak

Forenzično-kriminalistička istraživanja kaznenih djela u suštini razumijevaju aktivnosti otkrivanja, osiguravanja i razjašnjavanja tragova koji mogu poslužiti kao dokazi u kaznenom postupku. Kod teških i složenih kaznenih djela ključnu ulogu često imaju mikrotragovi te su u svezi s istima potrebna adekvatna postupanja koja u pravilu razumijevaju uporabu uređaja visoke tehnologije. Učinci implementacije visoke tehnologije, u ovom slučaju skenirajućeg elektronskog mikroskopa, u područje forenzično-kriminalističkih istraživanja razmatrani su u kontekstu ispitivanja tragova pucanja iz vatrenog oružja provedenih u Centru za forenzična ispitivanja, istraživanja i vještačenja „Ivan Vučetić" MUP-a RH, za razdoblje od 2008. do 2015. godine. Uvođenje naznačenog uređaja u područje ispitivanja tragova pucanja, razmatrajući navedeno razdoblje, rezultiralo je značajnim promjenama glede broja i strukture naznačenih predmeta primljenih u rad Centra. Osim prethodnih iskustava i aktualnog stanja primjene skenirajućeg elektronskog mikroskopa u istraživanjima važno je razmotriti i perspektive njegove primjene u budućem razdoblju. U tom smislu iznesena su razmišljanja o potencijalnim mogućnostima implementacije predmetnog uređaja visoke tehnologije i u drugim područjima forenzično-kriminalističkih istraživanja (istraživanje algi kremenjašica u istraživanju kaznenih djela ubojstava i samoubojstava) jer se on u srodnim područjima već koristi – ali samo u znanstvene svrhe. Kontinuirani razvoj i implementacija visoke tehnologije može dovesti do razvoja i implementacije niza metoda koje bi mogle značajno pridonijeti razrješavanju i rasvjetljavanju specifičnih situacija/činjenica/okolnosti u slučajevima teških i složenih kaznenih djela.

Ključne riječi: *skenirajući elektronski mikroskop; tragovi pucanja iz vatrenog oružja; alge kremenjašice; ubojstvo i samoubojstvo.*

[188] Igor Špoljarić, bacc. crim., MUP-CFIIV „Ivan Vučetić", vještak za balistička i mehanoskopska vještačenja, e-mail: igor.spoljaric@gmail.com
[189] Dr. sc. Ante Orlović, profesor, Visoka policijska škola Zagreb, e-mail: aorlovic@gmail.com
[190] Doc. dr. sc. Gordan Mršić, MUP-CFIIV - načelnik CFIIV-a, e-mail: gmrsic@mup.hr

1. UVOD

Forenzično-kriminalistička istraživanja činjenica i okolnosti povezanih s kaznenim djelima i njihovim počiniteljima u suštini razumijevaju poduzimanje aktivnosti od strane ovlaštenih osoba glede otkrivanja, osiguravanja, ispitivanja, vještačenja i razjašnjavanja tragova, koji mogu poslužiti kao dokazi u kaznenom postupku. *Tragovi* u kriminalističkom smislu (Modly, Šuperina i Korajlić 2008:856) razumijevaju „materijalne promjene u objektivnoj stvarnosti koje su spoznate i koje su nastale u svezi ili povodom počinjenja ili pripremanja kaznenog djela i koje imaju određenu dokaznu vrijednost u postupku kriminalističke identifikacije". Tragovi se mogu klasificirati prema više relevantnih kriterija prema kojima se dijele na različite skupine i podskupine. U kontekstu implementacije visoke tehnologije u forenzično-kriminalističkim istraživanjima važni su mikrotragovi kao kategorija tragova koji se ne mogu detektirati i istraživati isključivo ljudskim osjetilima. *Mikrotragovi* su takva vrsta tragova (Modly, Šuperina i Korajlić 2008:406) čiji „informacijski sadržaj leži ispod podražajnog praga ljudskih osjetila i zbog toga se te kriminalistički relevantne promjene ne mogu opaziti osjetilima i čije se postojanje pretpostavlja, a koje mogu biti učinjene otkrivačko-dokazno gledajući korisnima tek primjenom specijalnih principa kriminalističko-tehničkog traganja, kao i razvijanjem metoda i sredstava za njihovo osiguranje i vrednovanje".

Tragovi, njihovo izuzimanje i interpretacija kao dokaz, najčešće su povezani sa sljedećim dokaznim radnjama propisanim Zakonom o kaznenom postupku (NN 121/11, 143/12, 56/13, 145/13, 152/14): pretraga, privremeno oduzimanje predmeta, ispitivanje svjedoka, prepoznavanje, očevid, uzimanje otisaka prstiju i otisaka drugih dijelova tijela, vještačenje. Očevidom se činjenice u postupku utvrđuju ili razjašnjavaju opažanjem vlastitim osjetilima i njihovim pomagalima (članak 304.). Vještačenje se određuje kad za utvrđivanje ili ocjenu neke važne činjenice treba pribaviti nalaz i mišljenje od osobe koja raspolaže potrebnim stručnim znanjem ili vještinom (članak 308.). Postupanje policije u svezi s tragovima propisano je i Zakonom o policijskim poslovima i ovlastima (NN 76/09, 92/14) kojim je uređeno da se kriminalističko istraživanje provodi, između ostalog, radi otkrivanja i osiguravanja tragova i predmeta koji mogu poslužiti pri utvrđivanju činjenica vezanih za kazneno djelo i njegova počinitelja (članak 2, st. 1, t. 7).

Glede problematike tragova, posebno mjesto u sustavu MUP-a zauzima Centar za forenzična ispitivanja, istraživanja i vještačenja "Ivan Vučetić". Prema Uredbi o unutarnjem ustrojstvu Ministarstva unutarnjih poslova (NN 70/12, 140/13, 50/14, 32/15), taj Centar je samostalna ustrojstvena jedinica koja potpuno neovisno obavlja poslove forenzičnih ispitivanja, istraživanja i vještačenja (identifikacijskih, kemijsko-fizikalnih, toksikoloških, kontaktnih, tehničkih), po nalogu državnog odvjetništva, suda i policije te na temelju sporazuma ili u okviru suradnje s drugim tijelima. Za obavljanje poslova iz djelokruga rada Centra za forenzična ispitivanja, istraživanja i vještačenja »Ivan Vučetić« ustrojavaju se sljedeće službe: Služba daktiloskopije i identifikacije, Služba bioloških i kontaktnih vještačenja, Služba kemijsko-fizikalnih i toksikoloških vještačenja, Služba traseoloških vještačenja, Služba općih i tehničkih poslova, Služba za ispitivanje, tormentaciju i žigosanje vatrenog oružja (članak 105.). Uspješan rad Centra uvjetovan je permanentnim uvođenjem novih tehnologija i uređaja u sferu kriminalističko-forenzičnih istraživanja i vještačenja koje djelatnici Centra obavljaju.

U svezi s navedenim, u ovom radu se razmatraju učinci implementacije visoke tehnologije (skenirajući elektronski mikroskop) u forenzično-kriminalističkom istraživanju kroz predmete vezane za vještačenje tragova pucanja iz vatrenog oružja za razdoblje od 2008. do 2015. godine. U svezi s navedenim potrebno je istaknuti da je početkom 2007. godine objavljen članak (Mršić i Žugaj, 2007) o upotrebi skenirajućeg elektronskog mikroskopa u analizi tragova pucanja, čime je započela edukacija i informiranje svih policijskih službenika u svezi s mogućnostima primjene navedene tehnologije. U drugom dijelu rada prezentirana je mogućnost analize algi kremenjašica u istraživanju kaznenih djela ubojstava u kontekstu moguće primjene skenirajućeg elektronskog mikroskopa u svezi s tom problematikom (Mršić i Žugaj, 2007).

2. SKENIRAJUĆI ELEKTRONSKI MIKROSKOP (AKTUALNOSTI) – ANALIZA TRAGOVA PUCANJA IZ VATRENOG ORUŽJA

Tragovi pucanja iz vatrenog oružja mogu se naći na oružju, čahuri, zrnu, osobi koja je oružje uporabila, osobi prema kojoj je oružje uporabljeno, okolnim predmetima. Tragovi pucanja, između ostalog, dijele se na organske i anorganske.

Organski tragovi pucanja (Mršić i Žugaj, 2007) poznatiji kao baruti, dokazuju se pomoću "Gonzalesovog testa" poznatog i kao "parafinska rukavica" (Slika 1). Metoda se sastoji od nanošenja silikonske smjese na šake, te naknadnog skidanja ohlađene i stvrdnute "rukavice". Čestice baruta dokazuju se u laboratoriju gdje vještak tretira silikonske odljevke difenilaminskim reagensom za dokazivanje nitrata koji su sastavni dio baruta. Ukoliko je uzorak pozitivan, pojavljuje se karakteristično tamnoplavo obojenje. Kako su nitrati sastavni dio baruta kojim se puni moderno streljivo, ukoliko difenilaminski reagens dođe u kontakt s nitratima iz baruta, doći će do kolorne reakcije, tj. nastat će obojenje karakteristične tamnoplave boje. Nakon provedene kemijske analize tragovi se više ne mogu analizirati. Takva metoda je nedestruktivna i između ostalih nedostataka nije prihvatljiva suvremenom načinu dokazivanja tragova bez mogućnosti ponavljanja analize od strane druge stručne osobe ili druge stručne ustanove. Rezultat takve vrste vještačenja je samo indicija, a ne materijalni dokaz jer nitrata, osim u barutu, ima i u cijelom nizu drugih tvari kao što su pepeo, mokraća, deterdženti, umjetna gnojiva i sl. Stoga se može dogoditi da se na vještačenju dobije lažno pozitivan rezultat (Mršić i Žugaj, 2007). Na primjeru iz sudske prakse (Presuda Vrhovnog suda Republike Hrvatske: Broj: I Kž 904/04-8) vidljiva je nepouzdanost Gonzalesovog testa.

Potencijalni tragovi pucanja iz vatrenog oružja najčešće se izuzimaju s ruku i odjeće osumnjičene osobe. S oštećene osobe (žrtve) tragovi se najčešće izuzimaju s odjeće, ovisno o udaljenosti osobe od

usta cijevi vatrenog oružja iz kojeg je pucano. U nešto manje slučajeva tragovi se izuzimaju s ruku, iz ulazne rane na tijelu ili nekih drugih predmeta (automobilski prozori i upravljač, rukavice, kape i sl.) koji prema procjeni mogu biti kontaminirani tragovima pucanja iz vatrenog oružja.

Slika 1: Dio opreme provođenje Gonzales-ovog testa

Slika 2: Nanošenje Optosil smjese na ruke

Teodoro Gonzales iz Mexico City policijskog laboratorija, je 1933. godine uveo test na nitrate pomoću parafina kao standardnu metodu za organske tragove pucanja iz vatrenog oružja. Kasnije je metoda usavršena i uveden je test pomoću difenilaminskog reagensa, ali osnova je ostala ista, a to je parafinska rukavica (Slika 2). Difenilaminski reagens pokazuje tamno plavo obojenje (slika 3) nitratnih skupina u djelomično izgorenim i neizgorenim česticama baruta (Cowan i Purdon, 1967). Takav test daje dobru informaciju o razmještaju čestica na rukama jer nam upravo parafinska rukavica preslikava pozicije čestica na šakama.

Slika 3: Odljevak s kolornom reakcijom nakon tretiranja difenilaminskim reagensom

Harrison i Gillroy su 1959. godine razvili kolorimetrijski test za identifikaciju metala, dakle anorganskog dijela tragova pucanja, i to na olovo (Pb), barij (Ba) i antimon (Sb) koji su u oblicima olovo stifnat, barij nitrat i antimon sulfid korišteni kao spojevi inicijalne smjese (engl. Primer). Tada su prvi put potencijalni tragovi izuzimani brisanjem (engl. swabbing) pamučnom vatom (Harrison i Gilroy, 1959). Velika prednost natrij rodizonat testa nad do tada poznatim testovima bilo je smanjenje lažno pozitivnih rezultata. U narednom razdoblju

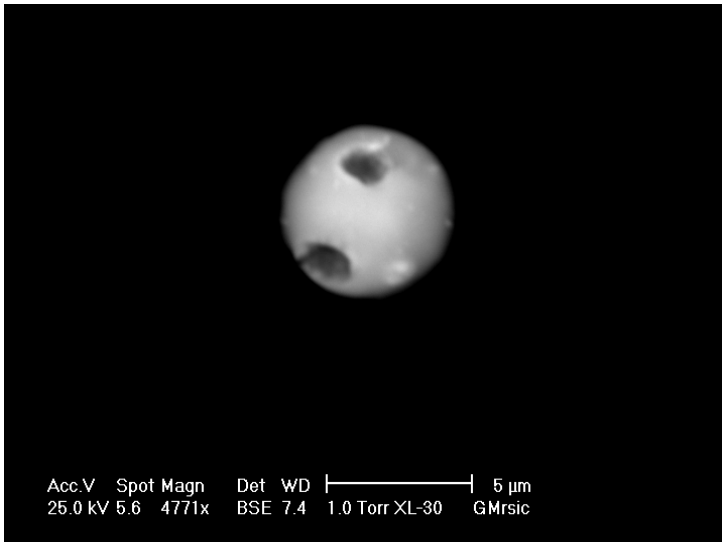
forenzičari su sa više pažnje istraživali anorganske tragove pucanja u potrazi za osjetljivijim tehnologijama detekcije kemijskih elemenata kao što su olovo, barij i antimon.

Instrumentalna tehnika, neutronska aktivacijska analiza (NAA, neutron activation analysis), uvedena je u praksu 1962. godine, u svrhu identifikacije barija i antimona (Ruch i sur., 1964). Rezultat analize nije kolorno obojenje koje je ovisno o prisutnosti metala, nego se kvantitativno mjeri koncentracija metala na rukama. Najveći problem bio je odrediti početne koncentracije metala na rukama osoba koje su koristile vatreno oružje kao i koncentraciju metala na rukama osoba koje nisu koristile oružje. Barij se može naći u prirodi i u sastavu zemlje, tako da nije bilo moguće točno odrediti izvor pozitivnog rezultata, tj. radi li se o metalima povezanih s tragovima pucanja ili se radi o kontaminaciji uzorka, u konačnici lažno pozitivan rezultat.

Gotovo 10 godina kasnije, 1971. godine, uvedena je metoda atomske apsorpcijske spektrometrije (AAS, atomic absorption spectrometry) (Krishnan, 1971), također za određivanje koncentracije metala. Kao i kod metode NAA, problemi su ostali identični, a to je određivanje granične koncentracije za pozitivan ili negativan rezultat i porijeklo pronađenih metala. Istraživanja pomoću skenirajućeg elektronskog mikroskopa započinju 1968. u Engleskoj (Heard, 1997), a 1971. godine prezentirana je prva snimka anorganske čestice tragova pucanja (Boehm, 1971). Prvi radovi su prezentirani 1975. godine i od tada kreće tehnološki napredak u istraživanju tragova pucanja iz vatrenog oružja pomoću SEM-a.

Anorganski tragovi pucanja (Mršić i Žugaj, 2007) iz vatrenog oružja (engl. Gunshot residue) nastaju eksplozijom sastava inicijalne smjese (olovo stifnat, barij nitrat i antimon sulfid) streljiva, te uslijed visoke temperature i visokog tlaka nastaju sferne ili okrugle čestice (Slika 4), elementnog kemijskog sastava olovo, barij i antimon. Čestice su veličine od 500 nm do 10 mikrometara a nerijetko nastaju i veće čestice do 50 mikrometara. U svrhu pronalaska, dokazivanja i karakterizacije takvih čestica koristi se oprema visoke tehnologije - skenirajući elektronski mikroskop (SEM) (Slika 5).

Anorganski tragovi pucanja mogu se klasificirati kao indikativni i karakteristični. Indikativne čestice se sastoje od jednog ili najčešće dva kemijska elementa od sastava inicijalne smjese, tako da mogu biti sastavljene od: antimona (Sb) i barija (Ba), barija (Ba) i olova (Pb), antimona (Sb) i olova (Pb). Čestice koje se nazivaju karakteristične su čestice one koje se sastoje od tri glavna elementa nastalih od sastava inicijalne smjese, a to su olovo (Pb), barij (Ba) i antimon (Sb). Karakteristične i indikativne čestice moraju biti sfernog ili okruglog oblika i moraju biti određenih dimenzija do cca 50 μm, iznimno i više, (Romolo i Margot, 2001).



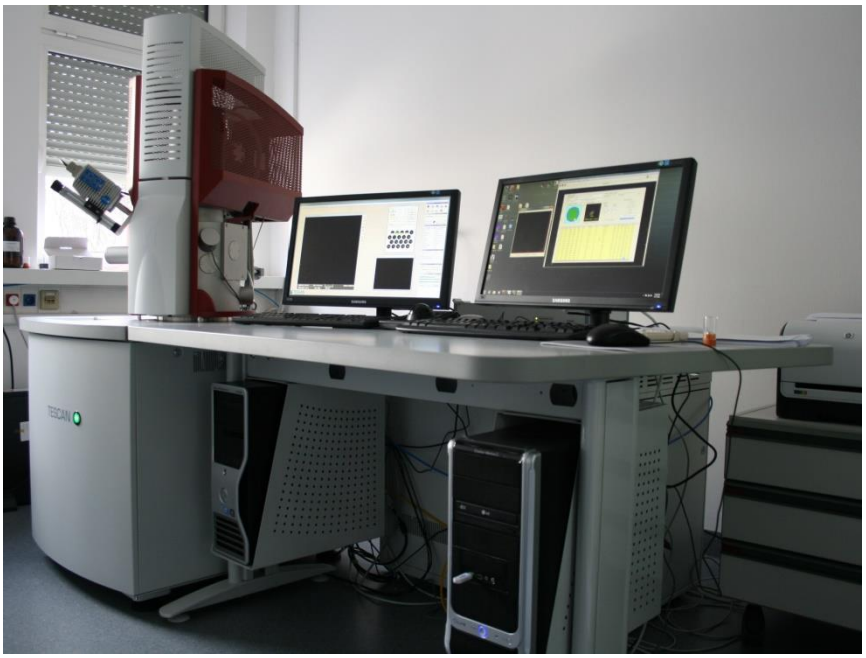
Slika 4: Anorganski tragovi pucanja (tzv. GSR čestice) snimljene skenirajućim elektronskim mikroskopom (SEM) u CFIIV "Ivan Vučetić

Način izuzimanja čestica za predmetnu mikroskopsku analizu je vrlo specifičan jer se čestice golim okom ne vide, pa to zahtijeva vrlo veliku stručnost i profesionalnost osoba koje izuzimaju tragove.

Tragovi se izuzimaju pomoću specijalnih ljepljivih traka koje se još nazivaju u GSR stub-ovi (Slike 5 i 6). Te tragove na mjestu događaja izuzimaju kriminalističkih tehničara, a u laboratoriju djelatnici CFIIV-a. Tragovi koji su prikupljeni na površini ljepljive trake i nakon analize ostaju nepromijenjeni i očuvani za eventualnu ponovnu analizu. Još jedna od prednosti metode analize tragova uporabe vatrenog oružja pomoću SEM-a je i nedestruktivnost tragova, za razliku od ostalih metoda (Gonzalesov test, NAA, AAS i dr.)

Slika 5: GSR stub sa zaštitnim poklopcem i zaštitnom folijom (izvor: CFIIV "Ivan Vučetić")

Slika 6: Postupak izuzimanja tragova sa ruku osobe pomoću GSR stub-a (izvor: CFIIV "Ivan Vučetić")



Slika 7: Skenirajući elektronski mikroskop sa EDX detektorom u Centru za forenzična ispitivanja, istraživanja i vještačenja "Ivan Vučetić"

Nabavnom skenirajućeg mikroskopa sa EDX detektorom (Mršić i Žugaj, 2007), u forenzično-kriminalističkim istraživanjima 1998. godine se počinje uvoditi metoda analize anorganskih tragova pucanja iz vatrenog oružja, koja punu primjenu doživljava 2008. godine. Radi osiguranja kvalitete analize i njenih rezultata, Centar "Ivan Vučetić" 2007. godine pokreće proces akreditacije metode za dokazivanje anorganskih tragova pucanja, tzv. GSR čestica pod nazivom SEM-EDX metoda tragova pucanja. Metoda je akreditirana po međunarodnoj normi HRN EN ISO/IEC 17025:2007, što svrstava Centar u razred s ostalim vodećim svjetskim laboratorijima. Nadogradnjom SEM-a 2007. godine i kupnjom novog, tehnološki naprednijeg SEM-a 2011. godine, te sustavnom edukacijom djelatnika Centra postalo je moguće kvalitetnije provesti analizu i interpretirati podatke nego što je to bilo, primjerice, 2004. godine, dok je cjelokupna metoda bila u fazi uvođenja. U dijelu presude Vrhovnog suda Republike Hrvatske možemo vidjeti neselektivnost i površnost u interpretaciji rezultata GSR analize "*Na temelju balističkog vještačenja (vještak V. M., list 710-711 spisa) na dva gornja dijela trenirke opt. M. Š. nije dokazano prisustvo niti jedne GSR čestice, koje potječu isključivo iz pucanja vatrenim oružjem, a dokazani su tragovi dvokomponentnih čestica, koje u indikativne za pucanje, ali mogu nastati i na druge načine – primjerice prilikom kočenja automobila ili sagorijevanjem tehničkih masa kojima se pune petarde, baklje ili slična pirotehnička galanterija. Prema nalazu i mišljenju istog vještaka dvokomponentne čestice mogu se na odjeći zadržati relativno dugo, ovisno o tome kako se s odjećom postupalo, više mjeseci, pa čak i više godina i stoga se nije moglo vremenski preciznije utvrditi kada su dvokomponentne čestice kontaminirale gornje dijelove trenirki opt. M. Š., da li kritične zgode ili prije toga. Optuženik je inače ranije posjedovao pištolj „Češka Zbrojevka. Iz njegove obrane proizlazi da je često odlazio na pucanje u kamenolom i to obično u trenirkama.* (Presuda Vrhovnog suda Republike Hrvatske: Broj: I Kž 904/04-8). Naime, dvokomponentne

čestice nastale od automobilskih kočnica pomoću SEM-a i elementne kemijske analize mogu se vrlo jednostavno i razlikovati od dvokomponentnih čestica koje potječu od inicijalne smjese vatrenog oružja.

2.1. Obilježja predmeta primljenih u Centru „Ivan Vučetić“ tijekom 2008-2015. godine

Puni opseg primjene GSR analize (engl. Gunshot residue) pomoću skenirajućeg elektronskog mikroskopa (SEM) u Centru počinje 2008. godine. Zaprimaju se tragovi izuzeti sa šaka osumnjičene i/ili oštećene osobe, odjeća koja je povezana s događajem ili se sumnja da na odjeći postoje potencijalni tragovi pucanja i drugi predmeti na kojima također mogu biti tragovi. U 2008. godini zaprimljen je 151 predmet iz područja tragova pucanja iz vatrenog oružja (Tablica 2). Već 2010. godine, broj zaprimljenih predmeta je porastao za 10% (166 predmeta). Stupanjem na snagu novog Zakona o kaznenom postupku (NN 121/11.) broj primljenih predmeta u 2012. godini pada na 80, što je smanjenje u odnosu na prethodnu 2011. godinu za 56%. Konkretno, broj samoubojstava vatrenim oružjem na godišnjoj razini u razdoblju 2008.-2015. nije se značajno smanjivao da bi utjecao na smanjenje primljenih predmeta (Tablica 1).

Tablica 1: Broj dovršenih i nedovršenih samoubojstava vatrenim oružjem u RH u razdoblju 2008-2015. godine

godina	2008.	2009.	2010.	2011.	2012.	2013.	2014.	2015.
broj predmeta	127	133	111	103	122	110	104	89

Proizlazi da sudac istrage traži vještačenje tragova pucanja iz vatrenog oružja samo u određenim, specifičnim, prijeko potrebnim slučajevima. Tako je do 2012. godine, osim državnog odvjetništva i policija mogla zatražiti vještačenje temeljem zahtjeva za vještačenje, no izmjenama Zakona o kaznenom postupku, nakon 2012 godine, samo tužitelj može zatražiti vještačenje temeljem naloga (članak 308. ZKP-a) "Vještačenje se određuje kad za utvrđivanje ili ocjenu neke važne činjenice treba pribaviti nalaz i mišljenje od osobe koja raspolaže potrebnim stručnim znanjem ili vještinom" (Zakon o kaznenom postupku, “Narodne novine”, br. 152/14). Iz tablice 2, vidljivo je smanjenje broja zaprimljenih predmeta.

Tablica 2. Predmeti za područje tragova pucanja primljeni u razdoblju 2008-2015. godine

godina	2008.	2009.	2010.	2011.	2012.	2013.	2014.	2015.
broj predmeta	151	132	166	141	80	91	52	47

Osim tragova pucanja izuzetih s ruku osumnjičenih i oštećenih osoba, u Centar Ivan Vučetić dostavljaju se i organski tragovi pucanja za Gonzales-ovu metodu (Tablica 3), zatim odjeća sa koje se izuzimaju organski i anorganski tragovi pucanja (Tablica 4).

Tablica 4. Uzorci za analizu tragova pucanja izuzeti Gonzales-ovim testom – primljeni u razdoblju 2008-2015. godine

godina	2008.	2009.	2010.	2011.	2012.	2013.	2014.	2015.
broj predmeta	473	580	402	339	266	256	149	156

Tablica 5. Odjeća za analizu na tragove pucanja primljena u razdoblju 2008-2015. godine

godina	2008.	2009.	2010.	2011.	2012.	2013.	2014.	2015.
broj predmeta	84	273	259	230	179	159	134	100

Sustavnom edukacijom kroz seminare kao i zajedničkim radom na rješavanju predmeta i radom na mjestu događaja, policijski službenici dobivanju *nova saznanja i informacije* o mogućnostima rezultata analize na tragove pucanja iz vatrenog oružja. Iz tih razloga raste broj analiziranih uzoraka (GSR stub-ovi) za svaki pojedini predmet (Tablica 5) u odnosu na stanje iz 2008 godine. Broj dostavljene odjeće za utvrđivanje tragova pucanja također je porastu (Tablica 6).

Tablica 6. Omjer broja primljenih predmeta i broja GSR stub-ova (analiziranih uzoraka)

godina	2008.	2009.	2010.	2011.	2012.	2013.	2014.	2015.
broj predmeta	5,42	7,17	7,66	6,98	14,20	9,69	10,38	11,77

Tablica 7. Omjer broja primljenih predmeta i odjeće s potencijalnim tragovima dostavljenih na analizu tragova pucanja

godina	2008.	2009.	2010.	2011.	2012.	2013.	2014.	2015.
broj predmeta	0,56	2,07	1,56	1,63	2,24	1,75	2,58	2,13

Premda je smanjen broj primljenih predmeta (Tablica 2) svaki predmet ima više priloga/materijala tj. veći broj osumnjičenih osoba, odjeće i ostalih materijala za vještačenje povezanih s počiniteljem, s oštećenom osobom i s mjestom događaja. Ponekad su tragovi pronađeni na odjeći (*Povezujući ove indikativne okolnosti s činjenicom da su samo na odjeći oba optuženika nađene čestice GSR (ostaci inicijalnog punjenja;* Presuda Vrhovnog suda Republike Hrvatske: Broj: I Kž 757/10-7.) jedini tragovi pucanja i predstavljaju vrijedan dokaz u postupku pred sudom. Osim utvrđivanja postojanja tragova pucanja, u nalogu za vještačenje postavljaju se i dodatna pitanja koja bi mogla bolje povezivati tragove sa mogućim hipotezama u istraživanju ili istražiteljima dala dodatnu informaciju za usmjeravanje istrage. U Tablici 5. vidljivo je povećanje omjera primljenih predmeta i broja

GSR stub-ova po predmetu, u 2015. godini u odnosu na 2008. godinu za više od 100%. U Tablici 6 vidljivo je povećanje broja odjevnih predmeta koji su povezani sa tragovima pucanja iz vatrenog oružja po predmetu, i to u 2015. godini u odnosu na 2008. godinu za više od 400%.

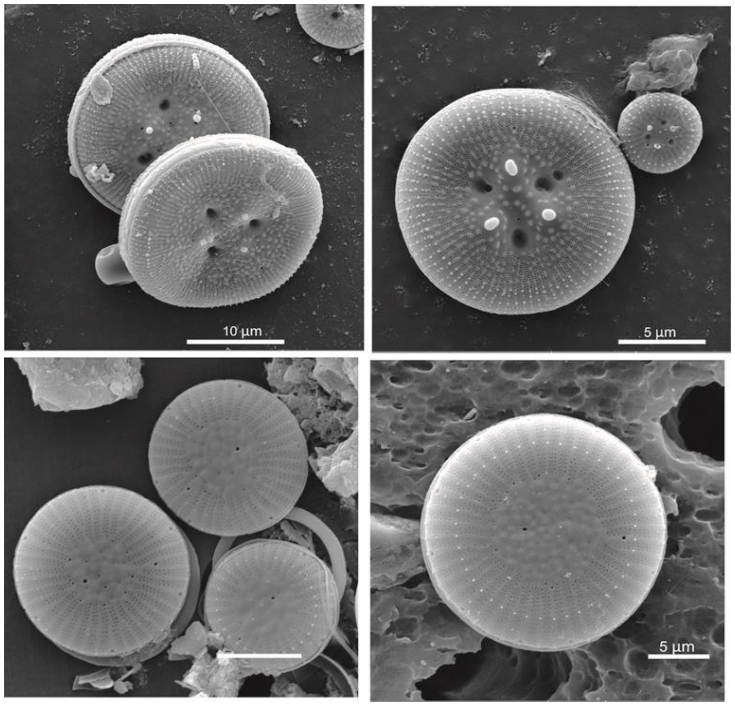
Metoda pomoću SEM-a je do sad najučinkovitija i najpouzdanija metoda za pronalazak i detekciju anorganskih tragova pucanja iz vatrenog oružja. Rezultat analize povezuje proces pucanja iz vatrenog oružja i osobu na kojoj su pronađene čestice (osoba je bila u kontaktu sa vatrenim oružjem ili na mjestu događaja) a u nekim slučajevima može je i direktno povezati sa vatrenim oružjem tj. da je ta osoba pucala iz vatrenog oružja. Zahvaljujući metodi pomoću SEM-a, rezultat analize materijalni je dokaz za razliku od ostalih testova (Gonzalesov test, NAA, AAS) kod kojih je rezultat analize samo indicija. Metoda nije destruktivna, što znači da sama analiza ne mijenja i ne uništava tragove te je druga stručna ustanova može ponoviti. Sve više primljenih predmeta ima specifične zahtjeve i pristup "case-by-case" a metoda pomoću SEM-a daje adekvatne rezultate za takav pristup rješavanju problema.

3. SKENIRAJUĆI ELEKTRONSKI MIKROSKOP (PERSPEKTIVA) – DETERMINACIJA ALGI KREMENJAŠICA KOD ISTRAŽIVANJA UBOJSTAVA I SAMOUBOJSTAVA

Alge kremenjašice ili diatomeje su jednostanični organizmi. Stanična jezgra im je građena od silicijevog oksida. Do sada je poznato oko 10 000 vrsta diatomeja, razvrstanih u 174 roda, različitih oblika i veličina (od 1 μm do 500 μm). Mogu se naći na kopnu, u stajaćim i tekućim vodama. U morima su zastupljenije u hladnijem dijelu godine. S obzirom na strukturu dijele se na Centricae (imaju radijalnu strukturu u odnosu na centralnu točku) i Pennatae (izdužene). Alge kremenjašice mogu se koristiti u kriminalističko-forenzičnoj znanosti pri otkrivanju zločina, povezivanju osumnjičenih osoba s mjestom događaja ili pak eliminiranju naznačene povezanosti. Prvenstveno zbog svoje jedinstvene građe, velike raznolikosti vrsta te činjenice da su kao materijal dosta vjerodostojne, kremenjašice mogu biti višestruki dokaz, jer se pojavljuju u određenim ekosustavima u određeno vrijeme, a njihove ljušturice nisu podložne raspadanju ili razgradnji. Kao materijalni dokaz u forenzici alge kremenjašice najviše se koriste u slučajevima utapanja osoba (Singh, Singh & Thakar, 2006). Kriminalističko-forenzični značaj i status testiranja i analiziranja diatomeja prilikom istraživanja kaznenog djela ubojstva u forenzici je dvojako, od toga da su diatomeje jedini pravi forenzični dokaz utapanja pa sve do mišljenja o testu na diatomeje kao „pseudoznanosti“ zbog učestalosti lažno pozitivnih rezultata testa. I forenzična je patologija, povijesno gledano, podijeljena u općem prihvaćanju diatomskog testa kao konačan dijagnostički test (Kumar, Deshkar, Naik & Yadav, 2012).

Nedostatak znanja i kontroverze čine ovaj test ograničenih vrijednosti i postavlja se pitanje o njegovu prihvaćanju. Test na diatomeje je test koji se temelji na teoriji da ljudi obično nemaju značajan broj diatomeja u nekim važnim organima poput bubrega, mozga, koštane srži i sl., ali ako se osoba utapa u vodi koja sadrži diatomeje, iz te vode diatomeje će stići do pluća i neke od njih će prodrijeti do alveolarnih zidova. Ako srce i dalje kuca, diatomeje koje

su ušle u krvotok mogu doprijeti i do udaljenijih organa kao što su bubrezi, mozak i koštana srž i prije smrti. Povećani broj diatomeja u unutarnjim organima je potvrda da se tijelo utopilo. S druge strane, ako je već mrtvo tijelo palo u vodu, diatomeje su mogle doći u pluća pasivnim putem ali diatomeje ne bi mogle ući u krvotok i ne bi trebale biti prisutne u udaljenim organima (Kumar, Deshkar, Naik & Yadav, 2012). Prednost ove metode je da se može koristiti čak i kod mrtvih tijela kod kojih je započeo proces truljenja (ispituju se zaštićena tkiva, kao što je koštana srž). Nažalost, test na diatomeje je često negativan, čak i u nedvojbenih slučajeva utapanja u plovnim putevima punih dijatomeja, a tu su i brojni lažno pozitivni rezultati (Krstic et al., 2002). Na Slici 8 su prikazane dvije vrste diatomeja iz jezera Visovac i Vranskog jezera. Radi se o vrstama *Cyclotella ocelata i Cyclotella cyclopuntata.*

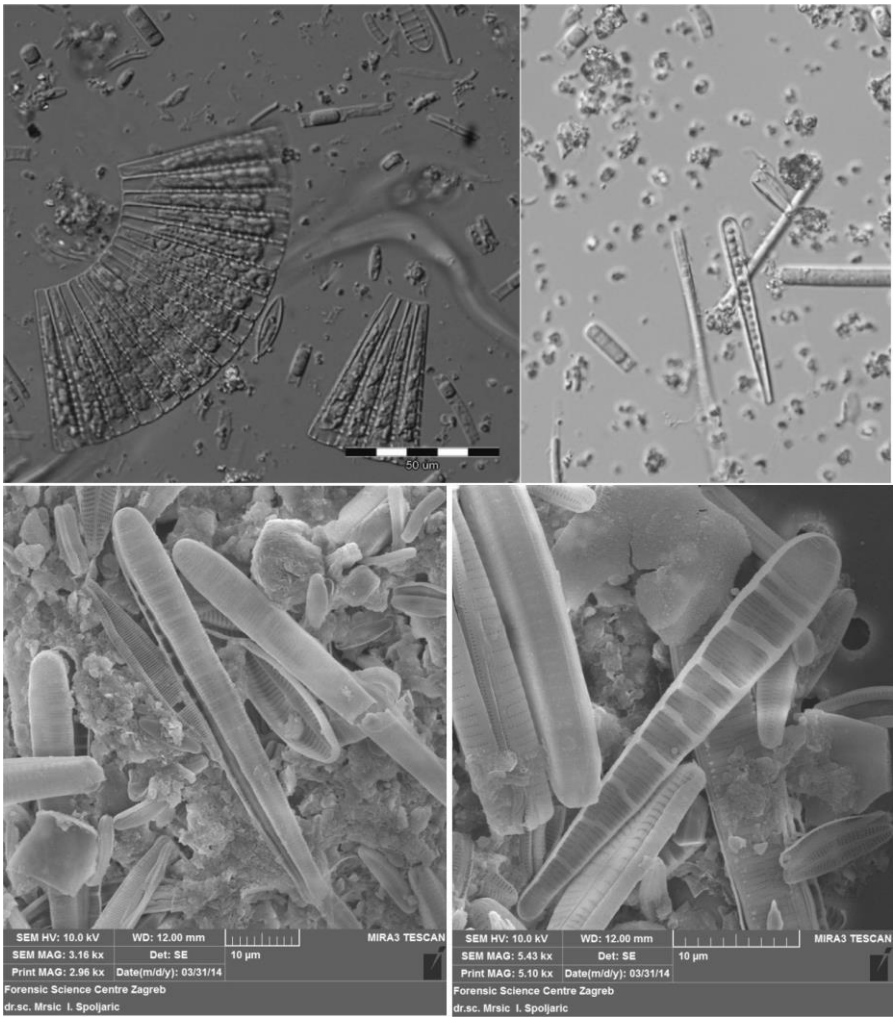


Slika 8: Diatomeje vrste Cyclotella ocelata i Cyclotella cyclopuntata

Diatomeje se mogu izuzimati i s odjeće (Uitdehaag, 2010) koja je bila u vodi ili u kontaktu s vodom. Takva informacija može biti od značaja u istraživanju ubojstava kao poveznica osumnjičenih osoba s određenim lokacijama. Michael Pollanen (Pollanen, 1998) je istraživao diatomeje u šest slučajeva ubojstava utapanjem. U svih šest slučajeva diatomeje su izuzete iz koštane srži. U pet slučajeva izuzete diatomeje iz koštane srži su uspoređivane s uzorcima diatomeja iz diatomejama vode mjesta utapanja. U svim slučajevima ista vrsta diatomeja se nalazila u koštanoj srži i vodi s mjesta utapanja. U dva od šest slučajeva tijela su nađena na zemlji, a jedno tijelo je pronađeno na zemlji i zapaljeno nakon smrti.

Tehnološki gledano, analiza i diferencijacija dijatomeja je gotovo nezamisliva bez upotrebe skenirajućeg elektronskog mikroskopa. Zbog tehnoloških ograničenja optičkih mikroskopa, koju su i dalje najrašireniji instrumenti za analizu dijatomeja, ostajemo zakinuti za cijeli niz

informacija o vrstama i podvrstama dijatomeja. Stoga često biolozi znaju reći da zbog SEM-a moraju proučavati sve ispočetka.



Slika 9: Gornji red fotografija su snimke uzoraka na optičkom mikroskopu; donji red su snimke diatomeja snimljene pomoću skenirajućeg elektronskog mikroskopa (Izvor: PMF Biološki odsjek i CFIIV "Ivan Vučetić")

Na Slici 9 može se vidjeti razliku između slika dobivenih klasičnim optičkim mikroskopom i snimki dobivenih skenirajućim elektronskim mikroskopom. Osim većeg povećanja slike, elektronski mikroskop nam daje i bolju rezoluciji slike a samim time i bolju diferencijaciju diatomeja, što je velika prednost s obzirom na mnogobrojnost vrsta i podvrsta dijatomeja.

4. ZAKLJUČAK

Rad je podijeljen u dvije cjeline. U prvom dijelu rada, autori daju kratki povijesni pregled razvoja analize na tragove pucanja iz vatrenog oružja i kritički osvrt na analitičke metode i rezultate analiza te detaljnije prikazuje trenutno stanje, nakon uvođenja u svakodnevni rad opremu visoke tehnologije, skenirajući elektronski mikroskop, koja je "must have" ne samo za znanstvene centre nego i za visokostručne ustanove gotovo svih vrsta djelatnosti. Uvođenjem spomenute opreme, analiza tragova pucanja iz vatrenog oružja.

Uvođenje skenirajućeg elektronskog mikroskopa u područje ispitivanja tragova pucanja, u promatranom razdoblju, rezultiralo je značajnim promjenama glede broja i strukture naznačenih predmeta primljenih u rad Centra, tako da su tragovi pronađeni osim na rukama i na odjeći dobili na važnosti (Presuda Vrhovnog suda Republike Hrvatske: Broj: I Kž 757/10-7) a neizuzimanje odjeće za analizu tragova pucanja može predstavljati propust u razjašnjavanju cijelog predmeta (Presuda Vrhovnog suda Republike Hrvatske: Broj: I Kž 1121/07-7). Analiza tragova pucanja iz vatrenog oružja u narednom razdoblju kreće u smjeru visoke specifičnosti zahtjeva rezultata analize i multidisciplinarnosti analize, koristeći znanja iz matematike, fizike i kemije. O upotrebi diatomeja u kriminalistici piše se zadnjih 100 godina, a nekolicina autora smatra da su diatomeje savršeni forenzički materijal, ali ima i kritičara, onih koji ne priznaju njihovu važnost u kriminalistici i forenzici. U većini prikazanih primjera, lokacija utapanja može se odrediti usporedbom vrsta dijatomeja i samim time odrediti točnu lokaciju utapanja. Također, zbog velikog broja vrsta i podvrsta dijatomeja vrlo je mala mogućnost kontaminacije uzoraka iz vanjskih izvora. Prikazano je šest slučajeva ubojstava utapanjem (Pollanen, 1998), kod koji je rađen test na dijatomeje. Test je dao važne informacije o uzroku smrti u svim slučajevima i u slučajevima kad su tijela izvučena iz vode na tlo, što je osobito bitno, jer i u zraku ima dijatomeja, posebno u slučajevima kad nema vidljivih uzroka nasilne smrti ili nema znakova prirodne smrti kao što je srčani udar i slično. Razvojem znanosti i tehnologije, moguće je koristiti i visoku tehnologiju kao što je skenirajući elektronski mikroskop. Kao izazov ostaje razrada metoda i tehnika prikupljanja, analiziranja i diferencijacije diatomeja specifičnih za svaki slučaj posebno te implementacija tih metoda i tehnika u svakodnevni rad.

LITERATURA

Boehm, E. (1971). Application of the SEM in forensic medicine. *Scanning Electron Microscopy*, 553-560.

Cowan, M.E., Purdon, P.L. (1967). A study of the parafin test. *Journal of Forensic Science*, 12, 19-36.

Čukurin, A., Gligora Udović, M., Žutinić, P., Kralj Borojević, K., Mršić, G., Špoljarić, I., Plenković-Moraj, A. (2014). *Functional classification of diatoms in relation to oligotrophic environmental in two deep karstic lakes*. Abstract book of the 8th Cental European Diatom Meeting, Zagreb.

Harrison, H.C., Gilroy, R. (1959). Firearms discharge residues. *Journal of Forensic Science*, 4, 184-199.

Heard, B.J. (1997). *Handbook of Firearms and Ballistics*. Chichester: Wiley.

Krishnan, S.S. (1971). Rapid detection of firearms discharge residues by atomic absorption

and neutron activation analysis. *Journal of Forensic Science,* 144-151.
Krstic, S., Duma, A., Janevska, B., Levkov, Z., Nikolova, K., Noveska, M. (2002). Diatoms in forensic expertise of drowning—a Macedonian experience. *Forensic Science International,* 127, 198–203.
Kumar, M., Deshkar, J, Naik SK, Yadav PK. (2012). Diatom Test- Past, Present and Future: A Brief Review, *Indian Journal of Research and Reports in Medical Sciences*, 2(3). http://www.ijrrms.com/pdf/2012/jul-sep-12-pdf/08.pdf (accessed 12/5/2015).
Modly, D., Šuperina, M., Korajlić, N. (2008). *Rječnik kriminalistike*. Zagreb: Strukovna udruga kriminalista.
Mršić, G., Žugaj, S. (2007). Analiza GSR čestica upotrebom elektronskog mikroskopa (SEM/EDX). *Policija i sigurnost,* 16(3-4), 179-200.
Pollanen, S. (1998). Diatoms and homicide. *Forensic Science International,* 91, 29-34.
Presuda Vrhovnog suda Republike Hrvatske: Broj: I Kž 1121/07-7
Presuda Vrhovnog suda Republike Hrvatske: Broj: I Kž 757/10-7
Presuda Vrhovnog suda Republike Hrvatske: Broj: I Kž 904/04-8
Romolo, F.S., Margot, P. (2001). Identification of gunshot residue: a critical review. *Forensic Science International,* 119, 195-211.
Ruch, R.R., Buchanan, J.D., Guinn, V.P., Bellanca, S.C., Pinker, R.H. (1964). Neutron activation analysis in scientific crime detection. *Journal of Forensic Science* 9, 119-132.
Singh, R., Singh, R., Thakar, M.K. (2006). Extraction methods of diatoms – a review. *IIJFMT* 4(2).
https://www.researchgate.net/publication/237479470_EXTRACTION_METHODS_OF_DIATOMS-A_REVIEW (accessed 12/12/2015).
Statistički pregled (2014).
http://www.mup.hr/UserDocsImages/statistika/2015/Statisticki_pregled_2014.pdf (pristupljeno 12.5.2015).
Uitdehaag, S. (2010). Extraction of diatoms from (cotton) clothing for forensic comparisons. *Forensic Science International,* 200, 112–116.
Uredba o unutarnjem ustrojstvu Ministarstva unutarnjih poslova (NN 70/12, 140/13, 50/14, 32/15).
Zakon o kaznenom postupku (NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13,145/13, 152/14).
Zakon o kaznenom postupku NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14 http://www.zakon.hr/z/174/Zakon-o-kaznenom-postupku (preuzeto 20. veljače 2016.)
Zakon o policijskim poslovima i ovlastima (NN 76/09, 92/14).

Igor Špoljarić
Ante Orlović
Gordan Mršić

IMPLEMENTATION OF HIGH TECHNOLOGY IN FORENSIC CRIME INVESTIGATION - SCANNING ELECTRON MICROSCOPE (CURRENT STATUS AND PROSPECTS)

Summary

Forensic crime investigations are essentially based on detection, securing and resolving traces that might serve as evidence in criminal proceedings. In serious and high profile cases micro traces often have a key role and they require proper handling, which generally implies the use of hi-tech devices.

The effects of the implementation of high technology, in this case a scanning electron microscope, in the area of forensic crime investigations are discussed in the context of gunshot residue traces examination conducted at the Forensic Science Centre "Ivan Vucetic" MUP RH, in the period from 2008 to 2015.

Considering the indicators in the mentioned period, the implementation of the mentioned device in the area of gunshot residue traces examination resulted in significant changes in the number and structure of cases involving the indicated issues that have been received by the Centre to work on.

In addition to previous experience and the current state of the scanning electron microscope application in forensic criminal investigations, it is important to consider the prospects of its future application possibilities.

Regarding this, reflections about potential possibilities of implementation of the mentioned high technology device in other forensic crime investigation areas (research on diatom algae in the study of homicides and suicides investigation) are expressed because the same device is already in use in related fields - but only for scientific purposes. Continuous development and implementation of high technologies may lead to the development and implementation of a series of new methods that could significantly contribute to the resolution and clarification of specific situations/facts/circumstances in serious and high profile cases.

Key words*: scanning electron microscope; gunshot residue traces; Diatoms; homicide and suicide.*

STRUČNI RAD

Žarko Ćulibrk[191]

ZNAČAJ VISOKIH TEHNOLOGIJA I ULOGA POLICIJE U UPRAVLJANJU VANREDNIM SITUACIJAMA – FAZA INFORMISANJA

Sažetak

Za osnovnu temu rada uzeti su značaj visokih tehnologija i uloga policije u upravljanju vanrednim situacijama, sa posebnim osvrtom na fazu informisanja. Tokom izrade rada korištene su različite metode, uglavnom eksplikativna analiza i deskriptivna analiza, te metoda analize sadržaja. Opisani su i objašnjeni upravljanje vanrednim situacijama, kao i najznačajnije hitne službe koje prve djeluju kada se vanredna situacija desi (policija, vatrogasci i hitna pomoć). Poseban naglasak dat je na policiju. Opisane su i objašnjene faze upravljanja vanrednim situacijama – pripravnost, odgovor (reagovanje), otklanjanje posljedica (oporavak), ublažavanje i informisanje – sa naglaskom na fazu informisanja. Posebno je obrađen sadržaj faze informisanja, u kojoj je je značajna upotreba visokih tehnologija. Isto tako, u okviru toga je opisana uloga policije u ovoj fazi. Osim toga prikazane su i određene šeme vezane za problematiku upravljanja vanrednim situacijama. Cilj ovog naučnog rada jeste da ukaže na značaj faze informisanja, kao važnog segmenta u ciklusu upravljanja vanrednim situacijama.

Ključne riječi: *Upravljanje vanrednim situacijama; informisanje; visoke tehnologije; komunikacije; hitne službe; policija.*

1. UVOD

Ljudsko društvo, kroz njegovu istoriju, ugrožavale su različite pojave. Svaki put, čovjek se nastojao zaštititi od ovih pojava, kako ne bi došlo do gubitka ljudskih života ili uništenja imovine. Činio je to na različite načine – pokušavao je spriječiti nesreću, pripremao se za nju, pokušavao je adekvatno odgovoriti na nju, ili se nastojao što brže oporaviti nakon nesretnog događaja. Svi ovi postupci za cilj su imali upravljati nesrećom (vanrednom situacijom). Važan element upravljanja vanrednim situacijama, u svakom od navedenih segmenata, jeste informisanje.

U ovom će radu ukratko biti opisani i objašnjeni upravljanje vanrednim situacijama, hitne službe (sa naglaskom na policiji), djelovanje policije u vanrednim situacijama, te faza informisanja, u kojoj značajan dio pripada upotrebi visokih tehnologija. Razumijevanje faze informisanja u procesu upravljanja vanrednim situacijama značajno je i za postupak reagovanja policije u vanrednim prilikama.

[191] doc. dr. Žarko Ćulibrk, Fakultet za bezbjednost i zaštitu, Banjaluka

2. UPRAVLJANJE VANREDNIM SITUACIJAMA

Nesreće i katastrofe kao uzrok vanrednih situacija vežu se isključivo za postojanje čovjeka, kroz neposredan ili posredan negativan uticaj na njegovo bitisanje. Upravljanje vanrednim situacijama kao pojam koji znači sveobuhvatno rješavanje različitih opasnosti relativno je nov, ali svojim korijenima seže u našu drevnu prošlost. Tako borba sa poplavama datira još iz starog Egipta,[192] prve vatrogasne jedinice formirane su u Starom Rimu,[193] Inke su regulisale pojavu klizišta,[194] itd.

Ne postoji jedinstvena formula upravljanja vanrednim situacijama, ali postoji razdoblje (sredina XX vijeka) kada je u velikom dijelu zemalja svijeta bila razvijena građanska samozaštita ili tzv. civilna odbrana. Iz ovih sistema, nastalih tokom hladnog rata, kasnije su se razvile mnoge agencije za upravljanje vanrednim situacijama (u Kanadi, SAD). Iako se upravljanje vanrednim situacijama razlikuje od zemlje do zemlje, postoje i neke sličnosti. Mnoge vlade, naročito nerazvijenih zemalja, razvijale su ovaj sistem po potrebi i naknadno su osnivale potrebna tijela za, dok druge zemlje nemaju nikakav oblik upravljanja vanrednim situacijama.

Cilj upravljanja vanrednim situacijama jeste sigurnost države i društva (pripravnost, reagovanje, otklanjanje i ublažavanje posljedica vanrednih situacija). Glavni cilj je zaštita života i zdravlja ljudi, zaštita imovine, kulturnih dobara i ključne infrastrukture. Ključnu ulogu u ovom procesu igraju hitne službe, na čelu sa policijom.

3. HITNE SLUŽBE

Nema jedinstvene definicije pojma **hitnih službi**. Obično se, pored opšteg pojma službi koje reaguju u vanrednim prilikama, pojam hitna služba vezuje za hitnu medicinsku pomoć, kako kod nas, tako i u drugim zemljama. Može se reći da ***hitne službe*** *predstavljaju organe, organizacije i institucije koje obezbjeđuju sigurnost države, društva i pojedinaca djelujući u različitim vanrednim situacijama*.[195]

Neke od ovih službi djeluju samostalno i zadužene su za neki od oblika ugrožavanja bezbjednosti. Druge službe su zadužene za određene vanredne situacije, uz postojeće poslove koje obavljaju. Pojedine službe djeluju preventivno i pomažu stanovništvu da se pripremi, reaguje ili izbjegne posljedice nesreća.

Obično se **tri hitne službe** smatraju osnovnim. To su: *1) Policija*; *2) Vatrogasna služba*; i *3) Služba hitne medicinske pomoći (hitna pomoć)*. Pored ovih službi, postoje i druge državne, javne i privatne službe koje mogu ili imaju obavezu reagovati u vanrednim situacijama.

---

[192] Za vrijeme vladavine Amenemheta III (1841–1797 p.n.e.) regulisan je tok rijeke Nil.
[193] Bili su to tzv. Gradski stražari (*Vigiles Urbani*), koje je 6. g. n. e. osnovao rimski car Avgust.
[194] Gradnjom zemljanih terasa Inke su sprečavale pokretanje zemlje.
[195] Ćulibrk, Ž.: *Upravljanje vanrednim situacijama*, Fakultet za bezbjednost i zaštitu, Banjaluka, 2016, str. 179.

4. POLICIJA

Saglasno različitim teorijskim izvorima, **policija** je zadužena da održava javnu i državnu bezbjednostu i sprečava kriminalna djela. Po profesoru Gaćeši „policiju možemo definisati kao posebno organizovanu državnu službu, čiji je prioritetan zadatak da štiti javni poredak, odnosno da se stara o javnoj i državnoj bezbjednosti i izvršavanju drugih unutrašnjih poslova iz djelokruga koji je određen zakonom.“[196]

Slično određenje daju i drugi izvori. Po američkom *Rječniku unutrašnje bezbjednosti i odbrane*, policija je grana vlasti zadužena za čuvanje javnog reda i mira; unapređenje javnog zdravlja, sigurnosti i morala; i za sprečavanje, otkrivanje i kažnjavanje zločina.[197] Po ruskom *Saveznom zakonu o policiji*,[198] policija štiti život, zdravlje, slobodu i prava ruskih građana, stranih državljana i lica bez državljanstva; bori se protiv kriminala; štiti javni poredak i imovinu; i čuva bezbjednost.

5. DJELOVANJE POLICIJE U VANREDNIM SITUACIJAMA

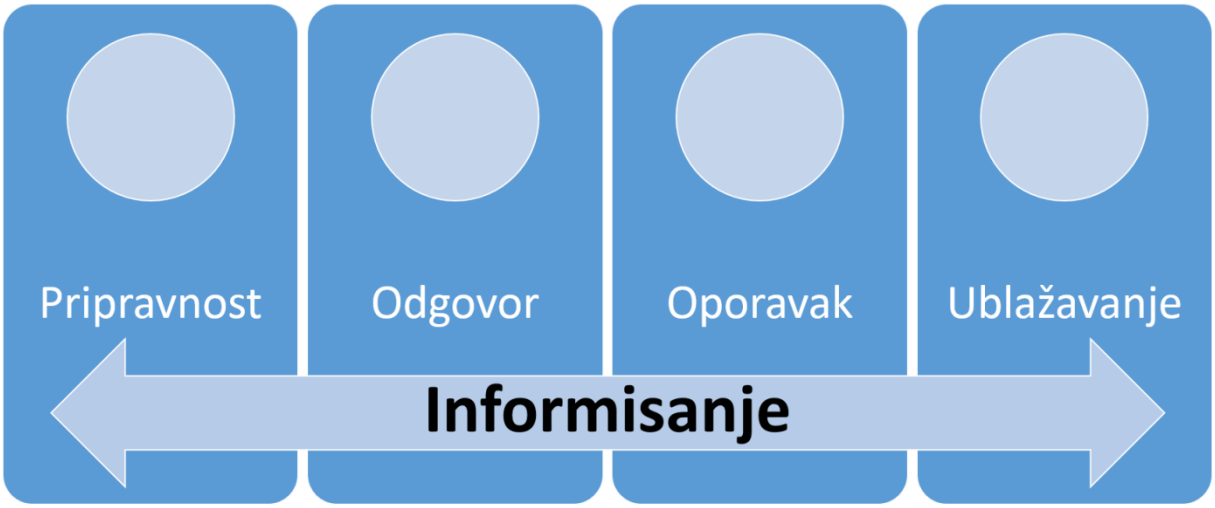
Upravljanje vanrednim situacijama je složen proces koji se odvija u nekoliko faza. Najveći broj izvora (Kopola,[199] američko ministarstvo obrazovanja,[200] Pampel,[201] Klements,[202] Kanton)[203] upravljanje vanrednim situacijama predstavlja kao ciklus od četiri koraka ili faze (pripravnost, odgovor, oporavak, ublažavanje), s tim da raspored faza nije uvijek jednak, što se objašnjava cikličnošću procesa i jednakim značajem svake od faza. Jedan broj autora (Handmer i Dovers)[204] upravljanje vanrednim situacijama svodi na tri faze (pripravnost, odgovor i oporavak), dok drugi autori proširuju ovaj ciklus na pet (Hedou i Bulok,[205] Felan)[206] i više faza (Štrbac). U svakoj od ovih faza, a različiti autori navode različit broj faza, policija ima odgovarajući značaj.

Ciklus upravljanja vanrednim situacijama, podijeljen u četiri faze, predstavlja čvrstu osnovu za kvalitetno rješavanje problema koje se tiče djelovanja policije u vanrednim situacijama, te za kvalitetno rješavanje problema koje nose različite vanredne prilike, i sa praktičnog aspekta

---

[196] Gaćeša, D.: *Policija – nadležnost, organizacija, rukovođenje*, Udruženje defendologa Republike Srpske – Glas srpski, Banjaluka, 1998, str. 28.
[197] O'Leary, M. R.: *The Dictionary of Homeland Security and Defense*, iUniverse, New York – Lincoln – Shanghai 2006, стр. 359.
[198] *Федеральный закон от 07.02.2011 N 3-ФЗ "О полиции"*
[199] Coppola, D. P.: *Introduction to International Disaster Management*, Elsevier – Butterworth-Heinemann 2007
[200] *Action Guide for Emergency Management at Institutions of Higher Education*, U.S. Department of Education 2009
[201] Pampel, F. C.: *Disaster Response*, Facts On File 2008
[202] Clements, B.: *Disasters and Public Health: Planning and Response*, Butterworth-Heinemann, Burlington – Oxford 2009
[203] Canton, L. G.: *Emergency Management: Concepts and Strategies for Effective Programs*, Wiley-Interscience, Hoboken 2007
[204] Handmer, J. and Dovers, S.: *The Handbook of Disaster and Emergency Policies and Institutions*, Earthscan, London - Sterling 2007
[205] Ublažavanje, odgovor, oporavak, pripravnost i veze [Haddow, G. and Bullock, J.: *Introduction to Emergency Management*, Second Edition, Butterworth-Heinemann 2006]
[206] Ublažavanje, pripravnost, odgovor, oporavak i obnova [Phelan, T. D.: *Emergency Management and Tactical Response Operations: Bridging the Gap*, Butterworth-Heinemann 2008]

je veoma koristan. Međutim, proces upravljanja vanrednim situacijama ne može se zamisliti bez komunikacija i informisanja, tako da ciklus upravljanja vanrednim situacijama možemo podijeliti u **pet faza**, gdje se peta faza – faza informisanja, proteže kroz četiri ostale faze (Šema 1).



Šema 1 Faze upravljanja vanrednim situacijama
Izvor: Obrada autora

6. INFORMISANJE

Peta faza upravljanja vanrednim situacijama, faza informisanja, sa razvojem tehnologije dobija sve značajnije mjesto. Autori je obično ne izdvajaju kao posebnu fazu, već je obrađuju u okviru nabrojanih faza. Mi ćemo je razmatrati kao posebnu fazu, koja se, kako je već rečeno, proteže kroz ostale četiri faze upravljanja vanredim situacijama. Ovu fazu čini nekoliko značajnih segmenata, kao što su komuniciranje, informisanje, obavještavanje. U svakom od ovih segmenata značajno mjesto zauzimaju visoke tehnologije. Uloga faze informisanja jeste da javnosti, u sve četiri navedene faze upravljanja vanrednim situacijama, obezbijedi pravovremenu i tačnu informaciju.

Uspjeh faze informisanja čine četiri ključne **pretpostavke**:
1) *Briga o građanima*;
2) *Posvećenost poslu*;
3) *Uključivanje informisanja u planiranje i operativni rad*; i
4) *Saradnja sa medijima*.

Briga o građanima, koji su glavni „korisnici“ rada svih hitnih službi, pa tako i policije, ključ je efikasnog informisanja. Potrebe pojedinaca i potrebe zajednice moraju biti na prvom mjestu. Adekvatna medijska pažnja i izdavanje odgovarajućih vodiča tome znatno doprinose.

Posvećenost poslu odgovornog policijskog rukovodstva podrazumijeva dobru komunikaciju, razmjenu i distribuciju informacija – interno i eksterno (unutar policijske organizacije, sa partnerima i sa javnošću). Savremene tehnologije olakšavaju i unapređuju ovaj proces.

Najvažniji dio djelatnosti rukovodilaca policije jeste **uključivanje informisanja u planiranje i operativni rad** (planiranje i konkretne aktivnosti u četiri osnovne faze). To znači da specijalisti za informisanje učestvuju u radu timova za planiranje i koordinaciju, i da je informisanje uvršteno u sve organizacione aktivnosti полиције u procesu upravljanja vanrednim situacijama. Za razliku od prošlosti, kada tehnologija nije bila toliko razvijena i informisanje se nije smatralo presudnim za upravljanje vanrednim situacijama, danas je drukčije stanje.

Saradnja sa medijima četvrta je značajna pretpostavka uspješnog informisanja. Mediji igraju glavnu ulogu u komunikaciji sa javnošću. Nijedna hitna služba, niti neka druga organizacija uključena u upravljanje vanrednim situacijama, pa tako ni policija, ne mogu razviti sistem za prenos informacija uporediv sa već postojećim RTV sistemima, štampom i internetom. Kako bi se informacije javnosti pravovremeno dostavljale, policija mora uspostaviti partnerski odnos sa medijima, utemeljen na međusobnom povjerenju. Obično je taj odnos slab, praćen tenzijama oko želje medija da saznaju sve informacije (šta je bilo, kako se to dogodilo i ko je kriv) i zadatka policije da pruži samo najpotrebnije podatke. U ovom sukobu jedini gubitnik je javnost, koja u tom slučaju ostaje uskraćena za pravovremenu i tačnu informaciju. Rukovodioci policije moraju shvatiti potrebu medija da informišu, ali i njihovu pozitivnu ulogu u prenosu informacija javnosti, koja će se ostvariti uspješnom saradnjom. S druge strane, saradnja medijima omogućava pristup mjestima nesreće i dobijanje podataka koji će biti srž tačnosti njihovog izvještavanja. Dobra saradnja sa medijima pomaže u upravljanju javnim mnjenjem, u definisanju uloge policije i u podizanju morala radnika policije i žrtava.

Da bi informacija bila efektivno prenijeta, policija i ostale hitne službe koje učestvuju u upravljanju vanrednim situacijama moraju odrediti ko je krajnji **korisnik (konzument) informacija**. Obično su to građani, mediji, zvaničnici, službenici itd.

Po Artu Boterelu (*Art Botterell*), fazu informisanja u upravljanju vanrednim situacijama čine **četiri sloja**: 1) *Organizacija* – struktura, ciljevi, zadaci i pokazatelji koji određuju organizaciju; 2) *Ljudi* – ljudski činioci kao što su sposobnost, obuka, stavovi itd; 3) *Postupci* – modeli za rješavanje problema i sl; i 4) *Tehnologija* – prvenstveno sistemi i oprema za komuniciranje (Šema 2).

Šema 2 Slojevi informisanja i međusobni odnos tehnoloških promjena i percepcije problema u fazi informisanja

Izvor: Canton, L. G.: *Emergency Management: Concepts and Strategies for Effective Programs*

Problemi koji se javljaju u fazi informisanja percipiraju se kroz ova četiri sloja, s tim da razvoj tehnologije znatno utiče na pozitivno rješavanje problema.

7. ZAKLJUČAK

Bez obzira da li se radi o policiji, medijima, javnosti ili partnerima (ostalim hitnim službama), faza informisanja je ključna u upravljanju vanrednim situacijama. Odnos sa medijima mora biti otvoren i mora postojati kvalitetna saradnja, koja će obezbijediti stalan protok tačnih informacija, uz nesebično angažovanje zvaničnika, koji će biti objektivni i ponašati se u skladu sa situacijom. Pristup korisnicima informacija, naročito javnosti, mora biti neposredan i kooperativan, i mora uključiti programe upoznavanja građana sa mogućim opasnostima, kako se pripremiti za opasnost, kako je spriječiti, kako reagovati kada se nesreća desi, kako otkloniti njene posljedice.

Kvalitetno sprovedena faza informisanja doprinosi boljoj distribuciji informacija i boljoj razmjeni podataka. Dobro sprovedena faza informisanja doprinosi boljem komuniciranju, koje se poboljšava stručnom i optimalnom upotrebom savremenih tehnologija. Kvalitetno sprovedena faza informisanja doprinosi boljem obavještavanju javnosti. Razvoj visokih tehnologija svemu ovome daje dodatni doprinos.

LITERATURA

Action Guide for Emergency Management at Institutions of Higher Education, U.S. Department of Education 2009

Canton, L. G.: Emergency Management: Concepts and Strategies for Effective Programs, Wiley-Interscience, Hoboken 2007

Clements, B.: Disasters and Public Health: Planning and Response, Butterworth-Heinemann, Burlington – Oxford 2009

Coppola, D. P.: Introduction to International Disaster Management, Elsevier – Butterworth-Heinemann 2007

Ćulibrk, Ž.: Reagovanje, koordinacija i saradnja hitnih službi u vanrednim situacijama, Fakultet za bezbjednost i zaštitu, Banjaluka, 2011.
Ćulibrk, Ž.: Upravljanje vanrednim situacijama, Fakultet za bezbjednost i zaštitu, Banjaluka, 2016.
Erickson, P. A.: Emergency Response Planning for Corporate and Municipal Managers, Second Edition, Butterworth-Heinemann, Burlington 2006
Федеральный закон от 07.02.2011 N 3-ФЗ "О полиции"
Gaćeša, D.: Operativni rad policije na bezbjednosnom sektoru (praktikum), Udruženje defendologa Republike Srpske, Banjaluka, 2001.
Gaćeša, D.: Policija – nadležnost, organizacija, rukovođenje, Udruženje defendologa Republike Srpske – Glas srpski, Banjaluka, 1998.
Haddow, G. and Bullock, J.: Introduction to Emergency Management, Second Edition, Butterworth-Heinemann 2006
Handmer, J. and Dovers, S.: The Handbook of Disaster and Emergency Policies and Institutions, Earthscan, London - Sterling 2007
Jovičić, D.: Organizacija i nadležnost policije, Fakultet za bezbjednost i zaštitu, Banjaluka, 2008.
O'Leary, M. R.: The Dictionary of Homeland Security and Defense, iUniverse, New York – Lincoln – Shanghai 2006
Pampel, F. C.: Disaster Response, Facts On File 2008
Phelan, T. D.: Emergency Management and Tactical Response Operations: Bridging the Gap, Butterworth-Heinemann 2008
Planning for and Managing Emergencies, The Association of University Chief Security Officers 2008
Štrbac, K.: Humanitarne organizacije u zbrinjavanju civilnog stanovništva u vanrednim situacijama, Vojnoizdavački zavod, Beograd, 2008.
The Role and Responsibilities of the Police, Police Foundation - Policy Studies Institute, London, 1996.

Žarko Ćulibrk

THE IMPORTANCE OF HIGH TECHNOLOGY AND THE ROLE OF THE POLICE IN EMERGENCY MANAGEMENT – INFORMATION PHASE

Summary
The main topic of this paper is the importance of high technology and the role of police in emergency management with special emphasis on the phase of information. The main methods used in this paper are explicative and descriptive analysis, and content analysis. The paper describes and explains emergency management as well as the most important emergency services that first act when an emergency occurs (police, fire department and ambulance). Special emphasis is given to the police. Emergency management phases– preparedness, response, recovery, mitigation and information – are also described, with a focus on the phase of information. Particularly, the paper describes the contents of the phase of information, where the use of high technology is very important. Moreover, it describes the role of the police in this emergency management phase. Additionally, some schemes related to this issue are presented. The aim of this scientific paper is to highlight the importance of the phase of information, as an important segment in the emergency management cycle.

Keywords: *emergency management, information, high technology, communication, emergency services, police.*

STRUČNI RAD

Davorka Martinjak[207]
Danko Salopek[208]
Renata Odeljan[209]
Suzana Kikić[210]

DOPRINOS OTVORENIH IZVORA NA INTERNETU I SUVREMENIH INFORMACIJSKO-KOMUNIKACIJSKIH TEHNOLOGIJA U PRONALAŽENJU NESTALE DJECE

Sažetak

U zadnjih 20-tak godina koliko je internet u široj uporabi mnogi stručnjaci još i danas raspravljaju o prednostima i nedostacima korištenja interneta. Uz čitav niz kvalitetnih sadržaja, programa i aplikacija, nesporno je da postoje i rizici vezani uz korištenje modernih tehnologija posebno za djecu i mlade, međutim, u ovom radu autori će dati prikaz kako društvene mreže i drugi otvoreni izvori na internetu mogu doprinijeti, pomoći policiji u provođenju policijskih izvida u slučajevima bjegova i udaljenja djece iz obiteljskog doma ili odgojnih ustanova. Kako pomoću web pretraživača, društvenih mreža, blogova, foruma i slično locirati nestalo dijete. Danas imamo puno internet tražilica različitih namjena među kojima je najpopularnija Google, ali i neke druge tražilice koje mogu poslužiti u određenim slučajevima: Yahoo Search, America On Line; Microsoftova tražilica, GoTo Webcrawler; Wikipedia. Također, vrlo korisne tražilice su i Meta tražilice (Meta search engines) koje umjesto korisnika šalju upite na više različitih tražilica npr.: xquick; Dogpile Mamma; Search.com; Carot2, te tražilice koje ciljano tragaju za određenim osobama kao što je: https://pipl.com/; http://com.lullar.com/ itd. Pored tražilica značajnu ulogu u pronalaženju nestale djece imaju i društvene mreže posebno najpopularniji Facebook-a, Google+ i brojni drugi. Međutim, važno je napomenuti da se podaci dobiveni na internetu uvijek moraju uzimaju s dozom opreza, ali uvezivanjem tih podataka sa službenim podacima mogu biti ključ uspjeha u pronalaženju svih nestalih osoba.

Ključne riječi: *internet, otvoreni izvori, nestala djeca i maloljetnici, društvene mreže.*

[207] Dr. sc. Davorka Martinjak, viši predavač Visoke policijske škole, Zagreb, e-mail:dmartinjak@fkz.hr
[208] Danko Salopek, MUP, Ravnateljstvo policije, UKP, Odjel visokotehnološkog kriminaliteta, dasalopek@mup.hr
[209] mr. sc. Renata Odeljan, viši predavač Visoke policijske škole, Zagreb, rodeljan@fkz.hr
[210] Suzana Kikić, Voditeljica Programa specijalizacije u Službi za dodatno stručno osposobljavnje i usavršavnje, Policijska akademija, MUP RH, Zagreb.

1. UVOD

Nestanak osoba, a posebno nestanak djece i maloljetnika uvijek izaziva znatnu pozornost stručne i društvene javnosti te otvara mnoga pitanja o uzrocima te pojave. Definiciju pojma nestale osobe u Hrvatskoj sintezom različitih definicija objavljenih u kriminalističkoj literaturi dali su Šuperina i Gluščić (2003:152). Prema definiciji autora, osoba se smatra nestalom ako se udaljila iz svog uobičajenog okružja (mjesta prebivališta, boravišta) protivno svojoj volji ili u skladu sa svojom voljom, a pritom u određenom logički prihvatljivom razdoblju, imajući na umu njene dosadašnje životne navike, običaje ponašanja, socijalne kontakte, profesionalne aktivnosti i sl., nema spoznaja o njenom trenutnom boravištu ili nalazištu, odnosno općenito o njenoj sudbini (prema Šuperina, Dujmović, 2011:413).

Kada govorimo o nestaloj djeci i maloljetnicima, onda najčešće mislimo na udaljenja iz obiteljskog doma ili bjegove iz odgojnih ustanova. Međutim, nisu rijetki slučajevi odvođenja djece od strane drugog roditelja („roditeljske otmice“), nestanci sa smrtnim posljedicama (samoubojstva ili nesretni slučajevi, primjerice pri utapanju) te slučajevi kada djeca i maloljetnici postaju žrtve kaznenih djela.

Prema policijskim podatcima, najčešći razlozi udaljenja od kuće su avanturizam i skitnja, zatim obiteljski problemi i problemi u školi.[211]

Buljan Flander (2011) navodi da su udaljenjima iz obiteljskog doma najčešće podložne emocionalno nestabilne mlade osobe, impulzivne, agresivne ili odgojno zapuštene, dok je kod nekih više naglašena potreba za slobodom i neovisnošću. Adolescenti često bježe od kuće iz razloga što je doživljavaju neprijateljskom, da bi kaznili svoje roditelje, izazvali njihov osjećaj krivnje ili da bi pobjegli od kazne i obveza. Bježanje također može biti i trenutačna reakcija na sukob ili kontrolirano i planirano ponašanje kao odraz nepotpune socijalizacije ili neprilagođenosti. Bježanje može značiti i poziv u pomoć ili zahtjev mlade osobe da se odnos okoline prema njoj promijeni. Među najčešćim motivima i uzrocima bijega od kuće su oni obiteljski: poremećeni obiteljski odnosi (međusobni odnos roditelja, odnos roditelja prema djetetu/djeci), prisutnost alkoholizma kod člana obitelji, psihičko zlostavljanje i fizičko kažnjavanje ili pak loši stambeni i materijalni uvjeti. Ostali motivi bijega od kuće nalaze se u negativnom utjecaju društva, u želji za zabavom ili u školskom neuspjehu.[212] I Jelavić također navodi (2011) da su uzroci i razlozi udaljenja djece iz obiteljskog doma najčešće povezani s visokom razinom stresa i frustracije djeteta koju udaljenjem pokušava razriješiti, ali pritom dodaje da udaljenja od kuće mogu biti i situacijske prirode, kada dijete reagira na određeni aktualni događaj kao što je, primjerice, razvod roditelja. Takvo ponašanje može biti rezultat mladenačke nepromišljenosti te ne mora nužno ukazivati na duboke poremećaje u obiteljskoj dinamici ili kod djeteta.

Prema policijskim podatcima, najčešći razlozi bijega iz odgojne ustanove su problem adaptacije u ustanovi, izbjegavanje odgojne mjere u ustanovi, ne vraćanje s dopusta u ustanovu, bijeg zbog činjenja kaznenih djela, nepoštivanje autoriteta, te utjecaj vršnjačke

[211] MUP, Ravnateljstvo policije, UKP, Odjel maloljetničke delinkvencije i kriminaliteta na štetu mladeži i obitelji.

[212] *Trebamo li brinuti? Priručnik o adolescentima za roditelje i stručnjake,* Poliklinika za zaštitu djece grada Zagreba, http://www.poliklinika-djeca.hr/publikacije/trebamo-li-brinuti/ od 14. 3. 2016.

skupine.[213]

Marušić (2011) navodi da je bježanje djece ili maloljetnika iz odgojnih ustanova najčešće motivirano strahom od boravka u instituciji (prvenstveno bojazni od nepoznatog), nenaviknutošću na pravila i strukturirane uvjete života, sramom zbog boravka u instituciji, strahom od neprihvaćanja od strane ostalih štićenika, osjećajem neuklopljenosti u odgojnu grupu u adaptacijskom razdoblju, doživljajem doma kao neke vrste zatvora, nezadovoljstvom uvjetima smještaja, željom za povratkom obitelji, traženjem uzbuđenja, povodljivošću za osobom koja dulje planira bijeg i općenito povodljivošću za vršnjacima, strahom od sudskog postupka i njegova ishoda/sankcije, osjećajem prevarenosti i negativnim stavom prema predstavnicima sustava (socijalne skrbi, policije). Djeca rijetko bježe iz ustanova s ciljem povratka roditeljima, već se upute u skitnju gradom u kojem se ustanova nalazi ili u grad iz kojeg su otišli u dom. Nerijetko ih za vrijeme bijega zatiče policija u počinjenju kaznenog djela (pretežno krađama, provalama i razbojstvima), jer ne raspolažu nikakvim sredstvima za preživljavanje. Djeca ili maloljetnici skloni bježanju iz odgojnih ustanova ("djeca ulice") idealna su meta asocijalnih osoba izvan ustanova za vrbovanje i za ulogu žrtve različitih zloupotreba (podvođenje i uključivanje u prostituciju, uključivanje u trgovinu drogom ili trgovanje djecom). Usmjereni na sakrivanje od policije i odraslih osoba koje bi ih mogle zapaziti ili prijaviti, tijekom bijega iz odgojnih ustanova maloljetnici se često nalaze u napuštenim kućama, dvorištima, u vagonima na željezničkim kolodvorima, u improviziranim ostavama/kućicama kraj vrtova ili polja ili u praznim vikendicama

2. FENOMENOLOŠKA OBILJEŽJA NESTANAKA DJECE I MALOLJETNIKA

Prema statističkim pokazateljima Ministarstva unutarnjih poslova Republike Hrvatske,[214] tijekom posljednjih sedam godina (2009. – 2015.) ukupno 4770 djece i maloljetnika udaljilo se iz svog obiteljskog doma, i to 600 djece do 14 godina te 4170 njih u dobi od 14 do 18 godina. Od tog broja 1642 je bilo muškog spola, a 3128 ženskog spola. Kao što smo već ranije naveli, najčešći razlozi udaljenja iz obiteljskog doma su avanturizam i skitnja te obiteljski problemi. Udio djece i maloljetnika koji su se udaljili zbog skitnje i avanturizma u ukupnom broju udaljenja je 44,7%, dok udio udaljenja zbog obiteljskih problema iznosi 12,2%. Navedene podatke treba ipak uzeti s velikom dozom opreza jer za veliki broj djece i maloljetnika, njih 539 (11,2%), nije utvrđen razlog udaljenja. Jednako tako postavlja se pitanje koliko se djece i maloljetnika upustilo u avanturizam i skitnju zbog obiteljskih problema.

Distribucija nestale djece i maloljetnika po spolu ukazuje na značajna odstupanja. Naime, 65,5% djece i maloljetnika koji su se udaljili od kuće bili su ženskog spola. Ovaj podatak bi se mogao iskoristiti u svrhu izrade preventivnih programa, ali i usmjeravanja potražne djelatnosti policije u slučajevima nestale djece i maloljetnika.

---

[213] MUP, Ravnateljstvo policije, UKP, Odjel maloljetničke delinkvencije i kriminaliteta na štetu mladeži i obitelji.

[214] MUP, Ravnateljstvo policije, UKP, Odjel maloljetničke delinkvencije i kriminaliteta na štetu mladeži i obitelji.

U istom razdoblju 6592 djece i maloljetnika pobjeglo je iz neke od odgojnih ustanova, i to 704 djece do 14 godina te 5879 u dobi od 14 do 18 godina. Od tog broja 2883 su bili muškog spola, a 3574 ženskog spola. Udio djece i maloljetnika koji su pobjegli iz odgojne ustanove nevraćanjem s dopusta u ukupnom broju bjegova iznosi 39,5%, udio pak bjegova zbog izbjegavanja odgojne mjere iznosi 22,6%, dok bjegova iz ustanove zbog problema adaptacije iznosi 13,8%. I ove podatke treba uzeti s velikom dozom opreza jer za veliki broj djece i maloljetnika, njih 2606 (39,5%), nije utvrđen razlog bijega iz ustanove.

Distribucija djece i maloljetnika po spolu koji su pobjegli iz odgojne ustanove također ukazuje na značajno odstupanje. Naime, 54,2% djece i maloljetnika koji su pobjegli iz odgojne ustanove ženskog su spola.

3. ZAKONODAVNI OKVIR I NAČIN POSTUPANJA POLICIJE U SLUČAJEVIMA NESTALE DJECE I MALOLJETNIKA

Sukladno članku 48. Zakona o policijskim poslovima i ovlastima, policija provodi traganje za osobama i predmetima. Traganje se provodi raspisivanjem potrage i objave. Za nestalom osobom, pa tako i za djetetom i maloljetnikom, raspisuje se potraga s ciljem pronalaženja.[215]

Pravilnik o načinu postupanja policijskih službenika u člancima 75. – 78. propisuje način provedbe mjere traganja za osobama. U stavku 2. članka 75. navodi se da je policijski službenik dužan odmah poduzeti potrebne mjere u svrhu pronalaska osobe ili predmeta za kojim se traga. Sukladno potrebi, u svrhu traganja za nestalom osobom ili predmetom, može se primijeniti i mjera utvrđivanja položaja mobilnog telekomunikacijskog uređaja. Policijski službenik će o poduzetim radnjama sastaviti izvješće, koje se zajedno sa zapisnikom prilaže u spis potrage. Ako osoba čiji je nestanak prijavljen nije pronađena u roku od 24 sata od zaprimanja prijave, sastavit će se plan traganja za osobom koji odobrava nadležni rukovoditelj. Obrasci zapisnika o zaprimljenoj prijavi o nestanku osobe i zapisnika o zaprimljenoj prijavi o nestanku predmeta sastavni su dijelovi pravilnika.[216]

U slučajevima kada je nestalo dijete ili maloljetna osoba, prijavu može podnijeti roditelj, zakonski zastupnik ili skrbnik, kao i zaposlenik odgojne ustavne iz koje je dijete ili maloljetnik nestao. Prilikom zaprimanja prijave policijski službenici zatražit će od prijavitelja identifikacijske podatke, podatke o mjestu nestanka, podatke o osobnom opisu i odjeći koju je dijete ili maloljetnik imao na sebi kada je nestao, podatke o zadnjim osobama s kojima je dijete ili maloljetnik bio u kontaktu, podatke o njegovim svakodnevnim aktivnostima i kretanjima te navikama, mjestima na koja izlazi i koja posjećuje, podatke o sportskim aktivnostima i o školovanju, osobama s kojima se druži i o najboljim prijateljima, eventualno postojanje oproštajnog pisma, dnevnik, zdravstveno stanje, broj telefona ako ga ima itd. Prijavi nestanka će se uvijek priložiti i najnovija fotografija ili će se pak izraditi fotorobot

[215] Zakon o policijskim poslovima i ovlastima, NN 152/08., 76/09., 80/11., 121/11., 91/12. , 143/12., 56/13., 145/13. i 152/14. http://zakon.hr/z/174/Zakon-o-kaznenom-postupku od 4. 5. 2016.
[216] Pravilnik o načinu postupanja policijskih službenika, NN 89/10. i 76/15. http://www.propisi.hr/print.php?id=2160 od 4. 5. 2016.

nestalog djeteta ili maloljetnika.

Kada nestane dijete ili maloljetna osoba, kao i pri svim nestancima potrebno je odmah/žurno poduzeti potrebne mjere u svrhu njena pronalaska. Policija će, sukladno svojim zakonskim ovlastima, u slučajevima nestanka djece ili maloljetnih osoba (kao i slučajevima nestanka bilo koje osobe) provjeriti navode iz zapisnika o prijavi nestanka osobe, raspisati potragu za nestalom osobom kroz Informacijski sustav MUP-a RH, obavijestiti cjelokupni operativni sastav policije (lokalno, regionalno, nacionalno, a u slučaju sumnje da je dijete ili maloljetna osoba napustila zemlju, tada i međunarodno), ustupiti fotografiju i podatke o nestaloj osobi svim policijskim postajama diljem Hrvatske, obavijestiti i druga nadležna tijela i službe traganja, izvršiti provjere kod drugih službi (zdravstvenih ustanova, domova itd.) o njihovim eventualnim saznanjima o nestaloj osobi, zatim obaviti razgovore sa svim osobama koje bi mogle imati korisna saznanja o nestalom djetetu ili maloljetnoj osobi, pregledati objekte, prostorije i vozila osobito doma ili drugog mjesta gdje je nestala osoba boravila ili u kojima bi se eventualno mogla nalaziti, a povrh toga i obilaziti otvorene i zatvorene prostore koji su poznati kao mjesta okupljanja djece i maloljetnih osoba, pregledati snimke videonadzora, objaviti fotografiju i podatke o nestaloj osobi u sredstvima javnog priopćavanja itd.

Također, sukladno st. 1. i 2. članka 68. Zakon o policijskim poslovima i ovlastima, policijski službenici mogu u svrhu traganja za osobom zatražiti od davatelja komunikacijskih usluga provjeru istovjetnosti, trajanja i učestalosti komunikacije s određenim elektroničkim komunikacijskim adresama te utvrđivanje položaja komunikacijskog uređaja, kao i utvrđivanje mjesta na kojem se nalaze osobe koje uspostavljaju elektroničku komunikaciju te identifikacijske oznake uređaja.[217]

4. OTVORENI IZVORI NA INTERNETU I INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

Temeljni je cilj ovog rada da se, pored pravnog temelja za postupanje policijskih službenika u slučajevima traganja za djecom i maloljetnicima, prikaže doprinos društvenih mreža i drugih otvorenih izvora na internetu u potragama, odnosno ukratko pokazati kako se pomoću mrežnih pretraživača, društvenih mreža, blogova, foruma i sličnih izvora može locirati nestalo dijete ili maloljetnik.

Brzi razvoj mobilnih telefona i mobilnog pristupa internetu omogućio je razvijanje različitih aplikacija za mobilne platforme (mobilne telefone, tablete, prijenosna računala i sl.) koje omogućavaju građanima da lociraju svoj otuđeni mobitel ili prijenosno računalo. Također, one omogućavaju roditeljima da, uz malo tehničkog znanja, relativno lako prate trenutnu lokaciju svoje djece, odnosno lokaciju članova obitelji i prijatelja. Isto tako, ove aplikacije pomažu i policiji u lakšem pronalaženju djece koja su se udaljila od kuće, pobjegla iz

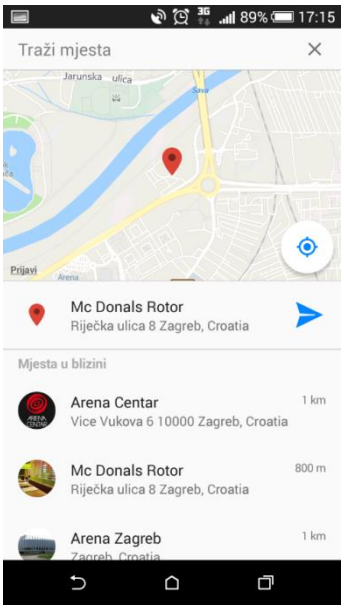
[217] Zakon o policijskim poslovima i ovlastima, NN 152/08., 76/09., 80/11., 121/11., 91/12. , 143/12., 56/13., 145/13. i 152/14. http://zakon.hr/z/174/Zakon-o-kaznenom-postupku od 4. 5. 2016.

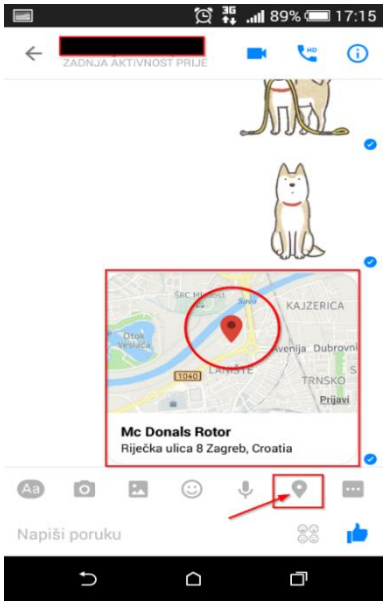
ustanove ili su nestala pod nerazjašnjenim okolnostima. Danas postoji i više aplikacija koje su besplatne, većina njih ima svoje inačice za sve danas vodeće operativne sustave poput Androida, iOS-a, Windowsa i Linuxa te ih se lako može pronaći na službenim stranicama odnosno u mrežnim trgovinama. Većina aplikacija određuje lokaciju koristeći globalni položajni sustav (GPS) mobilnog uređaja. Za brže određivanje lokacije mogu koristiti i bežične mreže (WiFi mreže) te mobilnu mrežu. Pomoću ovih aplikacija korisnici mogu međusobno razmjenjivati i kratke poruke, npr. mogu poslati poruku kad su u opasnosti, a u toj poruci će biti integriran i podatak o njihovoj lokaciji.

U slučajevima kada je policiji prijavljen nestanak djeteta ili maloljetnika, a on i njegova obitelji koristi ovakvu aplikaciju, poželjno je od obitelji zatražiti pristup, iako se može dogoditi da je uređaj isključen ili nije u dometu mreže, odnosno da je nedostupan. Pregledavajući zabilježene podatke na uređaju (povijest kretanja mobilnog uređaja – mobilni uređaj i nestala osoba ne moraju biti zajedno) može se doći do korisnih podataka o vremenima i lokacijama na kojima je uređaj bio.

No osim ovih, na neki način specijaliziranih aplikacija, i većina današnjih aplikacija za komuniciranje kratkim porukama, poput npr. Vibera ili Facebook Messengera, također omogućava korisniku da s porukom podijeli i svoju trenutnu lokaciju, što isto može biti jako korisno kada se traga za nestalim djetetom ili maloljetnikom.

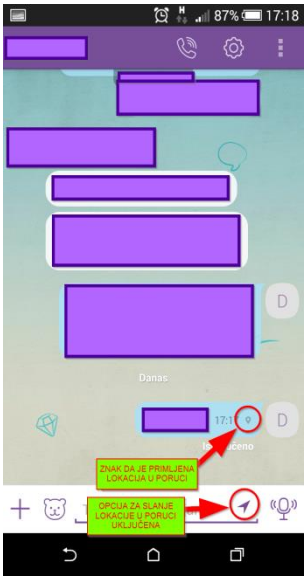
Slika 1. Aplikacija Family Locator

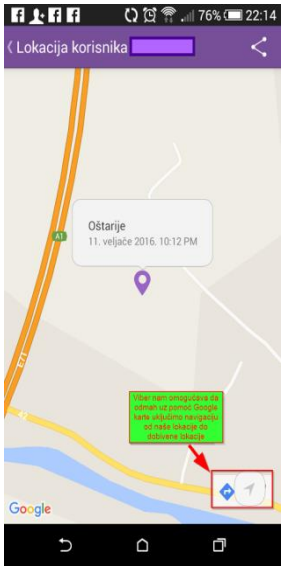




Slika 2. Facebook Messenger - slanje lokacije

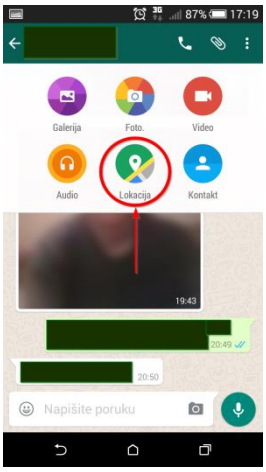
Slika 3. Facebook Messenger - primljena lokacija





Slika 4. Viber

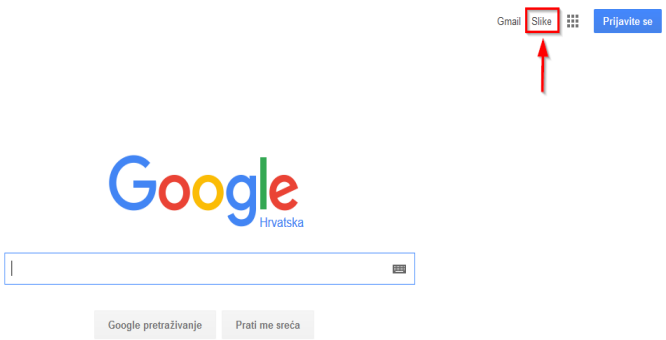
Slika 5. Viber



Slika 6. WhatsApp

Korištenjem otvorenih izvora na internetu može se doći do korisnih podataka o tome gdje se netko u prošlosti nalazio ili gdje se trenutno nalazi, a ako otvorene izvore uparimo sa zakonskim mogućnostima koje policija ima na raspolaganju (kao što su provjere IP adresa i sl.), otvaraju se brojne mogućnosti koje nam mogu pomoći u pronalasku nestalih osoba. U tekstu koji slijedi navest će se samo neke od tih mogućnosti.

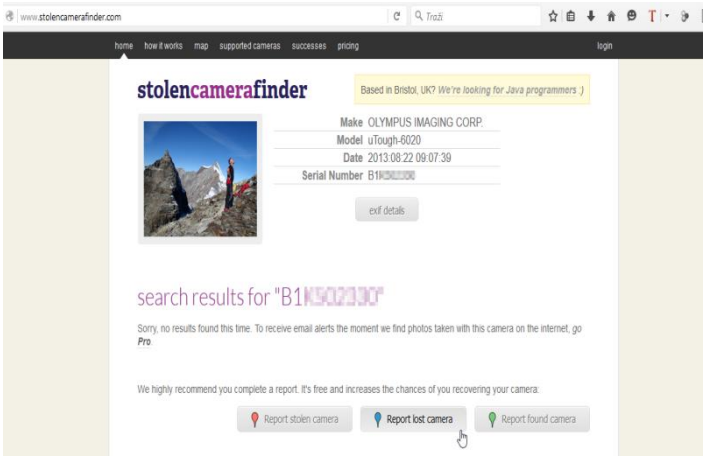
Google je danas vjerojatno najmoćnija tražilica i dobro mjesto na internetu za početak svakog traganja za nestalom osobom. Osim što možete "googlati" razne pojmove, tražilicom Google možete pretraživati i internetske fotografije. Ako je dijete pobjeglo od kuće, ali mrežno objavljuje fotografije, može se pretraživati internetske fotografije koristeći Google te čak doći do lokacija na kojima su eventualne fotografije nestale. Danas postoje razni dodatci (proširenja) za mrežne preglednike koji olakšavaju ovakvo traženje, pa nije ni potrebno napuštati stranicu (lokaciju) na kojoj je pronađena određena fotografija koja je postala predmetom interesa i za koju se misli da može pomoći u traganju za nestalom osobom. Desnim klikom miša na fotografiju i odabirom opcije *Search Image by Google* (ovo je primjer proširenja pod nazivom *Google Image Search* za mrežni preglednik Mozilla Firefox) pretražuje se internet za odabranu fotografiju.



Slika 7. Google - opcija pretraživanja fotografija

No, osim Googlea, postoje brojne druge mrežne tražilice i servisi koji nam mogu pomoći, primjerice http://www.stolencamerafinder.com/ koji npr. služi za traženje ukradenih kamera. Naime, autor ove stranice bio je žrtva kaznenog djela kada mu je netko otuđio njegov digitalni fotoaparat. On je iskoristio činjenicu da danas na internetu postoje razni servisi koji omogućavaju besplatno mrežno pohranjivanje i objavljivanje fotografija, pa je pokrenuo ovo mrežno sjedište i napravio program za pretraživanje spomenutih servisa i bilježenje podataka o serijskim brojevima kamera (i drugih identifikacijskih podataka) kako bi se moguće saznalo je li netko i tko koristio otuđenu kameru, odnosno na mrežu postavio fotografiju napravljenu njome.

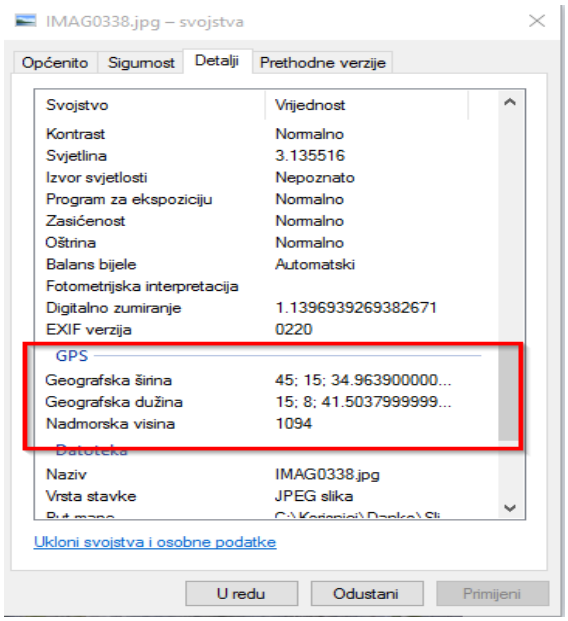
Uz pomoć ovog servisa i samo jedne pronađene fotografije koja je napravljena fotoaparatom ili mobitelom nestalog djeteta može se u određenim okolnostima čak pronaći to nestalo dijete. Naravno, preduvjet za to jest da nam je poznat serijski broj fotoaparata (mobitela), koji se inače kod niza kamera nalazi u EXIF metapodatcima fotografije, na način da iz njih izvučemo serijski broj koji tražimo. Daljnjim pretraživanjem fotografija na internetu mogu se tada pronaći i druge fotografije snimljene istom kamerom, pa čak i njihova lokacija. Dakako, ova metoda, kao uostalom i sve ostale ovdje opisane, ne mora biti uspješna jer ne pohranjuju svi fotoaparati/mobiteli serijski broj uređaja u metapodatke, a i pojedina mrežna sjedišta (poput npr. Facebooka) radi zaštite privatnosti svojih korisnika uklanjanju EXIF metapodatke.



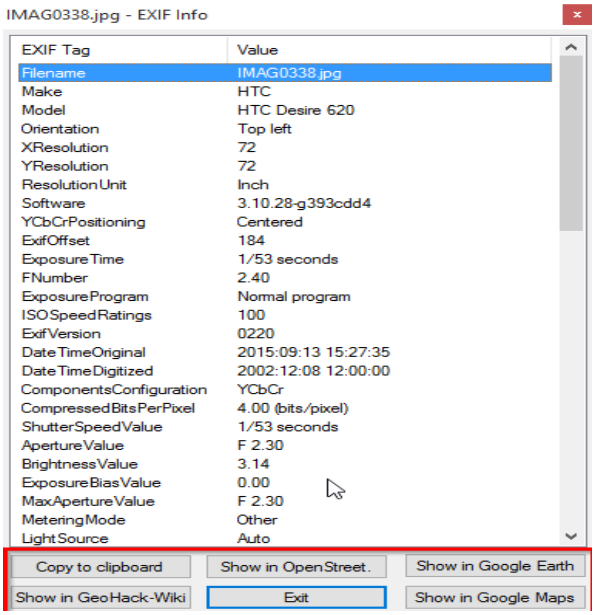
Slika 8. www.stolencamerafinder.com

Uz već opisane mogućnosti u kojima je opisano kombiniranje otvorenih izvora na internetu i metapodataka iz fotografija, postoji još jedna opcija koja je možda i najučinkovitija od svih, a to je korištenje podataka o geolokaciji iz fotografija. Danas gotovo svi mobilni uređaji imaju ugrađen GPS prijamnik, a korisnici nerijetko (posebice djeca) u postavkama fotoaparata imaju uključenu opciju bilježenja geografskih koordinata lokacije prilikom fotografiranja.

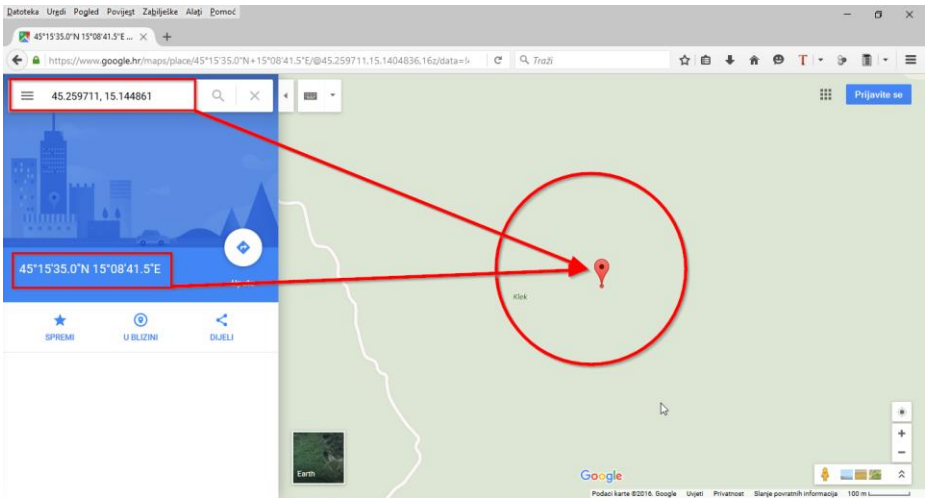
EXIF metapodatke je lako pronaći i kada korisnik ne posjeduje neki od specijaliziranih programa za pregled fotografija jer sami operativni sustavi (npr. Windowsi) imaju tu mogućnost. Besplatni programi (poput IrfanViewa i dr.) olakšavaju korisniku rad i pristup jer imaju dodatke iz koji se izravno može vidjeti gdje je fotografija snimljena.



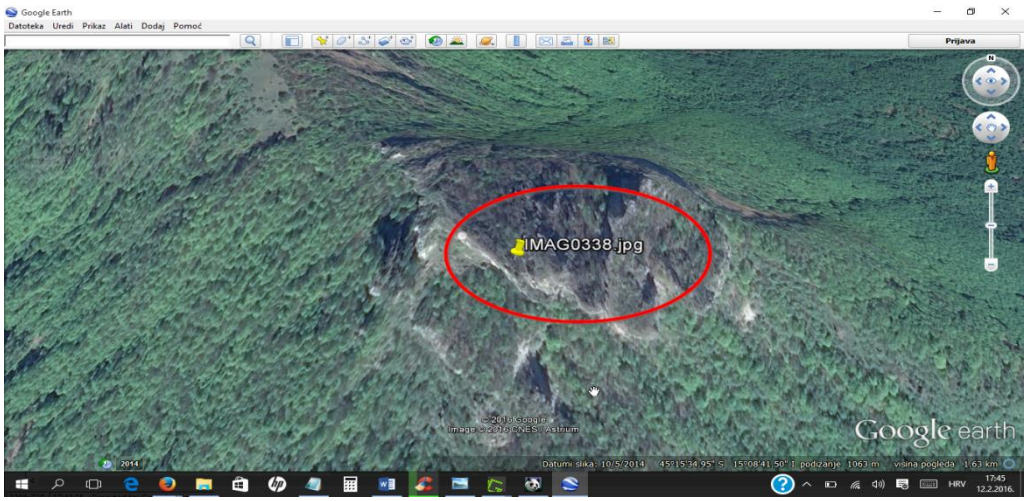
Slika 9. EXIF i GPS metapodatci fotografije prikazani u operativnom sustavu Windows



Slika 10. EXIF metapodatci prikazani u programu IrfanView



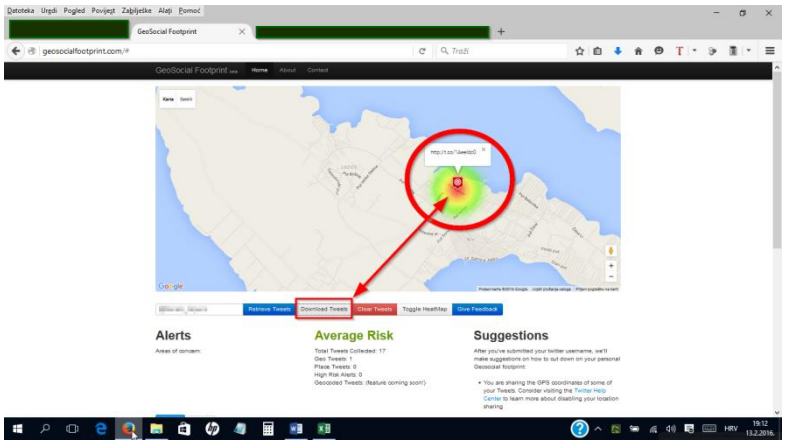
Slika 11. Koordinate iz EXIF metapodataka upisane i prikazane u tražilici Google karte



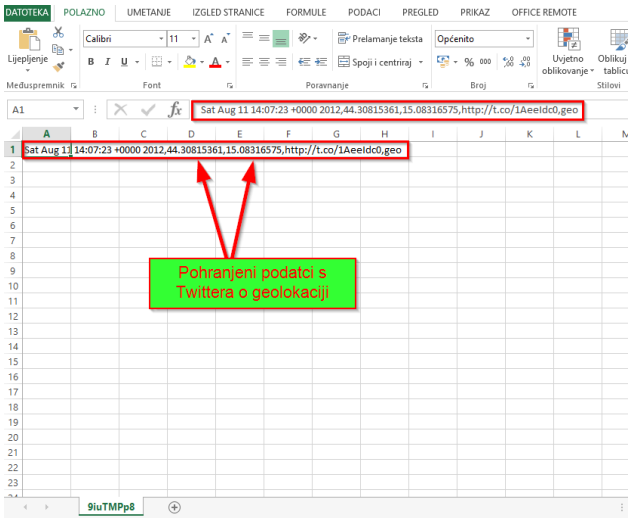
Slika 12. Mjesto nastanka fotografije prikazano u programu Google Earth korištenjem IrfanViewa

Pretraga uz pomoć fotografskih metapodataka prilično je jednostavna i vrlo korisna. No što je s društvenim mrežama? Npr. s Facebookom, Twitterom i drugim mrežama na kojima se može pronaći puno podataka koji mogu pomoći u potrazi za nestalim djetetom ili maloljetnikom?

Društvena mreža Twitter omogućava svojim korisnicima da uz svoju poruku (*twit*) ostave i svoju geolokaciju. Na taj se način, koristeći otvorene izvore na internetu, može pretražiti nečije *tvitanje* i saznati lokaciju na kojoj se osoba nalazila kada je bila aktivna na Twitteru. Ti se podatci mogu skinuti te kasnije analizirati i npr. koristiti u potrazi za nestalim djetetom ili maloljetnikom.



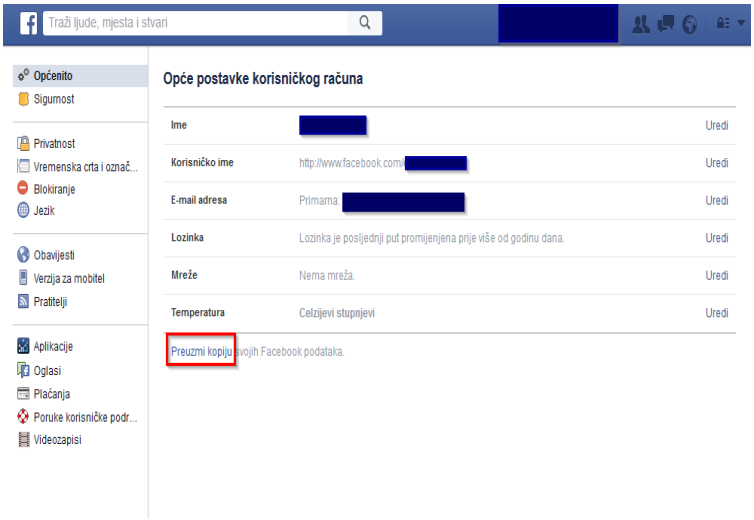
Slika 13. Primjer tvitanja s geolokacije i mogućnost pohrane podataka



Slika 14. Pohranjeni osobni podatci s Twittera

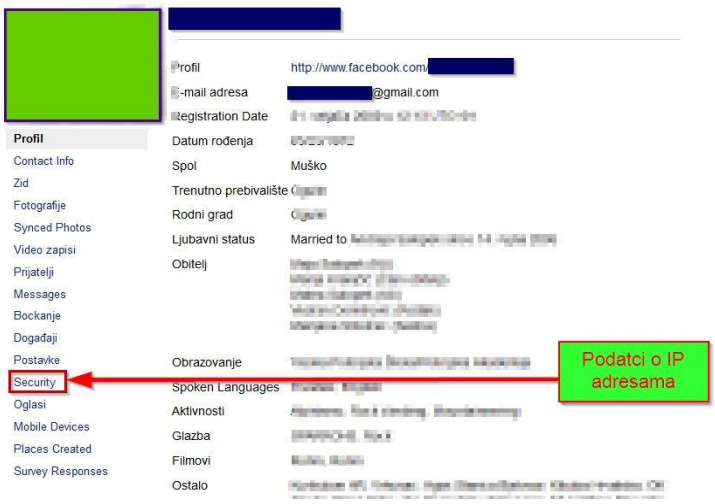
Facebook je, kako u svijetu tako i u Hrvatskoj, najpopularnija društvena mreža pomoću koje se također može odrediti lokacija nestalog djeteta ili maloljetnika ako korisnik s nekom objavom ostavi i podatak o lokaciji i ako je objava javna ili ako je osoba prijatelj s osobom kojoj ostavlja objavu. Velika prednost u traganju može biti ako roditelj ili druga djetetu bliska osoba ima pristup njegovu profilu na Facebooku jer se na taj način može preuzeti kopija profilnih podataka koji mogu pomoći u potrazi. Odlaskom na postavke računa (*Settings*) i klikom na mjesto prikazano na fotografiji koja slijedi mogu se dobiti podatci o IP adresama s kojih su vršene prijave u profil te IP adrese prigodom promjene zaporke, pa se na taj način može dobiti podatke o tome kome su konkretne IP adrese bile dodijeljene. Isto tako mogu se dobiti podatci o prijateljima, „obrisanim“ prijateljima, poruke koje su razmjenjivane, a nisu

obrisane, i – što je jako korisno – metapodatke fotografija; naravno, ako ih administrator u međuvremenu nije izbrisao.



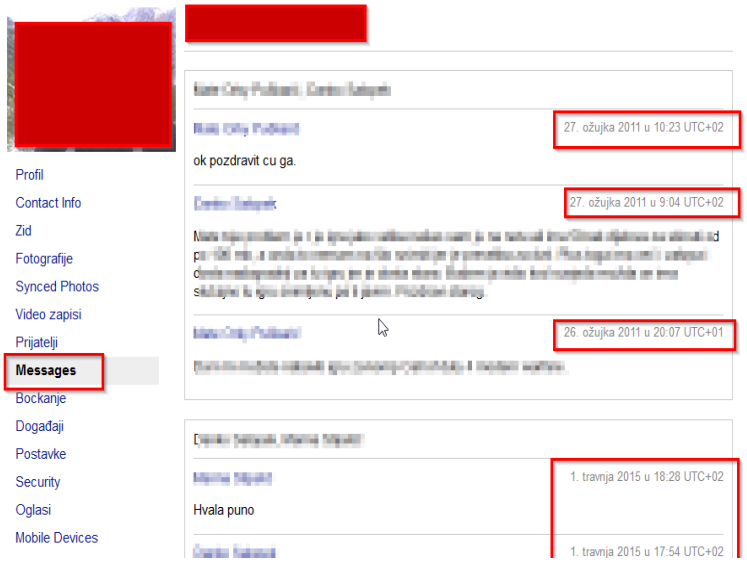
Slika 15. Opće postavke korisničkog računa na društvenoj mreži Facebook

Na sljedećih nekoliko fotografija mogu se vidjeti podatci koji mogu značajno pomoći u potrazi za nestalim djetetom ili maloljetnikom.

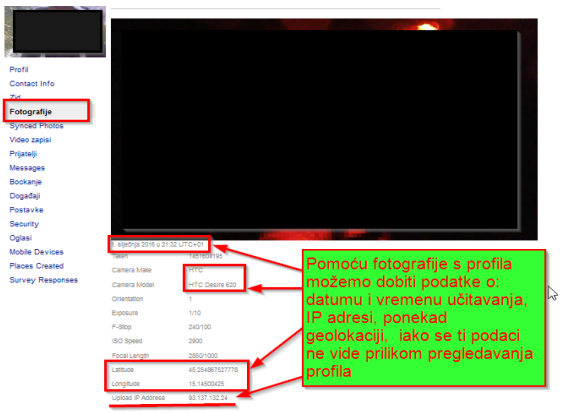


Slika 16. Poveznica na podatke s IP adresama

Slika 17. Prikaz podataka s IP adresama i drugi korisni profilni podatci

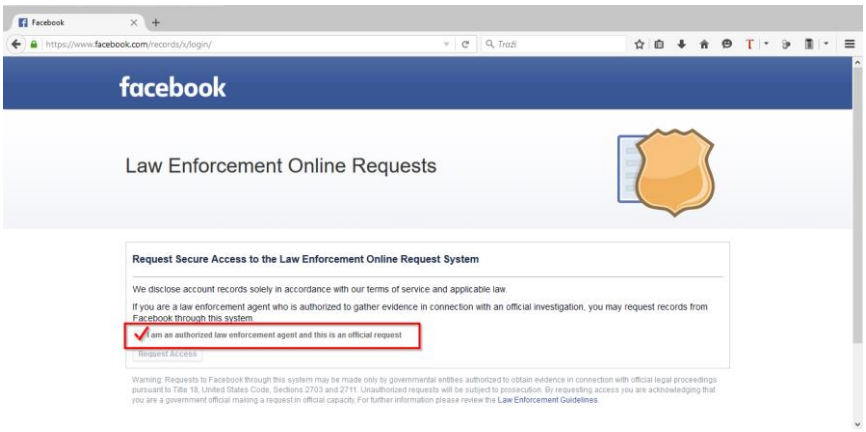


Slika 18. Neobrisane poruke na društvenoj mreži



Slika 19. Fotografija s profila koja sadrži puno korisnih podataka

Na kraju je važno spomenuti i mogućnosti, kada za to postoje zakonske osnove, da je tvrtka Facebook u obavezi na zahtjev policije dostaviti podatke o IP adresama s kojih se pristupalo nekom Facebook profilu, na temelju kojih policija može, ne samo doći do korisnih podataka već i pronaći nestalo dijete.



Slika 20. Mrežna stranica Facebook Records putem koje se podnose zahtjevi za mrežne podatke

5. ZAKLJUČAK

U radu je prikazan samo mali dio složenosti etiologije i fenomenologije nestanaka djece i maloljetnika, te mjera i radnji koje policija provodi tijekom traganja za nestalom djecom. Kao što smo i ranije naveli, cilj ovog rada je bio prikazati kako se pomoću pretraživača, društvenih mreža i drugih aplikacija, uparivanjem s podacima dobivenim uobičajenim policijskim radom može locirati nestalo dijete ili maloljetnika.

Svjesni činjenice da se danas veliki broj kaznenih djela čini isključivo putem računala i računalnih sustava, policija mora promišljati kako nove tehnologije iskoristiti i staviti u funkciju, kako u traganju za nestalim osobama tako i u sprječavanju i otkrivanju kaznenih djela. Kako bi policijski službenici bili uspješni u tome, moraju se kontinuirano stručno usavršavati ali sustavno. Ministarstvo unutarnjih poslova ne smije dozvoliti, da policijski službenici zaostaju za suvremenim tehnološkim postignućima koja uveliko mogu doprinijeti kvaliteti kriminalističkih istraživanja.

LITERATURA

Buljan Flander, G. (2011), *Trebamo li brinuti? Priručnik o adolescentima za roditelje i stručnjake,* Poliklinika za zaštitu djece grada Zagreba, http://www.poliklinika-djeca.hr/publikacije/trebamo-li-brinuti/ od 14. 3. 2016.
Jelavić, M. (2011), "Samovoljno udaljenje djece od kuće ili iz ustanove", http://www.nestali.hr/default.aspx?id=49 od 14. 3. 2016.
Marušić, D. (2011), "Bježanje djece iz odgojnih ustanova", http://www.nestali.hr/default.aspx?id=37 od 14. 3. 2016.
Pravilnik o načinu postupanja policijskih službenika, NN 89/10. i 76/15. http://www.propisi.hr/print.php?id=2160 od 14. 3. 2016.
Statistički pokazatelji bjegova iz odgojnih ustanova i udaljenja iz obiteljskog doma djece i maloljetnika za razdoblje od 2009. do 2015. godine, MUP, Ravnateljstvo policije, Uprava kriminalističke policije, Odjel maloljetničke delinkvencije i kriminaliteta na štetu mladeži i obitelji od 10.1.2016.
Šuperina, M., Gluščić, S. (2003), "Učestalost prijava nestanka osobe u Republici Hrvatskoj i postupanje policijskih službenika u traganju za nestalom osobom: Aktualizacija problema", *Pravni vjesnik*, 19(3-4), 151–187.
Šuperina, M., Dujmović, Z. (2011), "Nestanak osobe: utvrđivanje početnih istražnih situacija kod traganja za nestalom osobom (I. dio)", *Policija i sigurnost*, 1/15, Zagreb, MUP RH.
Zakon o policijskim poslovima i ovlastima, NN 152/08., 76/09., 80/11., 121/11., 91/12., 143/12., 56/13., 145/13. i 152/14. http://zakon.hr/z/174/Zakon-o-kaznenom-postupku od 14. 3. 2016.

Davorka Martinjak
Danko Salopek
Renata Odeljan
Suzana Kikić

USE OF SOCIAL NETWORKS AND OTHER OPEN SOURCES OF INFORMATION ON THE INTERNET FOR THE PURPOSE OF FINDING MISSING CHILDREN AND JUVENILES

Summary

In the last 20 years, with Internet becoming widely used, many experts still debate the advantages and disadvantages of using the Internet. With a wide range of quality content, and applications, there is no doubt that there are risks associated with the use of modern technologies, particularly for children and young people. However, the authors of this paper will provide a review on how social networks and other open sources on the Internet can contribute to help the police in conducting police investigations in cases of escapes and removal of children from the family home or educational institutions. How to locate a missing child, with the help from Web browsers, social networks, blogs, forums, etc. Today we have a lot of Internet search engines for different purposes including the popular Google or some other search engines that can be used in certain cases: Yahoo Search, America On Line;

Microsoft's search engine, GoTo Webcrawler, Wikipedia. Also, search engines are very helpful and Meta search engines that instead of users send queries to multiple search engines for ex.: xquick; Dogpile Mamma; Search.com; Carot2 and search engines targeted search for specific persons such as: https://pipl.com/; http://com.lullar.com/ and so on. In addition to searches an important role in finding missing children lays on social networks especially popular Facebook, Google+ and many others. However, it is important to note that the data obtained on the Internet should always be taken with caution, but linking these data with the official data may be the key to success in finding missing persons.

Key words: *Internet, open sources, missing children and juveniles, social networks.*

PROFFESIONAL PAPER

Vladimir Pivovarov[218]
Marjan Nikolovski[219]

SECURING THE CRIME SCENE – A PREREQUISITE FOR SUCCESSFUL CRIME SCENE INVESTIGATION

Summary

The purpose of the crime scene investigation is to help establish what happened at a crime scene. Unfortunately, practice shows that mostly police officers conduct the crime scene investigation. The investigators try is to find micro and macro trace evidence at the crime scene that occurred as a result of the crime, in a place originated from the perpetrator, the tools of commission or witnesses, if found.
Securing the crime scene until the arrival of crime scene investigators is a very important segment preceding the actual investigation. Any presence of uninvited people at the scene can change it (intentionally or unintentionally), which could greatly hinder the work of the investigators. This could mislead the investigation or give the suspect or accused person an opportunity to deny evidence that may incriminate them in court.

***Key words*:** crime scene investigation, securing the crime scene, perpetrator of a criminal act, victim to criminal act.

1. INTRODUCTION

A general rule of criminology is that from the moment of committing the crime all material, as well as verbal evidence that were created due to committing of the crime. At the crime scene, material evidence are primarily biological clues. These clues, because of weather conditions, are very often losing their quality partially or completely. Therefore, in the further procedure, they are difficult to be forensically examined, or they can be completely unusable.

During the time, verbal evidence can also be distorted, because of the past period or by accepting suggestions from interested persons. However, in criminologist practice (with unexplained reasons) there is not much attention paid to the securing of the crime scene, which usually comes before the inspection. Therefore, the investigation can be totally misguided, due to lack of expertise of the police officers who first arrive at the crime scene or the lack of the basic means for successfully performing this procedure (Angeleski, 2007). Due to the abovementioned, this study will make efforts to establish a basic protocol, which is supposed to be followed by the police officers. The police officers should be directed to follow the procedures, according to their description, with a list of their work tasks (Angeleski, 2007).

[218] Associate Professor Vladimir Pivovarov, MIT-University in Skopje e-mail: pivovarov_vladimir@yahoo.com
[219] Associate Professor Marjan Nikolovski, Faculty of Security in Skopje, e-mail: mnikolovski@fb.uklo.edu.mk

2. ACTIONS OF THE POLICE OFFICERS IN SECURING THE CRIME SCENE

Initial actions should be undertaken by the police officers to secure the crime scene. In terms of using clues and objects as the evidence (detected modifications of the objects), which are subject of interest of the forensics, as well as for providing witnesses of the criminal act, and to detect and identify of the perpetrator, the modern criminal activity begins to secure the crime scene (Angeleski, 2007). There is a moment of the temporary notification of the committed criminal act by the operation center which is on duty, up to the issuing of an order to the authorized officials to arrive on the crime scene at the shortest notice. There is certain period during which the crime scene could underwent certain modifications by an intentional action, which is undertaken by certain persons interested in the specific crime (the perpetrator and his/her accomplices), or unintentionally by providing help to the victim, or as a result of carelessness or curiosity. The second influence on the possible modification of the crime scene is the weather conditions, which can destroy part or all of the clues (primarily the biological ones), occurring during or after the perpetrating the criminal act (rain, sun or snow). On the other hand, the criminological practice indicates the fact that witnesses are often present at the crime scene, following the arrival of the police. Their verbal evidence is the most realistic due to several reasons:

- a short period passed following the committing of the criminal act, which was perceived up to the hearing (the memories are still fresh),
- possibility that the witnesses are influenced by the affected person or that they are also suspect is almost impossible,
- hearing sounds or speaking at the crime scene immediately after committing the criminal act, does not provide the witness to sporadically add his/her own presumptions (this often occurs during the later hearing).

Most often, the uniformed authorized persons (UAP) arrive first at the crime scene. Their task is to establish whether some event is a matter of criminal act, the need for other legal action or just false notice. If it is a matter of criminal act, they notify the operations center on duty, after which the following measures and actions should be taken (Angeleski, 2007). These measures are, as follows:

- UAP determine, mark and secure the crime scene, at which the inspection should be made depending on the criminal act and upon their own estimation,
- prohibition on access of unauthorized or non-involved persons at the crime scene, which is noticeably marked and at which the investigation should be performed,
- UAP are taking swift and safe measures in order to prevent alteration of the crime scene (because of a vis major, such as rain, sun, ice or snow) or contamination or clue spoliation,
- detention and identification of persons found near the scene, who could give useful information of the criminal act that has happened,
- UAP are adhering to the core principle “do not touch”, but also taking measures for non-involved persons not to move or enter into the scene, which should be roped off with a police tape saying “POLICE LINE - DO NOT CROSS!” (Vodinelić, 1995),

- the movement of the investigative judge, the public prosecutor and the authorized official persons at the crime scene must not be reckless; it must not violate the rule of criminology “process first”, and they should move from the periphery to the center of the crime scene in order not to distort the clues at the crime scene.

The errors that have arisen in the protected area, may never be rectified again. Taking into consideration the difference of the various criminal acts, but also the difference of the identical criminal acts, there is no rule of thumb for the manner of acting in a specific place, rather the general rules of criminology should be taken into consideration. General rules of criminology provide the best results in the search of clues at the crime scene and its surroundings (Vodinelić, 1995).
In case when it is necessary to help a victim on the crime scene, during the contact with him/her or with the objects around, the authorized official person is obliged to use gloves, in order not to contaminate the clues that the perpetrator has left at the crime scene, the victim or the objects. When certain visible clues coming from the perpetrated crime are protected (and thus dislocated), the place of their finding should be marked and photographed, whenever it is possible. It is obligatory for these actions to be noticed in the sketch and in the report (Maksimović, 2000).

The basic rule for the authorized official persons (AOP) who were the first to arrive on the crime scene, is to register the time of arrival, as well as to start taking the preliminary measures and to individually register them (Maksimović, 2000). The victim, or his/her friends or relatives, or all the present people, should be forbidden to remove or touch the objects in order not to alter the situation. The next task of the AOP in charge of securing the crime scene is to determine the surface of the area that should be secured. The final decision regarding the area that should be secured will be made on the part of the head of security, following a previously performed thought reconstruction of the order of the criminal act. Regardless of the weather conditions or the type of criminal act itself (murder, attempted murder or suicide and similar), the official persons must not leave the crime scene. In exceptional situations when the case involves a search of the perpetrator of the criminal act or administering first aid to the victim, the official person may leave the crime scene, but having first found people who would take the role of securing the crime scene (Maksimović, 2000).

Depending on the modus operandi of the committed act, as well as the type of criminal act (robbery, banditry, rape, homicide, suicide, arson, explosion and similar), adequate methods of securing the crime scene should be in place (Maksimović, 2000). Factors that affect the choice of the method of securing the crime scene, are classified into the three main groups:

1. the manner in which the crime is committed,
2. the objects that were used by the perpetrator while committing the crime,
3. the location of the place of the crime scene (open or closed space).

When securing the crime scene the AOP should respect the following main rules (Maksimović, 2000):

1. Nobody do not have to touch anything.
Each touching of the objects, found at the crime scene can cause serious problems in the further investigation, because thus contamination could misguide the entire investigation.

2. Nothing has to be changed.
Each change implies touching of the objects, which are material evidence. Therefore, each changing the original state (a natural image that was caused when the crime took place) of the crime scene, can cause that the criminologist can acquire a false image, during observing what has happened and how it has happened, when cartain crime was committed.

3. Reducing unnecessary movements to a minimum.
Each movement in the area where the inspection is carried out and the ground where the crime took place (no matter how careful we are), can destroy micro clues left there after the crime. On the other hand, the persons who are present in that same area leave their footprints, also leave other clues which can lead to a serious confusion during the investigation (Maksimović, 2000).

These are the reasons why the police officers should take the following measures and actions (Maksimović, 2000):

- non-involved persons must stay at a certain distance,
- witnesses of the crime can be legitimized and must be kept in isolation, until operational workers arrive,
- careful observation of the locality of the crime scene, as well as the persons who are in a walking distance (often the perpetrator returns at the crime scene),
- continuous reporting and consulting with the operational center on duty,
- if the perpetrator of the crime is caught in flagranti, he/she is detained or arrested,
- if the officials that came first at the crime scene are not sufficient to secure it, through the operational center which is on duty, they shall call for back-up according to the assessment of the head of security (crimes that were committed by using explosive devices and where there are casualties, injured people or great property damage).

After determining the space that need to be secured, it is necessary to take the following measures and activities (Jackson and Jackson, 2011):

- If there is a need of an ambulance or a fire engine to intervene they must be warned not to destroy clues, and they must be coordinated for this measure by the officials responsible for securing the crime scene,
- Officials must pay attention to the non-involved persons, if the victim is in a poor health condition, but at the same time is still able to communicate, the official must conduct an initial informative talk with him/her, and note it down (preferably to make an audio recording),

- If at the crime scene there are persons who can be suspects, must not be allowed to help the victim,
- Weather conditions when securing the crime scene must be noted down,
- Generalities must be taken from everybody present at the crime scene,
- If there is a deceased person on the crime scene, he/she must be covered with a suitable cover that can be found nearby,
- Everything that was observed and all measures and actions undertaken by the official, must be noted down in the report.

3. FORENSIC PRINCIPLES AND SECURING THE CRIME SCENE

When securing the crime scene, authorized officials must adhere to the forensic principles, as following (Maksimović, 2000):

- principle of swiftness and surprise (operability),
- principle of confidentiality (of official secrecy),
- principle of truth,
- principle of objectiveness,
- principle of orderliness,
- principle of thoroughness,
- principle of persistency,
- principle of cost effectiveness.

When securing the crime scene, the control structure of the real (material) evidence must be taken into account. This control structure includes, as following (Maksimović, 2000; Jackson and Jackson, 2011):

a) disabling unauthorized disposal or transfer of the right to use the actual evidence,
b) rounding the responsibility for storage of evidence,
c) a list of material evidence, their identification label and determining the location where they are kept as well as the conditions in which they are kept,
d) entrusting material evidence to a third party: a natural or legal entity approved by a competent authority,
e) identification data and position of the person who is entrusted with the evidence,
f) explanation of the reasons for entrusting evidence
g) providing documented evidence that ensure entrusting the evidence for safekeeping is done legally,
h) permission for a competent body which eventually receives the evidence for safe- keeping.

It could be concludes from the above mentioned that securing the crime scene, in general, consists of five main activities (Maksimović, 2000):

1. determining the crime scene,
2. marking the crime scene,
3. distancing the persons away from the crime scene,
4. protecting objects and clues originating from the committed crime,
5. finding witnesses for the crime if there are any.

4. CONCLUSION

Securing the crime scene is the foundation for the inspection that follows and also a foundation for the further investigation which is supposed to build the "house" of evidence (Vodinelić, 1995). If before performing the inspection, material evidence were destroyed (completely or partially) or contaminated, either by the weather conditions, or deliberately by an involved party, the inspection becomes only a form which misguides the further investigation. Due to unknown reasons, our criminological practice does not pay attention to this very important process activity. In order to avoid such mistakes in the future, some established actions that the police officers can undertake when they are securing the crime scene, have to be determined. For ensuring the quality inspection, two basic requirements have to be met (Jackson and Jackson, 2011):

1. continuous education of competent police officers, who are engaged to secure the crime scene,
2. providing the necessary technical equipment for successfully securing the crime scene (a forensics kit that including sketches, pens, photo camera, police tape for closing the crime scene, nylon etc.).

Only this type of actions, when securing the crime scene, allows a quality inspection. Securing may result with successful detecting the micro and macro clues that are occurring when the crime was committed. Of course, we do not have to forget the personal (verbal) evidence of witnesses on the crime scene.

REFERENCES

Angeleski, M. (2007). *Kriminalistička taktika 2.* Skopje: Grafos Kumanovo.
Vodinelić, V. (1995). *Kriminalistička taktika 1*, Skopje: Univerzitet Kiril i Metodij.
Maksimović, R. (2000). *Kriminalistička tehnika*. Beograd: Policijska akademija.
Jackson, R.W., Jackson, J. M. (2011). *Forensic science*. London: Pearson.

STRUČNI RAD

Mile Matijević[220]

Aleksandar Miladinović[221]

KRIMINALISTIČKI ASPEKT FACEBOOK-a

Sažetak

Usljed kvalitativne i kvantitativne ekspanzije Facebooka, posljedica je razumljiv porast mnogobrojnih negativnih, u prvom redu kriminalnih aktivnosti na ovoj društvenoj mreži ili korištenjem mogućnosti ove društvene mreže. S obzirom na specifičnosti okruženja Facebooka, nameće se i neophodnost specifičnog reagiranja na ove negativne pojave. To se u prvom redu odnosi na kriminalističke specifičnosti reagiranja u virtualnom okruženju, korištenjem određenih mogućnosti, metoda i sredstava koja policiji stoje na raspolaganju, ovisno od kadrovskih, materijalno-tehničkih i normativnih ograničenja. U radu se ukazuje na potrebu prisutnosti policije u virtualnom okruženju, pogotovo na Facebooku, nakon čega se daje osvrt na određene mogućnosti koje Facebook može pružiti u kriminalističkom radu policije. Primjerice, u otkrivanju kaznenih djela i izvršitelja, identificiranju i lokalizaciji (pronalasku) izvršitelja, te na mogućnosti prikupljanja operativnih saznanja i informacija glede rasvjetljavanja i dokazivanja konkretnih kriminalnih (planiranih, pripremanih ili realiziranih) aktivnosti. Kriminalistički aspekt Facebooka se promatra kroz određene mogućnosti koje su svim korisnicima Facebooka na raspolaganju (pa tako i policijskim službenicima), kao i kroz određene mogućnosti koje podrazumijevaju sofisticirano znanje i tehničko-tehnološke resurse. Također, ukazuje se i na značaj prevencije zloupotrebe Facebooka među korisnicima, kao i na mogućnosti korištenja Facebooka u preventivne svrhe.

Ključne riječi: *Facebook, internet kriminal, policija na Facebooku, sigurnost na Facebooku.*

1. UVOD

Društvene mreže su posljednjih nekoliko godina jedna od najpopularnijih, ako ne i najpopularnija usluga na internetu. Međutim, kvalitativna i kvantitativna ekspanzija društvenih mreža svakako ima i svoju "tamnu stranu". Naime, usporedno s ekspanzijom društvenih mreža, primjetna je i ekspanzija kriminalnih aktivnosti na društvenim mrežama ili prema korisnicima društvenih mreža. Navedenome je razlog, prije svega, masovnost korisnika društvenih mreža, ali isto tako i needuciranost korisnika o sigurnosnim rizicima na

[220] Prof. dr. Mile Matijević, Fakultet pravnih nauka Univerziteta za poslovne studije Banja Luka, e-mail: *matijevicdrmile@gmail.com*

[221] Aleksandar Miladinović, mr., Visoka škola unutrašnjih poslova Banja Luka, e-mail: *aaleksandarbl@yahoo.com*

društvenim mrežama, vlastita pasivizacija mogućnosti zaštite, virtualni aspekt okruženja u kojem egzistiraju ove mreže i slično.

Usljed navedenog, razni se oblici kriminaliteta i drugih kriminogenih i asocijalnih pojava, kao i sami akteri navedenih aktivnosti, "preseljavaju" u okruženje društvenih mreža, s obzirom na to da im navedeno okruženje omogućuje da gotovo cjelokupne faze kriminalne aktivnosti (planiranje, pripremanje, vrbovanje žrtava, osiguranje sredstava, sama realizacija, pribavljanje koristi) realiziraju "iz sobe", odnosno korištenjem usluga interneta preko društvenih mreža, znajući da je mogućnost otkrivanja njihova identiteta minimalna. To je uvjetovalo ekspanziju klasičnih kriminalnih aktivnosti (prijevare, krađe, razni oblici nasilja, antiestablišmentsko djelovanje, terorizam), ali, isto tako, i suvremenih oblika kriminalnih aktivnosti (krađe identiteta, krađe vremena, internetskog piratstva, internetskog nasilja). U tom kontekstu, kao najučestaliji, ali naravno ne i jedini oblici kriminalnih aktivnosti na društvenim mrežama, promatraju se prijevare, krađe identiteta, piratstvo, pornografija, pedofilija, terorizam, vršnjačko nasilje, govor mržnje, te razni oblici antiestablišmentskog djelovanja korištenjem društvenih mreža (Miladinović, Petričević, 2012: 257).

Kada je u pitanju odražavanje mnogobrojnih različitih kriminalnih aktivnosti na internetu korištenjem mogućnosti koje pružaju društvene mreže, ni Facebook u navedenome nije iznimka. Kao i na drugim društvenim mrežama, tako se i na Facebooku izražava niz kriminalnih aktivnosti koje imaju karakteristike internetskog kriminaliteta, naravno, prilagođene specifičnom okruženju u kojem egzistira ova društvena mreža. Također, uslijed mnogobrojnih specifičnosti samog Facebooka kao društvene mreže u odnosu na druge društvene mreže, a pogotovo u odnosu na druge usluge interneta, kriminalne aktivnosti koje se iskazuju na Facebooku (unutar Facebook okruženja ili uz pomoć određenih mogućnosti Facebooka) imaju određene specifičnosti, ali se ipak ne može govoriti o novim pojavnim oblicima predočavanja na Facebooku internetskog kriminaliteta koji nije zastupljen na drugim društvenim mrežama ili na drugim uslugama interneta, već samo o djelomično drugačijim oblicima iskazivanja internetskog kriminaliteta. Drugim riječima, bez obzira na kvalitativni i kvantitativni aspekt kriminalnih aktivnosti koje se odražavaju na Facebooku ili koriste mogućnosti Facebooka ili egzistiraju u specifičnom Facebook okruženju, oni nisu novi pojavni oblici ni kriminaliteta, ni internetskog kriminaliteta, već samo prilagođeni, specifični oblici izražavanja poznatih, a moglo bi se reći i u internetskom okruženju etabliranih oblika manifestiranja internetskog kriminaliteta (Đukić, Miladinović, Petričević 2013).

2. KRIMINALNE AKTIVNOSTI NA FACEBOOKU

S obzirom na to da je "prosječan korisnik Facebooka, generalno gledano, netko s ispodprosječnim znanjem rada na računalu i skromnim iskustvom na *webu*", a imajući u vidu pravila privatnosti i anonimnost korisnika, njihovu masovnost, kao i Facebook okruženje, jasno je da je Facebook idealno mjesto za razne prijevare, krađe, sumnjive financijske transakcije, ucjene i iznude, pornografiju i slične kriminalne aktivnosti. Pored navedenog, Facebook je idealan i za širenje određenih ideja i sadržaja, ali i za prijetnje drugima, iz čega je jasno da je kvalitativni i kvantitativni fenomenološki aspekt Facebooka svakako i nemjerljiv i nepredvidiv (Banović, Miladinović, 2010: 46).

Praksa je pokazala da niz kriminalnih aktivnosti mogu imati određenu, nerijetko i posrednu, ponekad čak i latentnu, pa i fragmentarnu vezu s Facebookom, ali ta veza ipak postoji. Usljed navedenog, opravdano se postavlja pitanje povezanosti kriminalnih aktivnosti s Facebookom, bez ulaženja u kauzalistički odnos između konkretnih kriminalnih aktivnosti i Facebooka. Drugim riječima, nameće se pitanje na koji način su kriminalne aktivnosti koje se dovode u vezu s Facebookom povezane.

Najopćenitiji odgovor na pitanje je da (gotovo) svi oblici manifestiranja kriminalnih aktivnosti mogu imati određenu vezu s Facebookom, bez obzira na to da li se te kriminalne aktivnosti (u potpunosti ili samo jedan njihov dio) ispoljavaju na Facebooku, da li se samo ispoljavanje kriminalnih aktivnosti koristi mogućnostima koje im pruža Facebook i samo Facebook okruženje, eksploatiraju li kriminalnu aktivnost na Facebooku ili korištenjem mogućnosti Facebooka, koriste li Facebook za pripremanje ili planiranje, pa i za samu realizaciju kriminalne aktivnosti ili pojedinih faza kriminalne aktivnosti.

Upravo navedeno pruža uvid u mogućnosti ispoljavanja kriminalnih aktivnosti koje se mogu povezati s Facebookom. Drugim riječima, na Facebooku se mogu realizirati cjelokupne kriminalne aktivnosti, bez obzira na to što su posljedice primjetne i u realnom okruženju. Primjer za to bi predstavljala krađa identiteta kroz krađu profila korisnika Facebooka. Na Facebooku se mogu realizirati i samo dijelovi kriminalne aktivnosti, dok se manji ili veći dio kriminalne aktivnosti može realizirati i izvan Facebooka. Klasičan primjer za navedeno predstavlja vrbovanje žrtava pedofilije ili pornografije putem Facebooka, dok se ostali dio kriminalne aktivnosti realizira u realnom okruženju ili u internetskom okruženju. Povezanost Facebooka s kriminalnim aktivnostima može se promatrati i neizravno, gdje sam Facebook ne služi neposrednom ispoljavanju kriminalnih aktivnosti, ali se posredna veza ne može negirati. U ovom slučaju, zlonamjerni korisnici koriste mnogobrojne mogućnosti Facebooka kako bi identificirali i vrbovali potencijalne žrtve kriminalne aktivnosti koja se iskazuje u realnom okruženju. Na primjer, zlonamjerni korisnici pregledom statusa i drugih informacija i sadržaja na žrtvinom profilu, znaju kada se ona ne nalazi u stanu, te u pogodnom trenutku provaljuju u stan. Isto tako, Facebook služi i za eksploatiranje same kriminalne aktivnosti koja je realizirana u realnom okruženju. Najbolji primjer za navedeno predstavlja širenje terorističke i razne druge antiestablišmentski nastrojene propagande, govora mržnje i sličnih aktivnosti, ideja i stavova, materijala. U ovom kontekstu treba navesti da ima shvaćanja po kojima se i sam Facebook promatra kao sredstvo kojem je primarna uloga ispoljavanje kriminalnih aktivnosti, odnosno uloga Facebooka, prema ovome shvaćanju, promatra se kao sredstvo koje je isključivo namijenjeno (kreirano) u određene nelukrativne, pa i kriminogene, odnosno kriminalne svrhe.

Kao što je nesagledlv i nemjerljiv kvantitativni aspekt manifestiranja kriminalnih aktivnosti na Facebooku, isto tako je i teško sagledlv kvalitativni aspekt ovih aktivnosti promatran kroz konglomerat pojavnih oblika ispoljavanja samih kriminalnih aktivnosti parcijalno promatranih kroz oblike ispoljavanja samog internetskog kriminaliteta. Na Facebooku se ispoljava cjelokupan niz kriminalnih aktivnosti koje se mogu promatrati kroz ustaljeni kriminološko-fenomenološki aspekt samog iskazivanja internetskog kriminaliteta. Naravno, navesti cjelokupan niz kriminalnih aktivnosti na Facebooku čini se bespredmetnim,

pogotovo ako se ima u vidu da mnogobrojne kriminalne aktivnosti na Facebooku još uvijek nisu učestale (ne izazivaju pozornost), a isto tako, za dosta kriminalnih aktivnosti same ih žrtve nisu ni svjesne, te tako predstavljaju tamnu brojku kriminaliteta realiziranog na Facebooku ili uz pomoć Facebooka ili korištenjem mogućnosti Facebooka. Također, treba imati u vidu da se aktualni kriminološko-fenomenološki modaliteti ispoljavanja kriminaliteta na Facebooku svakodnevno mijenjaju i usavršavaju, a pojavljuju se i novi.

Imajući na umu prethodno navedeno, ne pretendujući na konačnost i sistematičnost fenomenoloških obrazaca ispoljavanja kriminalnih aktivnosti, te uz izvjesne rezerve, uvjetno se mogu navesti sljedeći modaliteti ispoljavanja kriminalnih aktivnosti na Facebooku: krađa profila unutar koje se promatra konglomerat načina kompromitacije identiteta korisnika samom krađom profila, zatim prijevare na Facebooku, gdje se promatraju specifični (prilagođeni Facebook okruženju) oblici ispoljavanja internetskih prijevara, vršnjačko nasilje i drugi oblici elektroničkog nasilja na Facebooku ili korištenjem mogućnosti Facebooka, piratstvo na Facebooku, pornografija i pedofilija, razni oblici narušavanja privatnosti korisnika, ucjenjivanje i iznuđivanje korištenjem Facebooka, antiestablišmentski aspekt Facebooka, u okviru kojeg se promatraju tzv. Facebook revolucije, *cyber* disidentizam, insajderske aktivnosti i "zviždački" aspekt Facebooka, terorizam, ubojstva, samoubojstva, širenje zabranjenog sadržaja i propagiranje zabranjenih ideja, govor mržnje, komunikacija kriminalaca, sektaško djelovanje, trolovanje i prisustvo Hoaxa (Miladinović, 2013).

3. INKORPORIRANOST POLICIJE U INTERNETSKOM OKRUŽENJU

Internetska populacija ne gleda blagonaklono na "prisutnost" policije u samom internetskom okruženju. Navedeno je najvjerojatnije rezultat (utopističkog) promatranja "interneta kao posljednjeg bastiona slobode" kojeg internauti baštine, uslijed čega "prisutnost" policije, kao (represivnog) tijela države promatraju kao negaciju ili pokušaj negiranja ili kontroliranja ili ograničavanja te slobode. U širem kontekstu, "prisutnost" policije u internetskom okruženju, a pogotovo određene policijske (kriminalističke) aktivnosti u ovom okruženju (za koje se tradicionalno smatra da je mjesto neograničene slobode, pa čak i ukoliko se vlastitom slobodom, odnosno pravima ugrožavaju tuđa prava, odnosno sloboda, što nije rijedak slučaj) neminovno se podvode pod (pokušaj) cenzuru samog interneta, odnosno komunikacije na internetu, aktivnosti na internetu, sadržaja na internetu i drugih aspekata samog interneta, odnosno onoga što on predstavlja.

Pojavom interneta, a pogotovo njegovom ekspanzijom među "običnu" populaciju, javila se i potreba za svojevrsnim reguliranjem odnosa između samih korisnika, odnosa između korisnika i davatelja internetskih usluga, afirmiranjem netikecije, službenim sankcioniranjem subjekata koji krše pravila. Navedeno je intenzivirano ekspanzijom niza antiestablišmentskih, kriminalnih, nedozvoljenih, nedruštvenih i nepodrazumijevanih aktivnosti koje su ubrzo preplavile internet, s obzirom na brojne mogućnosti anonimnog djelovanja u ovome okruženju. Međutim, svaki pokušaj bilo kakvog reguliranja interneta dovodio je do gotovo aklamativnog neslaganja kako internautske populacije, tako i niza subjekata koji su na određeni način vezani za internet. Naravno, neophodno je napomenuti da zahtjev za reguliranjem interneta nije samo rezultat državnih organa, već i niza subjekata koji

imaju određenu povezanost s internetom, ali žele unaprijediti vlastitu (ko)egzistenciju upravo reguliranjem interneta (Kurbalija, 2011).

Sukladno s navedenim, tradicionalni koncepti reguliranja interneta mogu se promatrati dijametralno suprotnim: s jedne strane su državni organi koji su nastojali (nastoje!) da internet reguliraju i stave ga "pod kontrolu" (kako su tvrdili oponenti ove krajnosti), dok su, s druge strane, subjekti koji su nastojali (nastoje!) internet održati u prvobitnom obliku, kao "prostoru necenzurirane i ničim ograničene slobode" (pa čak i kada ta sloboda ugrožava druge subjekte). Sve do početka drugog tisućljeća može se promatrati ova formalna i neformalna borba između dviju suprotstavljenih skupina subjekata, koja početkom drugog tisućljeća ipak dobiva nove obrise, iako se ne može reći da ni jedna ni druga skupina subjekata nije ni pobijedila, ni izgubila u višedesetljetnoj borbi za primat nad internetom po vlastitim stremljenjima. Iako se aktualnu razinu odnosa između suprotstavljenih skupina može promatrati kompromisnim i s održavanjem *statusa quo* (bez obzira na brojne, svakodnevne, a ponekad i ekstremne pokušaje promjene tog stanja), on svakako predstavlja izraz jedne praktične potrebe za, s jedne strane, neophodnošću reguliranja interneta, makar i u određenim rudimentarnim oblicima, dok, s druge strane, omogućuje određenu slobodu internautima i drugim zainteresiranim subjektima, nastojeći da sloboda ne ograničava ili ne ugrožava tuđa prava. Stoga se aktualnu razinu reguliranja odnosa na internetu i samog interneta upravo i može promatrati kao kvantitativna kompromisna i prešutna nadgradnja višedesetljetnog spora o reguliranju (kontroli) interneta (Putnik, 2009). Međutim, aktualni odnosi na internetu pokazuju i svoju kvalitativnu stranu, jer znanstveno-tehničko-tehnološkom ekspanzijom mnogobrojni zainteresirani subjekti svakako pronalaze mnogobrojne mehanizme (i pravne, i tehničke, i faktičke) kako bi zaštitili vlastite interese na internetu upravo u stanju koje karakterizira zamrznutosti prethodno spominjanog sukoba. U tom kontekstu, državni organi, s jedne strane, inkriminacijom nedozvoljenog ponašanja na internetu, kao i usavršavanjem i primjenom tehničkih mogućnosti nastoje osujetiti i adekvatno odgovoriti na brojne sigurnosne incidente unutar internetskog okruženja, dok, s druge strane, brojni subjekti, zahvaljujući brojnim "pravnim prazninama" i vlastitom znanju i sposobnosti, vješto izbjegavaju restriktivna pravila "kontrole" interneta, te se maksimalno koriste ovim "utopističkim prostorom slobode".

Kao jedan od modaliteta reguliranja i kontrole interneta kako je prethodno predstavljeno, svakako se pojavljuje i "prisutnost" policije na internetu, odnosno u internetskome okruženju. Ta "prisutnost" policije može se sagledati i kroz preventivno, ali i kroz represivno postupanje, kao i u tradicionalnim oblicima policijskog postupanja, s tim što su sadržajne razlike postupanja ogromne, što je i razumljivo, s obzirom na to da je uvjetovano specifičnim okruženjem kakvo je okruženje interneta.

4. MODALITETI PRISUSTVA POLICIJE NA FACEBOOKU

"Prisutnost" policije na internetu se možda najbolje može sagledati upravo kroz aktivnosti policije na Facebooku ili kroz aktivnosti policije uvjetovane aktivnostima na Facebooku. "Prisutnost" policije na Facebooku ili aktivnosti policije uvjetovane aktivnostima na Facebooku su, može se primijetiti, prošle sličan razvoj kao i uplitanje državnih organa i drugih subjekata u (pokušaj) reguliranje i kontrolu interneta. Razumljivo je da je u počecima Facebooka, policija relativno rijetke i relativno bezopasne sigurnosne incidente u vidu narušavanja privatnosti i nepodrazumijevanog ili neželjenog ponašanja prepuštala stihijskom ili samoorganiziranom reguliranju od strane samih korisnika, nakon čega su tu ulogu preuzeli administratori Facebooka (naravno, ne ograničavajući ni ulogu samih korisnika na tom planu, pogotovo u određenim segmentima). Međutim, ekspanzija Facebooka, odnosno broja korisnika Facebooka, svakako je uvjetovala i kvalitativnu i kvantitativnu ekspanziju sigurnosnih incidenata promatranih primarno, ali ne i jedino kroz kriminalne aktivnosti usmjerene od strane korisnika Facebooka ili prema korisnicima Facebooka ili korištenjem određenih mogućnosti Facebooka. Razumljivo je da je to uvjetovalo i rekonceptualizaciju uloge policije u Facebook okruženju i prema samom Facebooku, a potom neizostavno i prema samom internetskom okruženju, pa i prema samom internetu (Miladinović, 2013: 403). [222]

Usljed navedenog, (često postavljano) pitanje "prisutnosti" policije na Facebooku nije ni aktualno[223], ni opravdano[224], već ovo (nekad opravdano i aktualno, a danas prevladano)

---

[222] I samo zadiranje policije u sferu interneta i internetskog okruženja može se promatrati kroz segment ispoljavanja kriminalnih aktivnosti na internetu ili prema internautima ili korištenjem određenih mogućnosti interneta. Naime, kvalitativnom i kvantitativnom ekspanzijom ovih kriminalnih aktivnosti, svakako je nametnulo, odnosno uvjetovalo rekonceptualizaciju dotadašnje uloge policije u sferi interneta. Samo po sebi se nametnula potreba (i zahtjev) da policija zaštiti određene vrijednosti koje su bile ugrožene izvan tradicionalnog, odnosno realnog okruženja, tj. u internetskom okruženju. Naravno, u ovom kontekstu, treba ukazati i na pojedina shvaćanja (koja nisu bez osnove) da je država preko policije (kao svog tijela) upravo ove kriminalne aktivnosti iskoristila kao "kukavičje jaje" u cilju reguliranja, a potom (posredno) i kontrole interneta, prvo inkriminacije određenog ponašanja, a potom davanjem i ovlasti policiji da zadire u samu arhitekturu interneta, a vrlo brzo i omogućavanjem nizu subjekata formalne, pa i poluformalne, nacionalne ili globalne provinijencije da reguliraju, a posredno i kontroliraju sam internet.

[223] Za Federalni istražni ured (FBI) se smatra da je prvi ozakonio vlastitu "prisutnost" na Facebooku, kao i korištenje određenih resursa i mogućnosti s ove društvene mreže, što je i razumljivo iz više razloga. Sama teritorijalna i stvarna nadležnost ove savezne policijske (kriminalističke) agencije u SAD-u je nametnula tu neophodnost, dok, s druge strane, treba imati u vidu da ova agencija, kao jedna od najopremljenijih agencija takve vrste u svijetu, ispravno i pravodobno percipira nove trendove (ekspanzije) kriminaliteta (kakav je trenutačno računalni i internetski kriminalitet, a pogotovo kriminalitet društvenih mreža), te iznalazi i usavršava modalitete reagiranja na njega. Također, neophodno je ukazati na to da FBI, za razliku od većine drugih policijskih agencija u svijetu (a pogotovo na našim prostorima), nije krutih shvaćanja u pogledu primjene novih metoda, sredstava, tehnologija i strategija u kriminalističkom radu, štoviše, moglo bi se reći da potencira i favorizira nove pristupe (i u tehničko-tehnološkom, i u normativnom, i u strateškom, i u taktičkom, i u faktičkom) reagiranja na kriminalitet, gdje se "prisutnost" policije na Facebooku može promatrati samo kao jedan segment navedenog. Poučeni primjerom FBI-ja, i druge policijske agencije u svijetu su, različitim modalitetima, počele djelovati unutar Facebook okruženja, uslijed čega se može reći da danas gotovo sve policije (ali i druge sigurnosne agencije) imaju vlastito prisustvo unutar Facebook okruženja, bez obzira na to da li ga izričito ili prešutno priznaju.

[224] Kao što je već navedeno, upravo ekspanzija kriminalnih aktivnosti, te ugroženost mnoštva subjekata (ne samo korisnika i drugih internauta) na Facebooku uvjetovala je i neophodnost "prisutnosti" policije na Facebooku kako bi, između ostalih subjekata, zaštitila korisnike Facebooka i druge internaute, kao i sve druge subjekte koji su ugroženi negativnim djelovanjem na Facebooku ili korištenjem mogućnosti Facebooka. Drugim riječima, ukoliko svrhu djelovanja policije u zajednici i prema zajednici promatramo kroz (američki) koncept "Služiti i štititi", odnosno kroz uslužnu i zaštitnu funkciju koju ona (trebaju) ima prvenstveno prema građanima i drugim

pitanje treba promatrati u kontekstu sadržajnosti i prirode "prisutnosti" policije na Facebooku. Drugim riječima, s obzirom na to da je razumljivo da je policija "prisutna" na Facebooku, treba sagledati modalitete te "prisutnosti", pogotovo u kontekstu sprečavanja potencijalnih kriminogenih faktora, kao i u kontekstu neposredne zaštite korisnika Facebooka. Odgovor na navedeno nije nimalo jednostavan, niti se može promatrati konačnim, pogotovo imajući u vidu da policija svakodnevno unaprjeđuje vlastite aktivnosti, pogotovo s kvalitativnog aspekta u kontekstu tehničke, normativne, faktičke, internacionalne i druge prirode. Uvjetno promatrajući angažman policije na internetu, a pogotovo na Facebooku, bez pretenzija za konačnom i sveobuhvatnom klasifikacijom, sve aktivnosti policije bi se mogle promatrati kroz sljedeće segmente:

- pasivnu "prisutnost" policije na Facebooku kroz kreiran profil ili stranicu,
- online ophodnju policije u Facebook okruženju,
- preventivno reagiranje policije na potencijalne kriminogene čimbenike,
- klasično represivno djelovanje policije korištenjem mogućnosti koje pruža Facebook,
- forenzičke aktivnosti policije uz pomoć Facebooka ili na Facebooku (Miladinović 2013).

Kao najbezazleniji, odnosno najpasivniji oblik "prisutnosti" policije na Facebooku može se promatrati kreiranje profila ili službene stranice na Facebooku. Ovdje je razumljivo da se ne radi o nekoj službenoj, pa čak ni proaktivnoj aktivnosti policije, jer osim egzistiranja profila (ili stranice), u ovom slučaju se ne može govoriti ni o kakvoj policijskoj, a pogotovo ne kriminalističkoj aktivnosti. Ovaj oblik "prisutnosti" policije na Facebooku može se promatrati kroz svojevrsni informativni, a djelomično i preventivni segment, što je svakako značajno s aspekta onemogućavanja potencijalnih kriminalnih aktivnosti, a u skladu je s aktualnim trendom među preventivnim *cyber* aktivnostima većine policijskih agencija u svijetu.[225]

---

subjektima u društvu (a potom i u državi), razumljivo se nameće obveza zaštite korisnika i drugih internauta i u internetskom okruženju.
U ovom kontekstu, "prisutnost" policije na Facebooku mora se promatrati i kroz koncept rada policije u zajednici. Naime, prihvaćanjem ovog koncepta, policija se obvezuje da djeluje čak i na one uzroke koji još uvijek nisu kriminalne prirode (odnosno, nisu inkriminirani, pa ni zabranjeni), ali mogu dovesti do određenog kriminalnog ispoljavanja, odnosno mogu biti ili povodi ili čak i uzroci određenog kriminalnog ponašanja. Razumljivo je da su ovi faktori mnogobrojni i raznovrsni, što nameće neophodnost "prisutnosti" policije na Facebooku, ali i neophodnost adekvatnog preventivnog, a pogotovo represivnog djelovanja. Kroz "prisutnost", a potom i kroz djelovanje policije u Facebook okruženju, najizravnije se pruža zaštita korisnicima, ali se i sprječavaju potencijalne nedozvoljene ili nepodrazumijevane aktivnosti, te se na njih adekvatno i pravodobno reagira, ukoliko se ipak realiziraju.

[225] Da je ovaj oblik "prisutnosti" policije na Facebooku značajan, pokazuju kreirani profili i stranice brojnih policijskih agencija u BiH i okruženju. Štoviše, veći broj ovih agencija, shvaćajući značaj on-line "prisutnosti" u internetskom okruženju, a pogotovo u okruženju Facebooka, i na vlastitim službenim prezentacijama ima veze na vlastitim profilima na Facebooku. U ovom kontekstu, treba napomenuti da na Facebooku postoje mnogobrojni profili i stranice kreirane pod imenom određenih policijskih agencija, ali se ne radi o službenim stranicama, već o zaposjednutim digitalnim identitetima ovih agencija, odnosno stranicama koje nisu kreirane od strane korisnika koji ima za to neophodno odobrenje. Naravno, treba napomenuti da većina ovih stranica nije kreirana u nelukrativne svrhe, već upravo suprotno, ali navedeno svakako stvara određenu pomutnju u smislu službenog oglašavanja, informiranja i "prisutnosti" policije na Facebooku.

Aktivnost policije u internetskom okruženju, a pogotovo u Facebook okruženju koju bi, po ugledu na klasičnu ophodnju policije, mogli nazvati i on-line ophodnjom je sljedeća, kvalitativno i kvantitativno viša razina "prisutnosti" policije u ovom okruženju.[226] Za razliku od prethodnog oblika "prisutnosti" policije, u ovom slučaju policija ima proaktivnu ulogu u samom okruženju, ali bi se i ovdje moglo reći da se uloga policije sastoji u svojevrsnom pomatranju, praćenju, nadgledanju, ukazivanju na potencijalne opasnosti, preventivnom reagiranju, sprječavanju kriminalnog ili drugog nedozvoljenog ili nepodrazumijevanog ponašanja, otklanjanju uzroka koji bi doveli do takvog ponašanja. Isto tako, za razliku od sljedeće, kvalitativno i kvantitativno više razine "prisutnosti" policije na Facebooku, on-line ophodnja ne podrazumijeva poduzimanje bilo kakvih represivnih aktivnosti prema zlonamjernim korisnicima, već se aktivnost policije zadržava na preventivnim aktivnostima, ubrajajući u njih davanje upozorenja, ukazivanje na određene propuste korisnika, davanjem savjeta, itd.

Pored on-line ophodnje, i drugi vidovi preventivne aktivnosti policije u Facebook okruženju mogu biti zastupljeni. Te preventivne aktivnosti se mogu razlikovati i po sadržaju i po intenzitetu " prisutnosti ", ali je značajna karakteristika da se realiziraju u ovom okruženju i da su namijenjene primarno Facebook populaciji, odnosno korisnicima Facebooka. U ovom kontekstu se mogu podrazumijevati razni preventivni programi prilagođeni specifičnom Facebook okruženju, ali i specifičnoj populaciji Facebooka, ali ne treba zapostaviti ni niz "klasičnih" preventivnih aktivnosti koje policija ima i u stvarnom okruženju, ali uz izvjesne modifikacije može ih poduzimati i u internetskom, odnosno Facebook okruženju.[227] S obzirom na mnogobrojne sličnosti ovih aktivnosti s radom policije u zajednici kao (kod nas) novim konceptom rada policije u realnom okruženju, ovaj koncept bi se mogao nazvati i radom (ili "prisustvom") policije u internetskoj, odnosno Facebook zajednici.

Represivno djelovanje policije unutar internetskog, odnosno Facebook okruženja nastaje konstatiranjem konkretne kriminalne aktivnosti. Cilj ove aktivnosti je utvrditi

---

[226] *On-line* ili *cyber* ophodnja podrazumijeva vid policijske (kriminalističke) aktivnosti na internetu u okviru koje posebno obučeni i opremljeni pripadnici policije (najčešće i u okviru posebnih specijaliziranih jedinica policije – tzv. *high-tech* ili *cyber* jedinica) "ophode" internet okruženjem u potrazi za eventualnim kriminalnim aktivnostima ili počiniteljima ili planerima kriminalnih aktivnosti. Naravno, cilj *cyber* ophodnje je i samo prisustvo policije u internetskom okruženju, jer je razumljivo da će ono, kao i u stvarnom okruženju, svakako preventivno djelovati na potencijalne počinitelje. Sam način ove aktivnosti je raznolik i uvelike ovisi o materijalno-tehničkim i kadrovskim resursima same jedinice (mada ne treba zapostaviti ni normativna ograničenja), ali podrazumijeva "prisutnost" pripadnika policije na pojedinim uslugama interneta (društvene mreže, društveni mediji, forumi, elektroničko poslovanje...) ili u okviru konkretnog okruženja na internetu. Neophodno je napomenuti da *cyber* ophodnja (trebala bi) podrazumijeva jasno, nedvosmisleno i vidljivo prisustvo policije unutar određenog okruženja, što znači da profil ili drugi oblik sudjelovanja policije unutar *cyber* ophodnje drugim subjektima okruženja mora nedvosmisleno ukazivati na to da se radi o javnom i službenom policijskom djelovanju, uslijed čega se i sami pripadnici policije koji izvode ovu aktivnost trebaju tako ponašati i djelovati. Tajna, prikrivena ili neprimjetna aktivnost policije u internetskom okruženju ne podrazumijeva *cyber* ophodnju, već (brojne) druge oblike kriminalističke (forenzične) aktivnosti u ovakvom okruženju.

[227] Primjer za navedeno predstavljaju preventivno-edukativne aktivnosti Ministarstva unutarnjih poslova Republike Srpske u sprečavanju maloljetničke delinkvencije. Ovaj projekt je pokrenut 2009. godine i aktualan je i danas, s određenim modifikacijama, prilagođenim aktualnim sigurnosnim izazovima. Namijenjen je primarno školskoj populaciji, a jedan segment se odnosi na podizanje sigurnosne svijesti učeničke populacije o opasnostima i rizicima korišnjenja interneta, primarno Facebooka, te o potrebi i načinima vlastite zaštite prisutnosti i privatnosti tijekom korištenja ove društvene mreže (Đurić, 2015).

elemente same kriminalne aktivnosti, te da se kroz kriminalističko-diferencijalnu dijagnozu utvrde elementi konkretnog djela, prikupe dokazi glede navedene kriminalne aktivnosti, odnosno konkretnog kaznenog djela, te da se identificira i pronađe počinitelj tog kaznenog djela, te dokazi koji ukazuju na njegov odnos sa samim počinjenjem djela. Ovo djelovanje se može promatrati kroz dva segmenta: prvi segment podrazumijeva da se na temelju računalno-forenzičnih metoda u području informacijsko-komunikacijskih tehnologija dođe do dokaza koji ukazuju na postojanje kaznenog djela, identitet počinitelja i njegov odnos (doprinos počinjenju) s kaznenim djelom, dok drugi segment podrazumijeva klasičnu represivnu aktivnost potpomognutu određenim relevantnim informacijama do kojih policija može doći korištenjem resursa Facebooka.[228]

Jedan od načina utvrđivanja postojanja kaznenog djela i identifikacije počinitelja, a pogotovo načina prikupljanja dokaza može se promatrati kroz forenzične aktivnosti policije na Facebooku ili korištenjem aplikacijskih mogućnosti Facebooka, i to upravo predstavlja drugi segment represivne "prisutnosti" policije na Facebooku kako je prethodno diferenirano. Navedeno se obavlja brojnim forenzičnim alatima, kako na samom kompromitiranom ili spornom računalu, tako i korištenjem aplikacijske osnove i sadržaja samog Facebooka.

5. REAKCIJA POLICIJE NA KRIMINALNE AKTIVNOSTI NA FACEBOOKU

Na temelju prethodno navedenog, vidljivo je da je policija "prisutna" na Facebooku i aktualno i sadržajno, usljed čega se može postaviti pitanje konkretne pomoći, odnosno konkretnih policijskih (kriminalističkih) aktivnosti policije s namjerom represivnog djelovanja prema konkretiziranom kriminalnom ili drugom nedozvoljenom ponašanju zlonamjernog korisnika prema žrtvi u Facebook okruženju ili korištenjem određenih mogućnosti Facebooka. Drugim riječima, postavlja se pitanje na koji način policija može pomoći korisnicima koji su žrtve određene kriminalne aktivnosti na Facebooku, te kakva je sama procedura te aktivnosti, počevši od prijave konkretne negativne aktivnosti, indicija glede osumnjičenog, prikupljanja dokaza, te dokazivanja samog kaznenog djela i počinitelja navedenog kaznenog djela.

Proceduru (postupak) policije nakon konstatiranog kaznenog djela počinjenog od strane zlonamjernih korisnika prema korisniku Facebooka ili prema drugoj žrtvi, treba promatrati u kontekstu operativnog rada policije počevši od zaprimanja prijave, odnosno saznanja o počinjenom kaznenom djelu, preko poduzimanja niza operativno-taktičkih mjera i radnji i istražnih (i posebnih istražnih) radnji u cilju prikupljanja dokaza i utvrđivanja identiteta počinitelja, do podnošenja izvješća o počinjenom kaznenom djelu protiv konkretne osobe ili konkretnih osoba. Naravno, razumljivo je da se ova kriminalistička aktivnost policije na rasvjetljavanju računalnog i internetskog kriminaliteta (u što ulazi većina kriminalnih

[228] Brojni su primjeri korištenje Facebooka od strane policije prilikom planiranja ili realiziranja klasičnih operativno-taktičkih mjera i radnji i istražnih radnji u cilju rasvjetljavanja konkretnog kaznenog djela ili konkretne kriminalne aktivnosti. Naime, sam sadržaj Facebooka, kao i mnoštvo informacija koje korisnici postavljaju o sebi, te određene aktivnosti koje Facebook bilježi, što je često i nesvjesno priručnik, svakako da omogućuju određene eliminacijsko-identifikacijske indicije na temelju kojih se može utvrditi alibi za osumnjičenog, utvrditi lokacija boravka ili kretanja osumnjičenog, utvrditi indicije glede potencijalne ili konkretizirane kriminalne aktivnosti konkretne osobe, utvrditi koje odnose i s kim ima i koliko sadržajne, utvrditi njegova poznanstva, planirati vrijeme i mjesto realizacije određenih operativno-taktičkih mjera i radnji i istražnih radnji (npr. lišenje slobode), pratiti aktivnosti nakon postojanja indicija da je planirano, pripremano ili počinjeno kazneno djelo ...

aktivnosti počinjenih na Facebooku ili korištenjem mogućnosti Facebooka) sadržajno razlikuje od kriminalističke aktivnosti na rasvjetljavanju kaznenih djela klasičnog kriminaliteta, odnosno kriminaliteta počinjenog na tradicionalan način, ali se s kaznenoprocesnog, a u izvjesnoj mjeri i s policijskog (kriminalističkog) aspekta mogu sagledati ista pravila, odnosno ista procedura. U tom pogledu, cjelokupna kriminalistička aktivnost u cilju rasvjetljavanja konkretiziranih kriminalnih aktivnosti na Facebooku može se promatrati kroz zaprimanje prijave o počinjenom kaznenom djelu, provjeravanje navoda o prijavi, prikupljanje dokaza u pogledu počinjenog kaznenog djela, utvrđivanje identiteta počinitelja, prikupljanje dokaza glede njegove krivnje, te prezentiranje prikupljenih dokaza i saznanja tužitelju kroz podnesen izvještaj o počinjenom kaznenom djelu i o počinitelju.

Iako je moguće da policija do saznanja o počinjenom kaznenom djelu na Facebooku ili putem Facebooka dođe i vlastitom aktivnošću (kroz, npr. on-line ophodnju), najčešće su slučajevi da se o tome sazna putem prijava oštećenih ili drugih zainteresiranih subjekata (nevladinih organizacija, medija, stranaka, vladinih institucija, udruga građana...). Ovo je i razumljivo, s obzirom na to da će sami oštećeni (bez obzira na to da li se oštećeni, u ovom slučaju, promatraju kao pravne ili kao fizičke osobe) prvi biti upoznati s konkretnom kriminalnom aktivnošću, kao i s posljedicom, odnosno štetom koju ta aktivnost uzrokuje ili je prouzročila. Imajući to u vidu, oštećeni ove aktivnosti prijavljuju prilikom prijave, bez obzira na to je li ona usmena ili pismena, kao i bez obzira na to podnosi li se policiji ili tužitelju, trebaju navesti sve relevantne okolnosti same negativne aktivnosti producirane prema njima. Naravno, te relevantne okolnosti su specifične za konkretnu kriminalnu aktivnost na Facebooku, pa i za svaki slučaj posebno, ali je činjenica da oštećeni nekad neće biti svjesni svih okolnosti samog slučaja, a pogotovo ne relevantnosti određenih okolnosti u kaznenopravnom i u kriminalističkom smislu. Uslijed navedenog, policija ili tužitelj treba inzistirati na detaljima prilikom zaprimanja prijave o počinjenom kaznenom djelu preko Facebooka ili korištenjem Facebooka. Ovdje je potrebno navesti još jednu bitnu karakteristiku, a koja se posebno očituje kod kriminalnih aktivnosti realiziranih preko Facebooka ili korištenjem Facebooka. Naime, odmah nakon zaprimanja prijave, policija treba postaviti kriminalističko-diferencijalnu dijagnozu, odnosno odrediti je li prijavljeni događaj kazneno djelo ili samo sigurnosni incident ili uopće nije događaj koji inicira aktivnost policije, a ukoliko je kazneno djelo – treba odrediti koje je konkretno djelo u pitanju, te da na temelju navedenog planira odgovarajuće operativno-taktičke mjere i radnje i istražne radnje u sklopu kriminalističke metodike rasvjetljavanja te skupine kaznenih djela ili konkretnog kaznenog djela. Razumljivo je da većina negativnih aktivnosti na Facebooku nisu kaznena djela, pa ni bilo koji drugi sigurnosni događaji na koje bi policija trebala (i smjela) reagirati, uslijed čega je i razumljivo da mnogobrojne prijave od strane oštećenih ne mogu biti razmatrane. Međutim, u ovim situacijama, kada policija nema osnove za reagiranje, ona bi trebala oštećenog ili prijavitelja ili drugog zainteresiranog subjekta uputiti na koji način i kojim subjektima se može obratiti da eventualno sanira nastalu štetu ili da spriječi nastanak štete ili da spriječi aktualnu aktivnost za koju smatra da nije lukrativnog znakovlja prema njoj ili drugom subjektu. U tom smislu, policija će najčešće zainteresirane subjekte uputiti prema administratorima Facebooka, ali se može dogoditi da ih uputi i na druge, poput davatelja

internetskih usluga, operatere mobilne telefonije, internet-kafiće, školu, sud, zaštitarske i detektivske agencije i dr.

Nakon zaprimanja prijave, policija bi trebala poduzeti aktivnosti radi provjeravanja navoda koje je dobila od prijavitelja ili na drugi način, a koji ukazuju na postojanje samog kaznenog djela. Kada su u pitanju same kriminalne aktivnosti preko Facebooka, nerijetko će se provjera navoda moći realizirati i samim neposrednim uvidom u kompromitirani profil, skupinu, stranicu, status, fotografiju, sadržaj i slično, ali će mnogo češće navedeno zahtijevati mnogobrojne druge aktivnosti kako bi se postavila adekvatna kriminalističko-diferencijalna dijagnoza, a na temelju nje, kao što je i navedeno, planirale i poduzele konkretne mjere, radnje i aktivnosti specifične za metodiku rasvjetljavanja konstatiranog kaznenog djela. Te aktivnosti ne moraju se bazirati samo na aktivnosti u internetskom okruženju, već se mogu odnositi i na klasične aktivnosti, odnosno klasične mjere i radnje kojima se nastoji diferencirati određeni segment konkretizirane kriminalne aktivnosti na Facebooku.[229]

Kao i u prethodnom slučaju, nerijetko će se identitet počinitelja konkretizirane kriminalne aktivnosti saznati, odnosno moći utvrditi neposrednim uvidom u sam inkriminirani sadržaj ili inkriminiranu aktivnost na Facebooku, ali je neophodno napomenuti da u određenim situacijama to neće biti moguće, uslijed čega se identitet počinitelja mora utvrđivati određenim kriminalističko-forenzičnim ili drugim metodama. Tek utvrđivanjem identiteta počinitelja, moguće je pristupiti prikupljanju dokaza glede njegove krivnje, mada se određeni dokazi mogu prikupiti i prije utvrđivanja identiteta, a to su najčešće oni dokazi koji ukazuju na postojanje i okolnosti samog kaznenog djela, a ne na izravnu vezu između samog kaznenog djela ili počinitelja. Neophodno je spomenuti prethodno navedenu jednu od karakteristika računalnog i internetskog kriminaliteta koja se upravo konkretizira u ovoj fazi operativnog rada policije, a to je da je vrlo teško utvrditi identitet počinitelja konkretizirane kriminalne aktivnosti računalnog i internetskog kriminaliteta, pogotovo počinjenog na Facebooku ili korištenjem mogućnosti Facebooka.

Prikupljanje dokaza glede krivnje počinitelja, kao i u pogledu samog postojanja konkretnog kaznenog djela moguće je i prije utvrđivanja identiteta počinitelja, ali ova aktivnost najčešće podrazumijeva zajedničke aktivnosti i na utvrđivanju okolnosti postojanja kaznenog djela, na utvrđivanju identiteta i na okolnosti utvrđivanja konkretizirane kauzalističke veze između samog počinitelja i konkretizirane kriminalne aktivnosti. Razumljive su određene poteškoće i prikupljanja, odnosno identifikacije i utvrđivanja ovih dokaza, ali je činjenica da se određene teškoće u ovoj fazi operativnog rada javljaju i kada je u pitanju osiguranje, odnosno fiksiranje identificiranih relevantnih dokaza, uslijed "nestalnosti" digitalnih dokaza koji se javljaju u većini slučajeva kod ovog oblika kriminaliteta.

Predstavljanje prikupljenih dokaza i saznanja tužitelju koji bi na temelju navedenog, ukoliko je dovoljna kvaliteta i količina dokaza, trebao podigći optužnicu protiv konkretne

[229] Na primjer, ukoliko se podnosi prijava o neovlaštenom korištenju tuđe marke ili žiga ili proizvoda i slične zaštićene vrijednosti počinjena neovlaštenim kreiranjem stranice na Facebooku gdje se taj brend zloupotrebljava ili čak neovlašteno komercijalizira, provjera navoda prijave (koja i ne mora biti podnesena od oštećenog) bi obuhvaćala i klasične kriminalističke aktivnosti poput obavljanja obavijesnog razgovora, prikupljanja obavijesti, uvida u određenu dokumentaciju i slično, kako bi se utvrdilo stvarno pravo vlasništva (raspolaganja) nad brendom, proizvodom...

osobe za konkretno kazneno djelo, obavlja se podnošenjem Izvješća o počinjenom kaznenom djelu i o počinitelju. Ovo izvješće bi, u biti, trebalo sadržavati sve dokaze, saznanja i informacije do kojih je policija došla tijekom operativnog rada, a koji ukazuju na postojanje kaznenog djela, identitet počinitelja tog kaznenog djela i kauzalistički odnos između samog djela i te osobe.

6. ZAKLJUČNA RAZMATRANJA

Policija mora napustiti svoj tradicionalni (moglo bi se reći i tradicionalistički) pristup u reagiranju na probleme u realnom okruženju, a pogotovo takav pristup nije adekvatan za rješavanje problema u internetskom okruženju, imajući u vidu mnogobrojne specifičnosti ispoljavanja kriminalnih aktivnosti u ovom okruženju. Konstantni, kontinuirani, proaktivni, strateški, preventivni, edukativni, ciljani, fokusirani, usmjeravani, segmentirani, problemski pristup sigurnosnim izazovima u internetslp, okruženju svakako mora biti vizija kriminalističkog, kriminološkog, a i policijskog djelovanja na planu suzbijanja ovog oblika kriminaliteta. Podrazumijeva se da se taj pristup ne može temeljiti na resursima i sposobnostima, pa ni na ovlastima samo policije, već mora biti i multidisciplinaran i multiagencijski, ali policiju ne amnestira primarne odgovornosti. Ako ni zbog čega drugog, onda zbog toga što će u nju biti "uperene oči javnosti, a pogotovo žrtve", ukoliko zataji bilo koji segment ili subjekt društva.

U ovom novom kriminalističkom (pa i policijskom) reagiranju, važan je edukativni i preventivni aspekt, koji se ne bi trebali odvojeno promatrati, već upravo zajedno, pa i sinergijski. U ovom kontekstu se mora naglasiti primarna i proaktivna uloga policije koja mora preuzeti inicijativu u sprječavanju sigurnosnih incidenata u ovom okruženju, imajući u vidu sve teškoće i ograničenja klasičnog, *post festum* represivnog reagiranja na iskrsle incidente. Navedena proaktivnost policije u skladu je s novom (proklamiranom) filozofsko-strateškom koncepcijom rada policije u novonastalim okolnostima, ali je činjenica da se policija još uvijek (pogotovo kod nas, ali i u drugim državama, ne izuzimajući ni razvijene države zapadne Europe i SAD-a) ne može oteti represivnom pristupu reagiranja na poslove i zadatke iz vlastite nadležnosti. Ukoliko bi se navedeno i moglo promatrati kao relikt preuzetih i naučenih obrazaca ponašanja (reagiranja) koji su ustaljeni nekoliko desetljeća, pa i stoljeće egzistiranja policije u društvu, taj izgovor se ne bi mogao koristiti za isti ovakav pristup u internetskom, odnosno Facebook okruženju. Upravo suprotno, imajući u vidu da je internetsko okruženje relativno "mlado", te da se policijske aktivnosti u ovom okruženju još uvijek nisu ustalile, a pogotovo nema "učahurenih" modaliteta reagiranja, neophodno je od strane relevantnih subjekata, a pogotovo relevantnih pojedinaca inzistirati na do sada konstatiranoj dobroj praksi aktivnosti policije u ovom okruženju koja se, primarno, mora temeljiti na proaktivnom pristupu, i to ne samo na sigurnosne incidente, već na sve faktore koji (mogu) imaju i etiološki i viktimogeni znak, pa čak i posredno promatrajući.

LITERATURA

Banović, B., Miladinović, A. (2010). Kriminološko-fenomenološki aspekt Fejsbuka. *Kriminalističko-forenzička istraživanja,* 1(1), 45-58.
Đurić, M. (2015). *Socijalno-psihološki aspekti reagovanja adolescenata na vršnjačko nasilje.* Banja Luka: Filozofski fakultet.
Kurbalija, J. (2011). *Uvod u upravljanje internetom.* Beograd: Albatros plus.
Miladinović, A. (2013). *Fejsbuk i kriminalitet.* Banja Luka: Internacionalna asocijacija kriminalista.
Miladinović, A., Petričević, V. (2012). Kriminogeni aspekt društvenih mreža. U: Šikman, M. (ur.) *Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal*, str. 257-271. Laktaši: Visoka škola unutrašnjih poslova Banja Luka i Hans Zajdel fondacija.
Putnik, N. (2009). *Sajber prostor i bezbjednosni izazovi.* Beograd: Fakultet bezbednosti.

Mile Matijević
Aleksandar Miladinović

CRIMINALISTIC ASPECTS OF THE FACEBOOK

Summary

Due to the qualitative and quantitative expansion of Facebook, the result is an increase of the many negative, primarily criminal activities on the social network or by using the possibilities of social networks. The specific environment of Facebook, emphasizes the necessity of a specific response to this negative phenomenon. This primarily relates to a criminal specifics of the reactions in a virtual environment, using certain features, methods and means that are available to the police, depending on the personnel, material and technical and regulatory constraints. The paper points to the need for police presence in the virtual environment, especially on Facebook, and then provides an overview of certain features that Facebook, in terms of criminology. For example, criminology can provide the information for the police in detecting crimes and perpetrators, identifying and localizing (invention) executors, and the ability to gather operational knowledge and information regarding clarifying and proving specific criminal (planned, crafted over or realized) activities. Criminalistic aspect of Facebook is seen through certain features, which are available to all users of Facebook (including police officers), as well as the specific features that include sophisticated knowledge and technical and technological resources. Also, it points out the importance of prevention of abuse among Facebook users, as well as the possibility of using Facebook for preventive purposes.

Key words: *Facebook, internet crime, police on Facebook, security on Facebook.*

IZVORNI ZNANSTVENI RAD

Joško Vukosav[230]
Joško Sindik[231]
Ivana Glavina Jelaš[232]

LIČNOST POČINITELJA NASILNIČKOG I NENASILNIČKOG KRIMINALITETA

Sažetak

Peterofaktorski (Big Five) model ličnosti može ukazivati na profil osobe koja će više ili manje biti sklona činjenju određenih vrsta kaznenih djela. Glavni cilj istraživanja bio je utvrditi mogu li u značajnoj mjeri različite osobine ličnosti razlikovati tri skupine osoba: pravomoćno osuđenih za najteža kaznena djela iz područja nasilničkog kriminaliteta (ubojstva, silovanja i sl., tj. NK), pravomoćno osuđenih za nenasilna kaznena djela (pronevjere, krivotvorenje isprava i sl., tj. NNK) te odgovarajuće skupine osoba iz opće populacije koje nikada nisu kažnjavane (OP). Nadalje, željeli smo utvrditi povezanost između varijabli ličnosti i varijabli agresivnosti, posebno za svaki uzorak: NK, NNK i OP. Ispitane su tri dobno ujednačene grupe muških sudionika: NK (N=138), NNK (N=149) te kontrolna skupina osoba OP (N=147). Primijenjena su dva mjerna instrumenta: International Personality Item Pool (IPIP50) te Upitnik agresivnosti A-87. Rezultati diskriminacijske analize pokazuju statistički značajnu razliku u ličnosti osoba koje pripadaju trima grupama sudionika (NK, NNK i OP) i to u aspektima ekstraverzije te u emocionalnoj stabilnosti. Mogu se detektirati i određene razlike u povezanostima varijabli za različite grupe sudionika istraživanja. Rezultati istraživanja mogu poslužiti u smjeru modeliranja uspješnih mjera prevencije, prvenstveno sa svrhom sprječavanja pojave nasilničkog ali i nenasilničkog kriminaliteta.

Ključne riječi: *kaznena djela, Peterofaktorski model ličnosti, pravomoćno osuđeni, razlike*

1. UVOD

Mnogi autori se slažu da je ličnost pojedinca važan čimbenik o kojem može ovisiti da li će određena osoba biti sklona činjenju kaznenih djela. Da bismo utvrdili razlike u pojedinim osobinama ličnosti počinitelja kaznenig djela, u ovom se istraživanju odabralo psihološke varijable tzv. peterofaktorskog (Big Five) modela ličnosti, koji pokriva pet širokih dimenzija ličnosti: ekstraverzija, neuroticizam, ugodnost, savjesnost i intelekt.

[230] Joško Vukosav, Visoka policijska škola, Avenija Gojka Šuška 1, Zagreb. E-mail: vjosko@fkz.hr
[231] Joško Sindik, Institut za antropologiju, Ljudevita Gaja 32, Zagreb. E-mail: josko.sindik@inantro.hr
[232] Ivana Glavina Jelaš, Visoka policijska škola, Avenija Gojka Šuška 1, Zagreb. E-mail: iglavina@fkz.hr

Individualizacija kažnjavanja

Temeljna svrha kazne trebala bi biti promjena one vrste ponašanja koja je dovela pojedinca u situaciju da bude kažnjen (rehabilitacijsko stajalište) ili pak odmazda društva za počinjena kaznena djela (retribucijski pristup) (Vukosav, Glavina Jelaš i Sindik, 2015). Četiri su osnovna cilja kažnjavanja kriminalnog ponašanja: zaštita društva od prijestupnika; njihova resocijalizacija odnosno socijalna integracija; preventivno djelovanje na potencijalne prijestupnike; odmazda društva za počinjena kaznena djela (Vukosav, 2001). S obzirom da je svaki počinitelj kaznenog dijela pojedinac za sebe, treba težiti individualizaciji samog kažnjavanja i drugih kaznenopravnih sankcija, kao i prilagođavanju samoga tretmana osobnim karakteristikama osuđenika. Međutim, postojeće metode korištene u penologiji kod nas nisu u dovoljnoj mjeri prilagođene pojedincu (Mejovšek, 1989). Stoga je posebno važno razmotriti osobine ličnosti pojedinca.

Peterofaktorski (Big Five) model ličnosti

Peterofaktorski (Big Five) model ličnosti je danas prema broju objavljenih radova dominantan model ličnosti, a razlozi za to su dobra teorijska i empirijska utemeljenost. Ideja o pet velikih dimenzija ličnosti postojala je dugo, jer su se javljale i u faktorskim analizama termina za opise ličnosti poput Allport-Odbertova popisa osobina i u upitničkim mjerama ličnosti (Ozer i Reise, 1994; McCrea i Costa, 1997, 1999). Naime, pokazalo se da se ljudi mogu dobro procijeniti unutar sustava od pet osnovnih dimenzija ličnosti, koje kao sržne osobine organiziraju veliki broj užih obilježja ličnosti. Osnovne su dimenzije uglavnom normalno distribuirane u općoj populaciji. Prva dimenzija u modelu je inteligencija ili tzv. ***otvorenost na iskustvo***: koliko smo intelektualno otvoreni za nove spoznaje i iskustvo, originalni i liberalni. Obuhvaća elemente poput maštovitosti, nezavisnosti u procjenama, usmjeravanja pažnje na osobne osjećaje, preferiranja raznolikosti, intelektualne znatiželje. Otvorene osobe zanima vanjski, ali i njihov unutarnji svijet, pa su njihova iskustva bogatija raznim doživljajima. Sklone su prihvaćanju novih ideja i nekonvencionalnih vrijednosti, dok pozitivne i negativne emocije doživljavaju intenzivnije od zatvorenih osoba (Costa i McCrae, 2005). Premda mnogi autori poistovjećuju ovu dimenziju s intelektom, Costa i McCrae (2005) navode da je ova dimenzija doduše povezana s nekim aspektima inteligencije, kao što je divergentno mišljenje, ali ni u kojem slučaju nije ekvivalent inteligencije (McCrae, 1987, prema Costa i McCrae, 2005). Ljudi s niskim rezultatima na Otvorenosti skloni su konvencionalnom ponašanju, obično su poslovni i praktični te politički konzervativni. Druga dimenzija naziva se ***neuroticizam ili emocionalna stabilnost***: smirenost, sigurnost u sebe, neranjivost, sklonost uzbuđenju zbog iznenadnih podražaja. Emocionalno nestabilne osobe snažnije reagiraju na potencijalni stres i teže se suočavaju s njim. Neuroticizam (N) je najšira dimenzija koja suprotstavlja emocionalnu stabilnost ili prilagodbu i neprilagodbu (Costa i McCrae, 2005). Srž N-dimenzije je opća sklonost doživljavanju negativnih emocionalnih stanja (poput straha, srdžbe, ljutnje, krivnje i gađenja), pa poremećene emocije kod ljudi s visokim rezultatom na N-ljestvici interferiraju s dobrom prilagodbom. Pored osjetljivosti na psihičke poteškoće, N ujedno mjeri i sklonost iracionalnim idejama, smanjenu sposobnost kontroliranja impulsa i neuspješnije suočavanje sa stresom. Međutim, visok rezultat na N ljestvici moguć je i bez postojanja bilo kakvog psihijatrijskog poremećaja (Costa i McCrae,

2005). Osobe s niskim rezultatima na ljestvici Neuroticizma emocionalno su stabilne, smirene, opuštene, uravnotežene i u stanju su suočiti se sa stresnim situacijama bez uznemiravanja. N-dimenzija u visokoj se mjeri podudara s istoimenom dimenzijom iz Eysenckova modela ličnosti (Eysenck i Eysenck, 1994_a; 1994_b). Isto vrijedi i za ***ekstraverziju*** (E), dimenziju koja upućuje na društvenost, asertivnost i razgovorljivost, ali i osobine temperamenta kao što su traženje uzbuđenja i pozitivna emocionalnost (Eysenck i Eysenck, 1994_a; 1994_b; Costa i McCrae, 2005). Ekstraverti su u odnosima s drugim ljudima druželjubivi i topli, brzo pričaju te obično preuzimaju vodstvo u grupi, dok su introvertirane osobe povučene, neovisne i uravnotežene. Četvrta dimenzija ličnosti se najčešće naziva ***savjesnost*** te opisuje pažljivost prema drugima, pouzdanost, te vlastitu savjesnost u pristupu privatnom i profesionalnom životu. Savjesnost (S) je obilježje osoba koje su odlučne, promišljene, točne, pouzdane, uspješne na akademskom polju te uredno obavljaju svoje društvene i građanske dužnosti (visoko su odgovorne i uredne). Savjesnost se može definirati kao nepatološki oblik opsesivno-kompulzivne ličnosti koju opisuje potreba za radom i redom, a pojednostavljeno se savjesnošću može smatrati „karakternost“ (Costa i McCrae, 2005). Osobe s visokim rezultatom na S su skrupulozne, a one s niskim rezultatom na S-skali nisu nužno bez moralnih načela, ali ih manje strogo primjenjuju, i opuštenije su u nastojanju da ostvare postavljene ciljeve. Ljudi s niskim rezultatima na S-ljestvici, vjerojatnije su manje uspješni u školi i na poslu. Peta dimenzija ličnosti je ***ugodnost:*** dobroćudnost, nesebičnost, nerazdražljivost, ugodnost komuniciranja s drugima i sklonost za kooperativnost. Drugim riječima ugodnost (U) je dimenzija koja se odnosi na interpersonalne sklonosti i na međuljudsku komunikaciju, slično kao i ekstraverzija (E) (Costa i McCrae, 2005). I dok se E definira kroz socijabilnost i potrebu za većim brojem socijalnih kontakata, ugodnost teži visokoj kakvoći međuljudskih odnosa, pa je ugodna osoba u biti altruistična, lako suosjeća, rado pomaže drugima te vjeruje da će joj ljudi uzvratiti na isti način (Costa i McCrae, 2005). Ugodna osoba je skromna, obazriva, iskrena. Osobe s niskim rezultatom na U-ljestvici su neugodne, egocentrične, odbijaju suradnju, skeptične su i paranoične prema drugima. Visoka ugodnost je povezana s ovisnim poremećajem ličnosti, a niska ugodnost s narcisoidnim, antisocijalnim i paranoidnim poremećajima ličnosti (Costa i McCrae, 2005).

Agresivnost, uzroci kriminaliteta i delinkvencija

Među crtama ličnosti koje se najčešće vežu uz kriminalitet, najčešće se spominje agresivnost. Agresivnost se u velikom broju istraživanja utvrđeno pokazala kao dobar prediktor budućeg delinkventnog ponašanja (Huesmann et al., 1984), dok su varijable agresivnosti uspješno razlikovale nasilne od nenasilnih delinkvenata (Mejovšek, Cajner-Mraović i Buđanovac, 1997), kao i nasilne delinkvente od nedelinkventne populacije (Žužul, Knezović i Šakić, 1987). Također, pokazalo se da postoje značajne međusobne razlike na pojedinim skalama agresivnosti između počinitelja različitih kaznenih djela (Knezović i sur., 1989). I dok se u početnim istraživanjima smatralo da su agresivnost i kriminalitet u izravnoj uzročno posljedičnoj vezi, kasnije su prevladavale koncepcije koje su polazile od uvjerenja da su agresivnost i kriminalitet kompleksno povezane pojave, pa se više može govoriti o njihovom paralelizmu (Mednick & Christiansen, 1977). Rezultati različitih istraživanja su pokazali da različiti čimbenici mogu utjecati na razinu agresivnosti kod djece: roditeljsko zanemarivanje i zlostavljanje, nepovoljno obiteljsko ozračje, odrastanje u „nasilnoj“ okolini,

alkoholizam roditelja, niski socio-ekonomski položaj primarne obitelji, i slično (Vukosav, 2002). Kako je agresivnost relativno stabilna osobina ličnosti koja pokazuje vremensku dosljednost, a uz utvrđeni odnos između agresivnosti i kriminaliteta, navedene varijable mogu biti posredni prediktori budućeg delinkventnog ponašanja (McGuire, 2004).

Više različitih teorija pokušava objasniti pojavu delinkvencije. rezultati istraživanja usmjerenih na čimbenike nastanka kriminaliteta važnu pokazale su da na etiologiju kriminaliteta utječe više kategorija različitih čimbenika, među kojima se ističu skupine bioloških, socijalnih, ekonomskih, okolinskih i psiholoških (Vukosav, 2006). S obzirom da navedeni čimbenici imaju različite razine utjecaja, i njihov utjecaj može biti izravan ili posredan, pri istraživanju uzroka kriminaliteta istodobno treba istraživati veći broj tih čimbenika, da bi se mogla razlučiti i razumjeti njihova uloga u nastanku kriminaliteta u pojedinim populacijama (Vukosav, 2006). u ovom slučaju istražili smo prvenstveno skupinu psiholoških čimbenika: strukturu ličnosti mjerenu primjenom Peterofaktorskog modela, te model agresivnosti, koja se može očitovati ili kao latentna tendencija za agresijom ili kao manifestno agresivno ponašanje. Međutim, agresivnost je u ovom istraživanju korištena samo kao varijabla koju smo doveli u vezu s preostalim crtama ličnosti pojedinca, s obzirom da smo u prethodnom istraživanju utvrdili razlike između osoba koje se nalaze na izdržavanju kazne za djela nasilničkog kriminaliteta, pravomoćno osuđenih za djela nenasilničkog kriminaliteta te kontrolne skupine sudionika (Vukosav i sur., 2015). U tom istraživanju, nasilni prijestupnici su se pokazali statistički značajno agresivniji u odnosu na nenasilne prijestupnike i kontrolnu skupine sudionika u dva instrumenta za mjerenje agresivnosti.

Glavni cilj ovog istraživanja bio je utvrditi razlike u Velikih Pet (Big Five) osobina ličnosti, pravomoćno osuđenih za najteža kaznena djela iz područja nasilničkog kriminaliteta (ubojstva, silovanja i sl., tj. NK), pravomoćno osuđenih za nenasilna kaznena djela (pronevjere, krivotvorenje isprava i sl., tj. NNK) te odgovarajuće skupine osoba iz opće populacije koje nikada nisu kažnjavane (OP). **Drugi cilj** istraživanja je utvrđivanje povezanosti između pojedinih osobina ličnosti (međusobno), osobina ličnosti i aspekata agresivnosti te između pojedinih aspekata agresivnosti (međusobno), posebno za uzorke NK, NNK te OP.

2. METODE

2.1. Sudionici

Ispitane su pravomoćno osuđene muške osobe koje se nalaze na izdržavanju kazne za djela NK (N=138), za djela NNK (N=149), kao i po relevantnim varijablama ujednačena (po dobi i spolu) skupina osoba OP (N=147). Svi sudionici u tri skupine bili su muškarci, približno istih godina. OP osobe bile su relativno najmlađe (u prosjeku imaju 33,03 godine), nešto starija (34,99 godina) bila je skupina NK, dok je skupina NNK bila relativno najstarija (35,59 godina). Međutim, dobne razlike među skupinama nisu bile statistički značajne.

2.2. Postupak

Sudionici koji se nalaze u kaznenim zavodima, kao i sudionici iz kontrolne skupine, testirani su dvama upitnicima agresivnosti (jedan je korišten u ovom istraživanju), jednim upitnikom ličnosti, te upitnikom o socioekonomskom statusu. Samo ispitivanje provedeno je u kaznenom zavodu Remetinec tijekom redovitog psihodijagnostičkog postupka kojeg obavezno prolaze sve pravomoćno osuđene osobe, dok je testiranje kontrolne skupine provedeno u Zavodu za zapošljavanje u Zagrebu (u sklopu redovnih aktivnosti testiranja osoba koje su povremeno prijavljene na burzu rada). Ispitivanje je provedeno grupno, u više grupa, najčešće do desetak sudionika. Prije testiranja sudionicima je bila pročitana uputa o načinu odgovaranja na tvrdnje iz svakog upitnika, a naglašena je i znanstvena svrha istraživanja uz garantiranu anonimnost. Kod prve dvije skupine sudionika (pravomoćno osuđene osobe za različita kaznena djela), varijabla obilježja počinjenog djela (NK ili NNK), kontrolirala se putem članka Kaznenog zakona na temelju kojeg su osuđeni. U kontrolnoj skupini sudionika (OP) isključeni su oni koji su prije provođenja istraživanja bili kažnjeni, bilo prekršajno, bilo kazneno. Nemotivirani sudionici iz sve tri grupe (koji su npr. zaokružili isti odgovor, npr. procjenom „1“ u svim testovima), bili su također eliminirani iz daljnjeg postupka. Vrijeme riješavanja nije bilo ograničeno, a sudionici su za vrijeme riješavanja upitnika mogli tražiti objašnjenja za nejasnoće.

2.3. Instrumenti

U prikupljanju podataka za potrebe ovog istraživanja korišteni su sljedeći mjerni instrumenti:

1. International Personality Item Pool (IPIP50) (Mlačić i Goldberg, 2007), koji mjeri ekstraverziju, neuroticizam, ugodnost, savjesnost i intelekt;
2. Upitnik za mjerenje agresivnosti (A-87) (Žužul, 1989) koji mjeri fizičku manifestnu i latentnu agresivnost, verbalnu manifestnu i latentnu agresivnost, te indirektnu agresivnost.

2.3.1. International Personality Item Pool (IPIP50) skala

IPIP50 sadrži 50 čestica te mjeri pet širokih dimenzija ličnosti iz modela Velikih Pet (Big Five) (ekstraverzija, neuroticizam, ugodnost, savjesnost i intelekt). Jednaka faktorska struktura pronađena je u više desetaka istraživanja koja su koristila različite uzorke sudionika, provođenih u različitim razdobljima, što upućuje na zaključak da je petofaktorska struktura stabilna u vremenu (Digman i Inoyue, 1986). I u hrvatskoj verziji IPIP50 upitnika, dobivena je jasna peterofaktorska struktura (Mlačić i Goldberg, 2007). Zadatak sudionika bio je da za svaku pojedinu tvrdnju označi u kolikoj mjeri pojedini iskaz opisuje baš njega, onakvog kakav se sada vidi. Dakle, na skali od pet stupnjeva (raspon od 1=posve netočno do 5=posve točno), sudionici označavaju broj koji odgovara njihovu samoopisu. Prilikom unosa i transformacije te kasnije analize podataka, procjene za dio tvrdnji se jednostavno zbraja (tvrdnje koje direkno ukazuju na posjedovanje neke osobine), dok se procjene za dio tvrdnji rekodiraju (tvrdnje koje opisuju manje posjedovanje neke osobine).

Bratko i Sabol (2006) ističu dobru pouzdanost tipa unutarnje konzistencije (Cronbach alfa) pojedinih skala. Koeficijenti se kreću od 0.88 za ekstraverziju, 0.81 za ugodnost, 0.82 za

savjesnost, 0.90 za neuroticizam te 0.78 za intelekt. Pojedine su skale u umjerenim korelacijama, pa tako ekstraverzija korelira s ugodnošću (r=0.33), savjesnošću (r=0.09), emocionalnom stabilnošću (r=0.23) te intelektom (r=0.34). Nadalje, ugodnost korelira sa savjesnošću (r=0.22), emocionalnom stabilnošću (r=0.06) te intelektom (r=0.17). Savjesnost je povezana s emocionalnom stabilnošću (r=0.19) i sa intelektom (r=-0.01). Dobivena je i povezanost između emocionalne stabilnosti i intelekta (r=0.09). U našem istraživanju (Vukosav i sur., 2015), koeficijenti nutarnje konzistencije upitnika iznose 0.86 za ekstraverziju, 0.83 za ugodnost, 0.83 za savjesnost, 0.88 za neuroticizam te 0.79 za intelekt. Korelacije između pojedinih skala upitnika pokazane su u tablici 1.

2.3.2. Upitnik agresivnosti A-87

A-87 temelji se na pretpostavci da postoje dva osnovna oblika agresije, impulzivna i instrumentalna, ovisno o motivaciji koja se nalazi u njihovoj podlozi (Žužul, 1989). Agresivnost kao crta ličnosti se očituje ili kao latentna tendencija za agresijom ili kao manifestno agresivno ponašanje. Upitnik mjeri pet različitih značajki agresivnosti: fizičku manifestnu i latentnu agresivnost, verbalnu manifestnu i latentnu agresivnost, te indirektnu agresivnost. Suštinski je namijenjen mjerenju impulzivne agresivnosti (kao latentne i manifestne osobine ličnosti). Sastoji se od 15 opisanih situacija koje se odnose na ranije spomenute dimenzije agresivnosti koje upitnik mjeri, a pet mogućih odgovora za svaku situaciju se odnose na 5 navedenih modaliteta agresivnog reagiranja. Zadatak je sudionika je da za svaki od 5 ponuđenih odgovora izrazi svoj stupanj slaganja, u rasponu od: 1= „baš se nikad tako ne ponašam“ do 5= „vrlo često se tako ponašam“. Rezultati na svim subskalama definirani su kao jednostavna linearna kombinacija, a veći zbroj procjena znači i veću agresivnost.

U istraživanjima, koeficijenti nutarnje konzistencije upitnika (Cronbach alfa) kreću se u rasponu od 0.76 (za indirektnu agresivnost) do 0.91 (za fizičku latentnu agresivnost), dok je pouzdanost cijelog upitnika izrazito visoka i iznosi 0.97 (Knezović i sur., 1989). U našem istraživanju (Vukosav i sur., 2015), koeficijenti nutarnje konzistencije upitnika (Cronbach) kreću se u rasponu od 0.79 (za indirektnu agresivnost) do 0.93 (za fizičku latentnu agresivnost), dok je pouzdanost cijelog upitnika izrazito visoka i iznosi 0.97.

2.4. Statističke analize

Podaci su analizirani statističkim paketom IBM SPSS 20.0. Uz temeljnu deskriptivnu statistiku za čestice upitnika (izračunatu u sklopu diskriminacijske analize), ispitane su pouzdanosti interne konzistencije u oba primijenjena upitnika *(Cronbach alpha).* Pearsonovim koeficijentima korelacije utvrđena je povezanost između pojedinih osobina ličnosti (međusobno), osobina ličnosti i aspekata agresivnosti te između pojedinih aspekata agresivnosti (međusobno), posebno za uzorke NK, NNK te OP. Diskriminacijskom analizom utvrđeno je postojanje faktora razlika između rezultata koje postižu sudionici iz tri različite skupine (NK, NNK i OP).

3. REZULTATI

Pearsonove interkorelacije svih dimenzija upitnika agresivnosti A-87 za uzorke NK, NNK i OP pokazuju podjednake tendencije: sve korelacije su pozitivne, u prosjeku srednje visoke i statistički značajne uz $p<0,01$. I interkorelacije između svih dimenzija upitnika IPIP50 za uzorke NK, NNK i OP pokazuju podjednake tendencije: sve korelacije su pozitivne, u prosjeku su relativno niske i većinom statistički značajne uz $p<0,01$ (jedina statistički neznačajna korelacija pronađena je u uzorku NK, koji u prosjeku ima najmanje povezane karakteristike ličnosti). Unakrsne korelacije između dimenzija upitnika ličnosti IPIP50 te upitnika agresivnosti A-87 za tri različite skupine sudionika pokazuju prilično različite tendencije. Primjerice, za skupinu OP broj statistički značajnih korelacija je najmanji (4), sve su pozitivne i pronađene su između varijabli agresivnosti (verbalne manifestne i verbalne latentne) i intelekta te ekstraverzije. Skupine kažnjenika (tj. NK i NNK) pokazuju slične obrasce korelacija. Premda su sve korelacije statistički značajne, negativnog smjera i vrlo niske, sve su pronađene su između istih osobina ličnosti (ugodnost, savjesnost i emocionalna stabilnost) i varijabli agresivnosti.

Tablica 1. Korelacije između dimenzija upitnika ličnosti IPIP50 te upitnika agresivnosti A-87 za tri različite skupine sudionika istraživanja

Nasilnički kriminalitet	vermanif	fizmanif	indirekt	verlaten	fizlaten	intelekt	ekstrave	ugodnost	savjesno	emocstab
ver. manifestna	1	,696**	,698**	,699**	,537**	,094	,022	-,154	-,181*	-,266**
fiz. manifestna		1	,814**	,541**	,821**	-,045	,024	-,294**	-,246**	-,218*
indirektna			1	,642**	,781**	-,113	,019	-,306**	-,253**	-,309**
ver. latentna				1	,672**	,069	-,028	-,065	-,212*	-,139
fiz. latentna					1	-,042	,015	-,258**	-,264**	-,178*
intelekt						1	,157	,409**	,302**	,217*
ekstraverzija							1	,228**	,203*	,269**
ugodnost								1	,468**	,369**
savjesnost									1	,250**
emoc.stabilnost										1
Nenasilnički kriminalitet	vermanif	fizmanif	indirekt	verlaten	fizlaten	intelekt	ekstrave	ugodnost	savjesno	emocstab
ver. manifestna	1	,678**	,757**	,720**	,645**	,087	,122	-,084	-,268**	-,256**
fiz. manifestna		1	,770**	,524**	,801**	,002	-,034	-,193*	-,242**	-,313**
indirektna			1	,740**	,754**	-,040	-,005	-,181*	-,375**	-,419**
ver. latentna				1	,665**	,060	,058	,011	-,264**	-,342**
fiz. latentna					1	,053	,009	-,165*	-,275**	-,362**
intelekt						1	,439**	,482**	,448**	,315**
ekstraverzija							1	,482**	,292**	,371**
ugodnost								1	,562**	,421**
savjesnost									1	,595**
emoc.stabilnost										1
Neosudivani	vermanif	fizmanif	indirekt	verlaten	fizlaten	intelekt	ekstrave	ugodnost	savjesno	emocstab
ver. manifestna	1	,571**	,629**	,626**	,554**	,197*	,207*	,060	-,021	,024
fiz. manifestna		1	,794**	,363**	,756**	,026	,031	-,117	-,097	-,107
indirektna			1	,591**	,753**	,042	,079	-,097	-,118	-,100
ver. latentna				1	,571**	,218**	,170*	,074	,011	,154
fiz. latentna					1	,066	,079	-,120	-,087	-,058
intelekt						1	,581**	,579**	,391**	,265**
ekstraverzija							1	,426**	,336**	,366**
ugodnost								1	,442**	,333**
savjesnost									1	,453**
emoc.stabilnost										1

Vrijednost Wilksove λ pokazuje da je prva diskriminacijska funkcija statistički značajna te da stoga statistički značajno razlikuje tri grupe sudionika po varijablama ličnosti iz IPIP50 upitnika (tablica 2). Centroidi grupa su dosta udaljeni, te iznose 0,079 za grupu NK, -0,317 za NNK te 0,254 za OP (drugim riječima, najudaljenije su grupe OP i NNK). Predviđanjem grupne pripadnosti na temelju diskriminacijske funkcije, pokazalo se da se na temelju diskriminacijske funkcije može uspješno grupirati 45% originalno grupiranih slučajeva. Rezultati univarijatne analize varijance u odnosu na diskriminacijsku funkciju ukazuju na postojanje statistički značajnih razlika u dvije dimenzije ličnosti iz upitnika IPIP50: Ekstraverzija (najveći prosječni rezultati za OP) i Emocionalna stabilnost (najveći prosječni rezultati za NNK) (tablica 2).

Tablica 2. Diskriminacijska analiza rezultata tri grupe sudionika istraživanja na temelju dimenzija upitnika ličnosti IPIP50

	Karakter. korijen	% varijance	Kanonička korelacija	Wilksov lambda (df)	**p**
	0,059	79,3	0,236	**0,930 (10)**	**0,001**

Varijabla	Wilks λ	Stand. disk. koefic.	F-test (2,428)	p	**M** nasilnički	**σ** nasilnički	**M** nenasilnički	**σ** nenasilnički	**M** neosuđivani	**σ** neosuđivani
intelekt	,990	-,362	2,072	>,10	29,686	4,695	29,567	5,552	30,750	5,958
ekstraverzija	,979	,218	**4,491**	**<,02**	31,066	5,339	30,907	5,815	**32,694**	5,649
ugodnost	,997	-,520	,627	>,10	37,365	5,641	36,947	6,926	37,778	6,401
savjesnost	,992	,475	1,728	>,20	36,686	6,058	37,833	7,051	36,563	6,191
emoc. stabilnost	,977	,325	**5,109**	**<,01**	33,102	7,155	**35,760**	7,593	33,965	6,868

4. RASPRAVA

Tri grupe sudionika iz ovog istraživanja (NK, NNK i OP) razlikuju se po varijablama ličnosti iz IPIP50 upitnika. Najekstravertiraniji su pripadnici OP, a emocionalno najstabilniji NNK. Među ostalim osobinama ličnosti nisu pronađene statistički značajne razlike. Najveću emocionalnu stabilnost u uzorku NNK može se potencijalno protumačiti činjenicom da je jedna od značajki uzorka neosuđivanih osoba (OP) iz ovog istraživanja njihov radni status. Premda većina članova uzorka OP ima trenutačno zaposlenje, mnogi od njih su zaposleni na određeno vrijeme, a u doba gospodarske krize i recesije ovakav status može biti dodatni izvor frustracije zbog straha za vlastitu materijalnu egzistenciju, što može utjecati i na razinu njihove agresivnosti (Vukosav et al., 2014), ali i emocionalne nestabilnosti. Naime, u mnogim je istraživanjima pokazano da nezaposlene osobe iskazuju visoku razinu agresivnosti (Pakes i Pakes, 2009).

Podjednake tendencije interkorelacija koje su pronađene u sve tri grupe sudionika za A-87 i IPIP50 upitnike jednostavno mogu ukazivati na činjenicu da upitnici imaju jedinstvene predmete mjerenja (ličnost, odnosno agresivnost u najširem smislu). Unakrsne korelacije drugačije su za skupine kažnjavanih (NK, NNK) u odnosu na nekažnjavane (OP) sudionike. Vrlo niske a pozitivne korelacije između relativno poželjnih oblika agresivnosti (verbalna agresivnost – manifestna i latentna) i intelekta te ekstraverzije u uzorku OP mogu se protumačiti vjerojatnom impulzivnošću ekstraverata (Eysenck i Eysenck, 1994_a, 1994_b), koji vjerojatno imaju i veću mogućnost sukobljavanja s okolinom, tijekom vlastitog traganja za novim iskustvima. S druge strane, niske negativne korelacije između osobina ličnosti (ugodnost, savjesnost i emocionalna stabilnost) i varijabli agresivnosti zapravo se mogu očekivati kod kažnjavanih osoba općenito, a posebno pravomoćno osuđenih osoba za kaznena djela s elementima nasilja (NK). Naime, kod tih osoba je općenito povišena agresivnost, što su pokazali i rezultati ranijih istraživanja (Knezović i sur., 1989.; Mejovšek i sur., 1997.; Farrington, 2003.; McGuire, 2004).

Pri tumačenjima dobivenih rezultata, treba imati u vidu činjenicu da je ovo istraživanje provedeno za vrijeme uobičajenog psihodijagnostičkog tretmana kojeg prolaze sve pravomoćno osuđene osobe i o čijim rezultatima može ovisiti smještaj osuđenika u kaznene zavode (zatvoreni, otvoreni ili poluotvoreni) (Vukosav i sur., 2015). Iz navedenih razloga, osobito u slučaju upitnika agresivnosti, moguće je da su nenasilni osuđenici potcjenjivali razinu vlastite agresivnosti nadajući se povoljnijem ishodu, što je moglo utjecati i na povezanosti među varijablama agresivnosti ali i između varijabli agresivnosti i varijabli ličnosti. Također, moguće je da su svi sudionici, u većoj ili manjoj mjeru, imali težnju favorizirati vlastite poželjne osobine ličnosti, što je moglo dovesti do minimaliziranja razlika u pogledu varijabli ličnosti, između tri uzorka sudionika. Istovremeno, ista potencijalna tendencija „prikazivanja u društveno poželjnom svjetlu“ mogla je rezultirati i nižim korelacijama s obilježjima agresivnog ponašanja. Ne smije se zaboraviti niti da, premda između navedenih skupina ne postoje statistički značajne razlike u dobi, grupa NNK je relativno bila najmlađa, nešto starija bila je skupina NK, dok je skupina OP bila najstarija. Budući da u starijoj dobi dolazi do određenog pada razine agresivnosti (Farrington, 2003),

moguće je da je i dobna struktura djelomice pridonijela dobivenim razlikama (Vukosav i sur., 2015).

Prednost istraživanja je u činjenici da je riječ o relativno rjeđem istraživanju u našem podneblju, koje je obuhvatilo specifičnu populacije pravomoćno osuđenih za kaznena djela nasilničkog i nenasilničkog kriminaliteta na izdržavanju zatvorske kazne, ali i specifične subpopulacije neosuđivanih sudionika (koji nemaju stalan radni status). Nedostatak istraživanja je veličina uzorka i situacijska specifičnost mjesta gdje je istraživanje provođeno, pa bi u budućim istraživanjima bilo pogodno obuhvatiti veći, reprezentativniji (npr. stratificirani) uzorak sudionika, diferenciran po razinama obrazovanja, spolu, dobnim skupinama (Vukosav i sur., 2015), ali po specifičnim oblicima kriminaliteta. Rezultati ovog i sličnih istraživanja mogu pomoći otkrivanju rizičnih čimbenika, koji u interakciji s „pogodnom“ okolinom mogu dovesti do delinkventnog ponašanja. Naime, utvrđivanjem tih rizičnih čimbenika može se sustavnije preventivno djelovati u smjeru smanjivanja razine njihove pojavnosti, a time i pojavnosti nasilničkog ali i nenasilničkog kriminaliteta.

5. ZAKLJUČCI

Interkorelacije između svih dimenzija upitnika IPIP50 i A-87 za uzorke NK, NNK i OP pokazuju podjednake tendencije: sve korelacije su pozitivne, u prosjeku su relativno niske i većinom statistički značajne uz $p<0,01$. S druge strane, unakrsne korelacije između svih dimenzija upitnika IPIP50 i A-87 za tri različite skupine sudionika pokazuju prilično različite tendencije. Za skupinu OP broj statistički značajnih korelacija je najmanji, a pozitivne, vrlo niske i statistički značajne korelacije pronađene su između varijabli relativno poželjnih oblika agresivnosti i intelekta te ekstraverzije. Skupine kažnjenika (tj. NK i NNK) pokazuju slične obrasce korelacija. Statistički značajne, negativne i vrlo niske korelacije kod ove dvije skupine pronađene su između istih osobina ličnosti (ugodnost, savjesnost i emocionalna stabilnost) i varijabli agresivnosti. Diskriminacijska finkcija statistički značajno razlikuje tri grupe sudionika po varijablama ličnosti iz IPIP50 upitnika, a razlike su razvidne u dvije dimenzije ličnosti: Ekstraverzija (najveći prosječni rezultati za OP) i Emocionalna stabilnost (najveći prosječni rezultati za NNK).

LITERATURA

Bratko, D. Sabol, J. (2006): Osobine ličnosti i osnovne psihološke potrebe kao prediktori zadovoljstva životom: rezultati on-line istraživanja. *Društvena istraživanja*, 4-5, 693-713.

Costa, P.T. Jr.,i McCrae, R.R. (2005). *NEO PI-R priručnik*. Jastrebarsko: Naklada Slap.

Digman, J. M., & Inoyue, J. (1986). Further Specification of the Five Robust Factors of Personality. *Journal of Personality and Social Psychology,* 50(1), 116-123.

Eysenck, H. J. i Eysenck, S. B. G. (1994_a). *Norme za Eysenckov upitnik ličnosti: Oblik za odrasle*. Ur. Miharija, Ž. Jastrebarsko: Naklada Slap.

Eysenck, H. J. i Eysenck, S. B. G. (1994_b). *Eysenckove skale ličnosti*. Ur. Vizek-Vidović, V. Jastrebarsko: Naklada Slap.

Farrington, D.P. (2003). Key results from the first years of the Cambridge Study in Delinquent Development. U: Thornberry, T.P., Krohn, M.D. (ur.) *Taking. Stock of Delinquency:An Overview of Findings from Contemporary Longitudinal Studies*. New York: Kluver Academic/Plenum Publishers.

Huesmann, L.R., Eron, L.D., Lefkowitz, M.M., Walder, L.O. (1984). Stability of aggression over time and generations. *Developmental Psychology, 20,* 1120-1134.

Knezović, Z., Kulenović, A., Šakić, V., Zarevski, P., & Žužul, M. (1989). *Psihološke karakteristike osuđenih osoba*. Zagreb: Znanstvena edicija časopisa Penološke teme.

McCrea, R.R., & Costa, P.T. Jr. (1997). Validation of the five-factor model of personality across instruments and observers. *Journal of Personality and Social Psychology,* 52, 81-90.

McCrea, R.R., & Costa, P.T. Jr. (1999). A five-factor theory of personality. In I.A. Pervin (ed.). *Handbook of personality: Theory and research*. New York: Guilford.

McGuire, J. (2004). *Understanding psychology and crime*. Glasgow: Bell & Bain Ltd.

Mednick, S.A.; Christiansen, K.O. (1977). *Biosocial Bases of Criminal Behaviour*. New York: Gardner Press.

Mejovšek, M. (1989): Evaluacija institucionalnog penološkog tretmana. *Penološke teme,* 4 (1-2), 1-9.

Mejovšek, M., Cajner-Mraović, I., Buđanovac, A. (1997). Obilježja ponašanja i obitelji maloljetnih počinitelja nasilnih i nenasilnih delikata. *Hrvatska revija za rehabilitacijska istraživanja*, 33, 23-35.

Mlačić, B, & Goldberg L.R. (2007). An analysis of a cross-cultural personality inventory: The IPIP Big-Five factor markers in Croatia. *Journal of Personality Assessment,* 88, 168-177.

Ozer, D.J., & Reise, S.P. (1994). Personality assessment. *Annual Review of Psychology,* 45, 357-388.

Pakes, F.J., Pakes, S. (2009). *Criminal psychology*. Cullompton, Devon: Willan Publishing.

Vukosav, J. (2001). Faktorska struktura novog upitnika agresivnosti. *Policija i sigurnost,* 10 (1-6), 1-22.

Vukosav, J. (2002). Razlike u agresivnosti i doživljaju tretmana između osuđenika iz otvorenih i zatvorenih kaznenih zavoda. *Policija i sigurnost, 11 (4-6),* 163-202.

Vukosav, J. (2006). Kriminalistika i psihologija. U: Pavišić, B., Modly, D., Veić, P. (ur.) *Kriminalistika.* Zagreb: Golden marketing-Tehnička knjiga, 51-91, 490-493.

Vukosav, J., Glavina Jelaš, I., Sindik, J. (2015). Razlikovna obilježja agresivnog ponašanja počinitelja nasilničkog kriminaliteta. U: *Proceedings book - 4th International Scientific and Professional Conference „Police College Research Days In Zagreb*“. Butorac, K. (ur.). Zagreb, Hrvatska, 23.-24.4.2015., str. 425-439. Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske.

Žužul, M. (1989). *Agresivno ponašanje: psihologijska analiza*. Zagreb: Radna zajednica Republičke konferencije Saveza socijalističke omladine Hrvatske.

Žužul, M., Knezović, Z., Šakić, V. (1989). Da li je agresivnost patološka osobina ličnosti? *Penološke teme, 4,* 201-206.

Joško Vukosav
Joško Sindik
Ivana Glavina Jelaš

PERSONALITY OF THE PERPETRATORS OF THE VIOLENT AND NON-VIOLENT CRIME

Summary

The five-factor personality model (Big Five) may single out the profile of a person who is more or less prone to commit certain types of crimes. The main aim of this study was to determine whether significantly different personality traits could distinguish three groups of persons: persons convicted of serious crimes in the domain of violent crime (murder, rape, etc., i.e. NK), persons convicted of non-violent crimes (fraud, forgery of documents, etc., i.e. NNK) and a relevant group of people from the general population who have never been convicted (OP). Furthermore, we wanted to establish the connection between personality variables and variables of aggressiveness, separately for each group: NK, NNK and OP. Three different homogeneous age group of male participants have been tested: NK (N = 138), NNK (N = 149) and the general population control group OP (N = 147). Two measuring instruments have been used: International Personality Item Pool (IPIP50) and Aggressiveness A-87 Questionnaire. Discriminant analysis results have shown statistically significant differences in the personalities of people belonging to each of the three groups of participants (NK, NNK and OP), precisely in aspects of extraversion and emotional stability. Moreover, some differences can be detected in the connections between research variables, for different groups of study participants. The results of the study can be used for modeling successful prevention measures, primarily for preventing the occurrence of violent or non-violent crimes.

Key words*: criminal acts, Five-factor personality model, convicted, differences.*

STRUČNI RAD

Ruža Karlović[233]
Danijela Petković[234]
Karla Kiš Kamenjarin[235]

STAVOVI POLICIJSKIH SLUŽBENIKA O UVOĐENJU NOVIH TEHNOLOGIJA U POLICIJSKI RAD

Sažetak

Cilj rada je utvrditi stavove policijskih službenika o uvođenju novih tehnologija u policijski način rada. Na temelju mišljenja policijskih službenika moguće je dobiti uvid u razinu njihove informiranosti te primjenjivosti elektroničke komunikacije u svakodnevnom policijskom radu, ali i stav u pogledu njihovog odobravanja ili neodobravanja o uvođenju novih tehnologija u policijski rad.

Analizirani podaci prikupljeni su anketnim ispitivanjem provedenim 2015. godine na prigodnom uzorku (N=50) policijskih službenika koji dolaze iz različitih policijskih uprava u Republici Hrvatskoj. Sudjelovalo je 78% muških (39) i 22% ženskih (11) ispitanika u rasponu starosne dobi od 28 do 45 godina (M=34) te u rasponu godina staža u policiji od 5 do 26 (M=14). Policijski službenici iskazali su stavove o novim tehnologijama u odgovorima na Likertovoj skali od 1 (potpuno se slažem) do 5 (uopće se ne slažem).

Važno je naglasiti da je ovo samo preliminarno istraživanje čiji rezultati sugeriraju kako bi i u budućnosti trebalo ispitivati stavove policijskih službenika kao krajnjih korisnika novih tehnologija, ali i pratiti učinkovitost policije u svakodnevnom radu. U ovom istraživanju se pokazalo da većina ispitanika odobrava uvođenje novih tehnologija, u policijsku svakodnevicu te da ispitanici imaju pozitivne stavove o jačanju odnosa policije, građana i drugih društvenih aktera kroz nove informacijsko-komunikacijske alate kao što su eDojave, snimanje policijskih intervencija, AVL sustav i slično. Posebnu pozornost u budućem istraživanju zaslužuju ambivalentni stavovi policijskih službenika o primjeni novih tehnologija u svakodnevnom radu policije.

Ključne riječi: *stavovi, policijski službenici, elektronička komunikacija, građani, policijski rad.*

[233] Ruža Karlović, Visoka policijska škola, Policijska akademija MUP RH
[234] Danijela Petković, Policijska akademija, MUP RH.
[235] Karla Kiš Kamenjarin, Služba za međunarodnu policijsku suradnju, MUP RH.

1. UVOD

U današnjem svijetu tehnologija je sastavni dio društvenih institucija i njihovih komponenti, tj. organizacija, grupa pa tako i policije kao društvene institucije i službe. Neki autori uvođenje tehnologije u policijski sustav navode u kontekstu razvojnih faza policijskih modela funkcioniranja. Tako, primjerice Kelling, Moore (1988) ističu kako je uvođenje tehnologije u policijski rad dio faze profesionalizacije policije 60-ih i 70-ih godina prošlog stoljeća. U toj fazi policijski posao se oslanjao na policijske radio-telefonske veze, sustav 911 i automobilske patrole, kako bi što brže reagirali na dojavu o nekoj intervenciji ili na pozive građana. U tom periodu policija se bavila samo kažnjivim radnjama, a na druge probleme u određenoj lokalnoj sredini gledalo se kao na probleme koje trebaju rješavati neke druge lokalne službe. Prije gotovo pola stoljeća, tj. 70-ih godina prošlog stoljeća započela je faza policije u zajednici *community policing.* Spomenuti autori Kelling, Moore (1988) u to doba su raspravljali o razvojnim fazama policije u američkom društvu jer je u navedenom periodu kriminal počeo rasti, ali su istraživanja pokazala da uvođenje tehnologije na tadašnjem stupnju razvoja kao što je sustav 911, računalna oprema u policijskog službi, ipak nije ispunila očekivanja koja je javnost imala od policije jer se policija prije svega fokusirala na brzi odgovor na kriminalna djela koja su se već dogodila, a nije se bavila uzrocima kriminala u konkretnoj zajednici, tj prevencijom kriminala. Policija se bavila samo kriminalom, a ostale probleme je prepuštala drugim društvenim službama, što je rezultiralo slabljenjem veza između policije i građana. Zato se pojavila potreba za daljnjim razvojem modela funkcioniranja policije na lokalnoj razini, tj. pokušaj spajanja novih tehnologija i vraćanja pješačkih patrola među građane.

Uvođenje novih tehnologija u policijski način rada s namjerom da jačaju veze između policije i građana te osjećaj sigurnosti kod građana, opet je aktualna tema. Ljudski faktor i fizički kontakt u svim fazama razvoja policije pokazao se ključnim. Mnogobrojna su istraživanja provedena na temu uvođenja (i korištenja) informacijskih tehnologija u policijski posao. Tijela za provođenje zakona u cijelome svijetu se sve više okreću informacijskim tehnologijama, što neminovno dovodi do značajnih promjena u obavljanju policijskih poslova. Nova tehnološka rješenja s jedne strane doprinose učinkovitijem radu policije jer omogućavaju policijskim službenicima brži i bolji pristup podacima o osobama i predmetima, a s druge strane "udaljavaju" policijske službenike od građana (tehnologija postaje posrednik između policijskih službenika i građana). Nova tehnološka rješenja rad policije skreću prema onome što se naziva *intelligence led policing* – postupanje policije koje se temelji na obavještajnim podacima. Fokus se odmiče od prevencije i represije te se približava postupanju po procjenama rizika koje se temelje na obavještajnim (i drugim) podacima (Sanders, Hannem, 2012).

Bez obzira što različita društva imaju različite modele funkcioniranja policije i tipove ustroja policijskih organizacija, uvođenje nove tehnologije u svakodnevni policijski rad zajedničko je većini policijskih organizacija. U sadašnjem društvu stručnjaci naglašavaju dvostruku ulogu novih tehnologija – s jedne strane olakšavanje policijskoga posla, a s druge strane nove prilike za počinitelje kaznenih djela. U skladu s tim, na europskoj razini prije nekoliko godina provodio se projekt ICT *Trends in European Policing* koji je započeo 2011.

godine[236]. U sklopu tog europskoga istraživačkog projekta pod akronimom COMPOSITE (*Comparative Police Studies in The EU*) kojemu je bio cilj istražiti promjene unutar policijskih snaga, jedan je radni paket bio posvećen tehnološkim prilagodbama, točnije procesima promjene u vezi s novim informacijskim i komunikacijskim tehnologijama. U navedenom projektu predstavljen je pregled ICT alata koji se koriste u policijskim tijelima diljem Europske unije. Jedna od tema koja se proučavala u sklopu navedenoga projekta bila je i kako policijski službenici prihvaćaju nove tehnologije. Zbog nedostatka sveobuhvatne edukacije o korištenju alata, policijski su službenici često stavljeni u pozicije da ne znaju (ili ne mogu) koristiti glavne značajke određenih alata. Kroz ovaj projekt pokazalo se da se tehnološki alati ne koriste zbog nedostatka prihvaćenosti takvih novina ili zbog nedostatka edukacije. Drugim riječima, koriste se samo osnovne značajke alata. Prilikom uvođenja novih ICT alata često se pojavljuje problem promjene ustaljenih obrazaca postupanja.

Europska unija je prepoznala važnost uvođenja novih tehnologija u policijski posao u svrhu približavanja policije građanima i obrnuto. Pet godina kasnije, kroz program Obzor 2020, Europska komisija financira projekte iz područja sigurnosti zajednice, namijenjene jačanju uloge policije u zajednici. Jedan od tih projekata je i *Unity*[237]. Navedeni projekt vodi *Office of the Police and Crime Commissioner for West Yorkshire* uz 15 partnera iz 10 europskih država, a Hrvatsku predstavlja Policijska akademija. Radi se o trogodišnjem projektu čiji je cilj jačanje veze između policije i zajednice u svrhu stvaranja sigurnijih društava u Europi. *Unity* želi pomoći agencijama za provedbu zakona u stvaranju novog oblika rada policije u zajednici (stvorit će novi oblik rada policije u zajednici), koji se temelji na potrebama zajednice u kojoj policija djeluje. Projektom će se istražiti koje su najbolje prakse u suradnji policije i građana te na temelju rezultata provedenih istraživanja pronaći nova tehnološka rješenja za jačanje, poticanje i ubrzavanje komunikacije između policije i građana. Komunikacijske tehnologije koje će se razviti na temelju rezultata istraživanja, testirat će se u šest država Europske unije (Hrvatska, Estonija, Njemačka, Belgija, Finska i Ujedinjeno Kraljevstvo). U sklopu projekta *Unity* provodit će se aktivnosti podizanja svijesti o policiji u zajednici te edukacija policijskih službenika o novim tehnologijama. U sklopu navedenoga projekta, na sastanku Konzorcija, u Zagrebu, u studenome 2015. godine, predstavljeni su i prvi rezultati uvođenja novih tehnoloških rješenja u hrvatskoj policiji u sklopu hrvatskog projekta e-Policija.

2. RAZLOZI I CILJ OVOG ISTRAŽIVANJA

Poznati sociolog Garland (2001) prije 15 godina raspravljao je o tome kako bi primjena tehnologije u kontroli kriminaliteta mogla postati nova kultura kontrole kriminaliteta i to više u negativnom kontekstu, nego u pozitivnom jer bi nova tehnologija mogla povećati nepovjerenje građana jednih u druge u nekom društvu. S obzirom na karakteristike suvremenih društava, policiji je važno, na lokalnom području osobito, pronaći ravnotežu u primjeni novih tehnologija u svrhu kvalitetnijeg funkcioniranja i jačanja socijalne kohezije među građanima. U literaturi se može pronaći tvrdnja kako informacijska tehnologija ima važan utjecaj na policijsku praksu. Autori koji to tvrde, također navode kako policijski

[236] Više na https://www.fit.fraunhofer.de/content/dam/fit/de/documents/composite_d41.pdf
[237] www.unity-project.eu

službenici mogu odbijati korištenje informacijskih tehnologija, ako vjeruju da će (im) nove tehnologije utjecati na njihove uloge u uobičajenoj društvenoj strukturi matične organizacijske jedinice, primjerice da će ih nove tehnologije sprječavati da se druže sa svojim kolegama (Colvin i Goh, 2005). Poznato je, iz rasprava o policijskog subkulturi, kako su policijski službenici pragmatični, što u kontekstu uvođenja novih tehnologija znači da će policijski službenici najprije tražiti moguće negativne posljedice uvođenja tehnologije u policijski posao. To znači da bi, kao i u slučaju svake druge promjene, proces implementacije očekivano, iz različitih razloga, mogao potrajati duži period. Međutim, Gottschalk, Holgersson (2006) navode kako korištenje informacijske tehnologije u policijskom radu poboljšava kvalitetu djelovanja policijske organizacije.

Percepcija je važna odrednica za korištenje informacijske tehnologije. Iako mnogi policijski službenici prikupljene podatke percipiraju kao moć, kontrolu i utjecaj te kasnije, kao vrijednost i dobitak, informacijska tehnologija nema isti utjecaj na proces prikupljanja podataka u policijskom radu kao na proces prikupljanja podataka u poslovnom svijetu zbog prirode policijskog posla (Manning, 2003).

Flanagan (2002) tvrdi da agencije za provedbu zakona imaju neke prepreke u usporedbi s ostalim agencijama u smislu dobivanja koristi od informacijske tehnologije. Struktura policijskih organizacija, karakteristike policijskog rada, zahtjev za postizanje učinkovite obrade podataka neke su od navedenih prepreka koje sprečavaju policajce u korištenju informacijske tehnologije kao učinkovitog alata, kao što to čine korisnici u drugim okolnostima, primjerice u poslovnom svijetu. Općenito, agencija za provođenje zakona ima tradicionalnu hijerarhijsku birokraciju u kojoj se nalozi dodjeljuju i diktiraju.

Collier (2006) upozorava da u policijskom radu glavni problem nije dostupnost informacije, nego pristup informaciji kad je to potrebno.

U hrvatskoj policiji je prije nekoliko godina započelo uvođenje novih aplikacija u svrhu modernizacije policijskog rada[238]. Projekt e-Policija u našem sustavu podrazumijeva: aplikaciju sustava rada policijskih službenika na terenu, aplikaciju sustava za snimanje postupanja policijskih službenika, aplikacije za dojave građana, geokodiranje događaja, unapređenje AVL – *Automatic Vehicle Location* sustava i korištenje *Viber i Whats App* aplikacija. U okviru projekta e-Sigurnost (e-Policija) izrađena je aplikacija sustava za rad policijskih službenika na terenu, koja se sastoji od stacionarnog dijela aplikacije za planiranje, pripremu, usmjeravanje i praćenje policijske službe na terenu te mobilnog dijela aplikacije za neposredan rad na terenu na mobilnom tablet uređaju.

Kao dio istog projekta e-Sigurnost (e-Policija) razvijen je i sustav za snimanje postupanja policijskih službenika, koji se sastoji od malih prijenosnih kamera, baznih uređaja za pohranjivanje kamera koje se ne koriste i aplikacije preko koje se prenose, pohranjuju, pregledavaju i koriste snimke koje su policijski službenici snimili tijekom službe.

U računala operativno-komunikacijskih centara instalirana je aplikacija za primanje dojava građana u obliku fotografija i/ili videosnimaka koje građani mogu poslati sa svojih

[238] http://www.mup.hr/222830/16.aspx na Policijskoj akademiji je prezentiran projekt e-Policija u listopadu 2015. godine.

mobilnih uređaja. Pritom je poželjno da građani imaju na svom uređaju aktiviranu opciju lociranja mjesta snimanja događaja. Programskom aplikacijom omogućeno je vremensko i prostorno praćenje događaja za što je nužno prilikom intervencije policijskih službenika bilježenje koordinata mjesta događaja (geografske širine i geografske dužine) koje policijski službenici na mjestu događaja očitavaju na TETRA uređaju veze kojom se služe tijekom službe. Vezano za navedene TETRA uređaje veze, poboljšan je sustav praćenja položaja policijskih službenika na terenu, odnosno poboljšan je rad AVL sustava.

Opći cilj ovog istraživanja bio je utvrditi stavove policijskih službenika o uvođenju novih tehnologija u policijski rad u sustavu policije u Republici Hrvatskoj. Pretpostavljalo se da će policijskih službenici s obzirom na svoje obrazovanje i radno iskustvo te uobičajene načine rada u službi, iskazivati pozitivne stavove o uvođenju novih tehnologija općenito, a osobito u kontekstu jačanja odnosa policije s građanima i drugim institucijama i službama s kojima policija surađuje.

3. METODE

U ovom radu podaci su prikupljeni anketnim ispitivanjima o uvođenju novih tehnologija u policijski rad na prigodnom uzorku policijskih službenika (N=50). Istraživanje na prigodnom uzroku policijskih službenika provedeno je anketom na izvanrednim studentima diplomskog studija kriminalistike na Visokoj policijskoj školi Policijske akademije.

Osnovne socio-demografske karakteristike uzorka policijskih službenika su u tablici 1.

Tablica 1: Osnovne socio-demografske karakteristike ispitanika

Uzorak	**Policijski službenici**
Godina istraživanja	2015
N	50
Raspon dobi	28 - 45
M_{dob} (SD)	34,37 (3,909) 5 - 26
Raspon staža	5 - 26
$M_{staž}$ (SD)	14,29 (4,626)
Udio muškaraca	39 (78%)

Tablica 2: Zvanja policijskih službenika

Zvanja	N	%
Policijski narednik	34	68,0
Viši policijski narednik	9	18,0
Policijski inspektor	2	4,0
Samostalni policijski inspektor	1	2,0
Viši policijski inspektor	1	2,0
Policajac	1	2,0
Ukupno	48	96,0
Bez odgovora	2	4,0
Ukupno	50	100,0

Tablica 3: Policijski rodovi

Rodovi policije	N	%
Temeljna	12	25,0
Kriminalistička	34	70,0
Osiguranje štićenih osoba	1	2,0
Ukupno	48	97,0
Bez odgovora	2	3,0
Ukupno	50	100,0

Tablica 4: Poslovi koje obavljaju policijski službenici

Policijski poslovi	N	%
Šef smjene	10	20,0
Kriminalistički poslovi	30	62,0
Prevencija	2	4,0
Osiguranje štićenih osoba	1	2,0
Instruktor za promet	1	2,0
Poslovi temeljne policije	2	4,0
Ukupno	48	96,0
Bez odgovora	2	4,0
Ukupno	50	100,0

Tablica 5: Policijske uprave iz kojih dolaze policijski službenici

Policijska uprava	N	%
zagrebačka	11	22,0
istarska	5	10,0
brodsko-posavska	4	8,0
međimurska	2	4,0
primorsko-goranska	6	12,0
karlovačka	2	4,0
sisačko-moslavačka	3	6,0
varaždinska	1	2,0
Ravnateljstvo	7	14,0
koprivničko-križevačka	3	6,0
požeško-slavonska	1	2,0
krapinsko-zagorska	3	6,0
osječko-baranjska	1	2,0
Ukupno	49	98,0
Bez odgovora	1	2,0
Ukupno	50	100,0

3.1. Instrument istraživanja

Empirijski dio istraživanja proveden je metodom ankete. U svrhu ovog istraživanja izrađen je vlastiti upitnik, tj. skala stavova Likertovog tipa od ukupno 12 tvrdnji. Prilikom sastavljanja tvrdnji vodili smo se razgovorima s policijskim službenicima koji su govorili iz vlastitog iskustva, ali i aktualnošću uvođenja novih aplikacija sa svrhom modernizacije policijskog rada. Sve tvrdnje u upitniku vezane su za nove tehnologije te njihovo probno uvođenje u pojedine policijske postaje na području Republike Hrvatske. Na tvrdnje se odgovaralo zaokružujući brojeve od jedan do pet koji su značili sljedeće: 1 – potpuno se slažem, 2 – uglavnom se slažem, 3 – ne mogu odlučiti, 4 – uglavnom se ne slažem, 5 – u potpunosti se ne slažem.

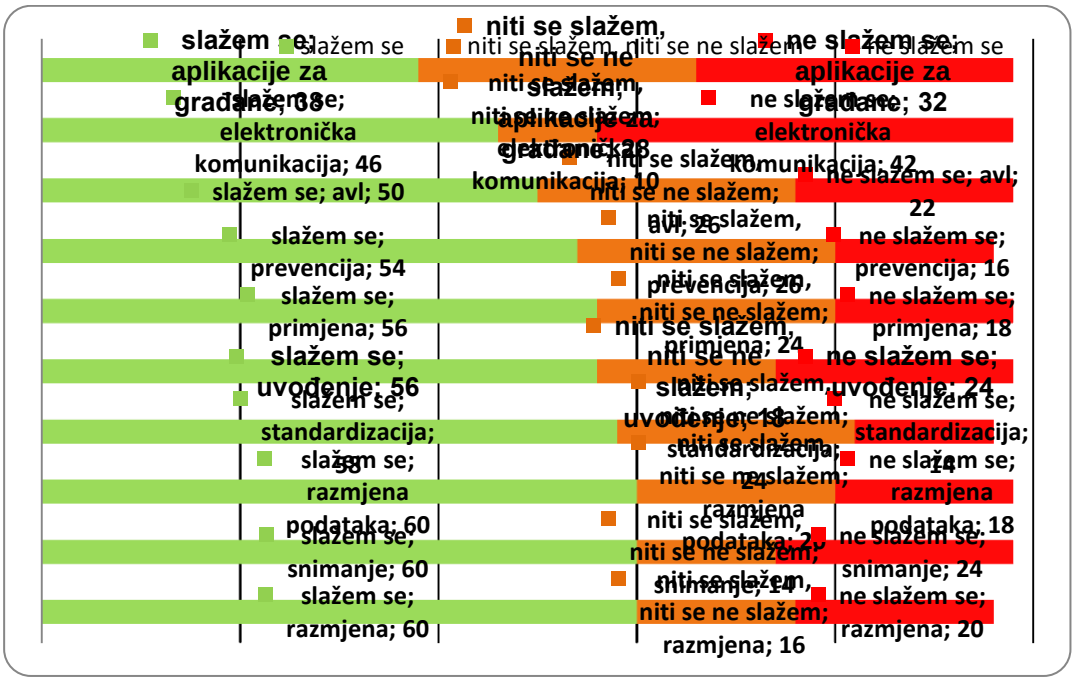
3.2. Postupak prikupljanja podataka

Upitnik je popunilo 50 ispitanika, tj. studenata specijalističkoga diplomskog stručnog studija kriminalistika. Ispitanici su popunjavali upitnik u Policijskoj akademiji, na Visokoj policijskoj školi tijekom seminarskog tjedna. Policijski službenici su popunjavali upitnik samostalno nakon što im je bio podijeljen i nakon što su dobili kratke upute za ispravno popunjavanje ankete. Anketiranim je osobama bila zajamčena anonimnost odgovora, to znači da upitnici nisu potpisivani, niti su imena sugovornika evidentirana.

3.3. Rezultati

Rezultati ovog upitnika samo su mali dio iskazanih stavova policijskih službenika. To u ovom slučaju znači onih koji završavaju specijalistički studij o uvođenju novih informacijsko-komunikacijskih tehnologija u svakodnevni policijski rad. Ovi ispitanici, kad nisu na studiju, na svojim su radnim mjestima u različitim policijskom upravama i s obzirom na poslove koje obavljaju svakodnevno su u kontaktu s građanima te rješavaju različite društvene devijacije na lokalnom području. U tom smislu, iako se radi o malom i homogenom uzorku, njihovi stavovi o uvođenju novih tehnologija te stavovi o zagovaranju suvremenih tehnologija u policijskom poslu, mogu ponuditi relevantnu osnovu policijskim rukovoditeljima koji rade na implementaciji novih tehnologija.

Za potrebe postizanja cilja ovog rada, u kontekstu statističke analize, za svaku tvrdnju iz upitnika navedene su distribucije rezultata, tj. frekvencije u pojedinoj varijabli kao jedan od načina dobivanja deskriptivnih informacija (Petz i sur., 2012).



Grafikon 1: Grafički prikaz frekvencije odgovora

Jačanje komunikacije policije i građana tema je koja zaokuplja pozornost u domaćoj i stranoj stručnoj literaturi već nekoliko desetljeća. U Republici Hrvatskoj, u policijskom diskursu, o toj temi u kontekstu reforme operativno-preventivnog rada policije u odori, tj. strategije policije u zajednici, intenzivno se raspravlja od 2003. godine[239] .

S obzirom na tehnološki razvoj društva, očekivano je da i policija u svoj rad uvodi različite informacijsko-telekomunikacijske alate.

[239] Više o tome vidi u objavljenom nacrtu projekta Reforma operativno-preventivnog rada policije u odori prije 13 godina (Faber, Cajner-Mraović, 2003), zatim Priručnik za policijske službenike o prevenciji kriminaliteta, objavljen 2013. godine kao nastavak Strategije policije iz 2013., godine.

Na tvrdnju u upitniku "Aplikacija za građane kojom mogu slati policiji sumnjiva ponašanja doprinosi jačanju odnosa između policije i građana", 38% policijskih službenika, od ispitanih se slaže, ali njih 32% se ne slaže, njih 28% niti se slažu, niti se ne slažu s tom tvrdnjom. Razlog takvim stavovima su možda njihova iskustava s građanima koji često zovu policiju i prijavljuju probleme koje policija ne bi trebala rješavati, primjerice kad građani, prema stvarnim događajima iz policijskog iskustva, zovu policiju jer je mačka zapela u kanti za smeće. Policijska patrola mora doći na mjesto događaja, mora zvati vatrogasce koji prerežu kantu i izvade mačku iz smeća. Međutim, za građane je već tradicionalno i uvriježeno pravilo da je policija služba dostupna 24 sata dnevno koja reagira na svaku dojavu i najoperativnija je služba u društvenoj strukturi

"Razmjena podataka s drugim institucijama elektroničkim putem je sigurna i jednostavna u mom poslu i mojoj instituciji", izjavilo je 46% anketiranih policijskih službenika, ali gotovo jednak postotak, 42% ispitanika, ne slaže se s navedenom tvrdnjom. Iskazani stavovi su možda rezultat manjka protokola o suradnji, tj, načinima razmjene informacija između ovlaštenih službi koji bi otklonili sumnje policijskih službenika o štetnim posljedicama razmjene podataka.

"Podaci o kretanju policijskih službenika na terenu će povećati policijsku učinkovitost (AVL – *Automatic Vehicle Location*)", izjavilo je 50% ispitanika. Ispitanici odobravaju praćenje pozicije policijskih službenika na terenu. Na taj način se dobiva ravnomjerna pokrivenost lokalnog područja, ali i pokrivenost onih mjesta koji su od sigurnosnog značaja za policiju te olakšava operativno-informacijskim centrima koordinacija patrola na terenu.

"Nove tehnologije doprinose prevenciji kriminaliteta", izjavilo je 54% ispitanih policijskih službenika. No, veliki dio ispitanika u ovom uzorku (26%), svoj stav o ovoj tvrdnji iskazao je kao neutralan, tj. niti se slažu niti ne slažu. Ovo zaslužuje detaljniju analizu, osobito veliki postotak izraženog ambivalentnog stava, zašto je to tako? Kroz razgovor s policijskim službenicima i na temelju njihovih iskustava, suvremene tehnologije, primjerice fiksne kamere za nadzor brzine kretanja vozila, sasvim sigurno pomažu policiji u kriminalističkom istraživanju kažnjivih ponašanja, ali postoji određena doza nezainteresiranosti i usuđujemo se reći skepticizma policijskih službenika prema prevenciji kriminaliteta. Sigurno postoji mnoštvo razloga koje ćemo istraživati detaljnije u budućem istraživanju na ovu temu.

"Primjenom novih tehnologija policajci će imati više vremena za rad na terenu", izjavilo je 56% ispitanika. Iskustveno je opaženo kako tehnologije podržavaju mladi jer se brzo adaptiraju te stariji koji su osobno motivirani za uvođenje novina u svoj rad, ostatak starijih policajaca pruža otpor zbog neznanja, manjka interesa, straha i slično.

"Da će uvođenje novih tehnologija jačati odnos policije s građanima i drugim institucijama", izjavilo je 56% ispitanika. Policajci iz iskustva također navode kako bi bilo vrlo praktično i učinkovito za postizanje bolje kvalitete života, pronaći način razmjene informacija s drugim institucijama i službama. Obrađene i razmijenjene informacije trebalo bi plasirati u javnu sferu kako bi građani bili upoznati s određenim sigurnosnim stanjem na području na kojem žive.

"Nove tehnologije će doprinijeti standardizaciji policijskog postupanja", slaže se 58% ispitanika. Policija se modernizira u tehnološkom smislu u skladu s financijskim mogućnostima, prije svega, ali i potrebama rada jer razvoj tehnologije potiče i razvoj fenomenologije kažnjivih djela. Projekt e-Sigurnost u hrvatskoj policiji započeo je s namjerom standardizacije rada policijskih službenika i kvalitetnijeg rada te financijske uštede. Velik postotak u ovom uzorku se niti slaže, niti ne slaže oko ove tvrdnje (24%). Jedan od razloga takvom stavu mogla bi biti još uvijek nedovoljna informiranost policijskih službenika o projektu koji je još u testnoj fazi, možda i sporije prihvaćanje ICT aplikacija. "Nove tehnologije će doprinijeti kvalitetnijoj razmjeni informacija između OKC-a i policijskih ophodnji", izjavilo je 60% ispitanika. Isti postotak ispitanika slaže se s tvrdnjom da "Snimanjem intervencija, policajci štite sebe od zlonamjernih prigovora građana na njihovo postupanje i građane od neprofesionalnog ili nezakonitog postupanja policijskih službenika".

4. ZAKLJUČAK

S obzirom na stavove policijskih službenika o njihovoj informiranosti i primjenjivosti informacijsko-komunikacijskih alata u policijskom radu, važno je naglasiti da je ovo samo preliminarno istraživanje čiji rezultati sugeriraju kako bi i u budućnosti trebalo ispitivati stavove policijskih službenika kao krajnjih korisnika novih tehnologija, ali i pratiti učinkovitost policijskih patrola u njihovom svakodnevnom radu. U ovom istraživanju se pokazalo da većina ispitanika odobrava uvođenje novih tehnologija u policijsku svakodnevicu te da ispitanici imaju pozitivne stavove o jačanju odnosa policije, građana i drugih društvenih aktera kroz nove informacijsko-komunikacijske alate kao što su e-Dojave, snimanje policijskih intervencija, AVL sustav i slično. Isto tako važno je naglasiti kako anketirani policijski službenici navode i neke nedostatke uvođenja novih tehnologija, kao što su neinformiranost policijskih službenika, strahovi od zlouporabe podataka te posebnu pozornost u budućem istraživanju zaslužuju ambivalentni stavovi policijskih službenika o primjeni novih tehnologija u svakodnevnom radu policije.

Hrvatska policija nedavno je uvela nova tehnološka rješenja koja su trenutno još uvijek u fazi oglednog projekta. Bit će zanimljivo vidjeti hoće li se stavovi policijskih službenika, kako su prikazani u ovome članku, promijeniti i koliko, nakon što se nove aplikacije uvedu u sve policijske postaje u zemlji.

LITERATURA

Collier, P. M. (2006). Policing and the intelligent application of knowledge. *Public Money & Management*, 26 (2), 109-116.

Colvin, C. A., Goh, A. (2005). Validation of the technology acceptance model for police. *Journal of Criminal Justice* 33, 89-95.

Faber, V., Cajner Mraović, I. (2003). *Reforma operativno-preventivnog rada policije u odori*. Zagreb: MUP.

Flanagin, A. J. (2002). The impact of contemporary communication and information technologies on police organizations. In H. Giles (ur), *Law enforcement, communication and community*, 85-103. Philadelphia: John Benjamins.

Garland, D. (2001). *The Culture of Control: Crime and Social Order in Contemporary Society*. New York: Oxford University Press.

Gottschalk, P., & Holgersson, S. (2006). Stages of knowledge management technology in the value shop: The case of police investigation performance. *Expert Systems*, 23 (4), 183.
http://www.comm.ucsb.edu/faculty/flanagin/CV/Flanagin2002b(GilesEd.).pdf
Kelling, G., and Moore, M. (1988). *"The Evolving Strategy of Policing, Perspectives on Policing,"* U.S. Department of Justice, National Institute of Justice.
https://www.ncjrs.gov/pdffiles/crimepre.pdf
Manning, P. K. (2003). Policing contingencies. Chicago, IL: The University of Chicago Press.
MUP Baden-Württemberg, MUP RH (2013). *Priručnik za prevenciju kriminaliteta - prevencija spaja*. Sv. I. Zelina: Tiskara Zelina d.d.
Pezt, B., Kolesarić, V., Ivanec, D. (2012). *Petzova statistika*. Jastrebarsko: Naklada Slap.
Sanders, B., Hannem, S. (2012). Policing "the Risky": Technology and Surveillance in Everyday Patrol Work. *Canadian Review of Sociology/Revue canadienne de sociologie*. 49 (4): 317-451.

Ruža Karlović
Danijela Petković
Karla Kiš Kamenjarin

POLICE OFFICERS ATTITUDES TOWARDS IMPLEMENTATION OF NEW TECHNOLOGIES TO POLICE WORK

Summary

The aim was to determine attitudes of police officers regarding the introduction of new technologies in police work. Based on the opinions of police officers we get an insight into their level of awareness and the applicability of electronic communication in everyday police work, as well as their attitudes on the approval or disapproval of introducing new technologies in police work. The data analysed were collected in a survey conducted in 2015 on a convenience sample (N = 50) of police officers from different police departments in Croatia. Participants were 78% male (39) and 22% female (11) ranging in age from 28-45 years (M = 34) and in years of police service 5-26 (M = 14). Police officers expressed their views on new technologies providing answers according to the Likert scale from 1 (strongly agree) to 5 (strongly disagree). It is important to note that this is only a preliminary study whose results suggest that in the future we should examine attitudes of police officers, as well as end users of new technologies, but also monitor the effectiveness of police officers in their daily work. This study showed that the majority of respondents approve of the introduction of new technologies in day to day police work and that respondents have a positive view on the role of new ICT tools such as eDojave (e-Reporting), recording of police interventions, AVL system etc. in strengthening the relations between the police, citizens and other social actors. However, in a future research, special attention is to be given to ambivalent attitudes of police officers on the application of new technologies in everyday police work.

Key words: *attitudes, police officers, electronic communication, citizens, police work.*

REVIEW PAPER

Marina Malish Sazdovska[240]

APPLICATION OF NEW SOFTWARE SOLUTIONS IN CRIMINAL INVESTIGATIONS SUMMARY

Summary

New technologies are a benefit used in various domains of social life. They are widely used within the criminal investigations. There are new and more sophisticated methods applicable worldwide at various stages of criminal investigations. The question is how these methods serve as a part of the daily work of the police forces in the region.
The author of the paper addresses several software solutions and the development of special computer programs used in the detection of crimes as well as the collecting of information needed for the clarification of certain criminal events. The paper makes special reference to the computer program used for crime mapping in the Republic of Macedonia.

Key words: *new technologies, crime detection, investigation, crime mapping.*

1. INTRODUCTION

The scope of work of authorities responsible for detection of crimes necessitates application of adequate measures and activities by the authorized officials. These measures and actions are part of the police toolkit, which consists of operational and tactical measures as well as investigative actions. In addition to these measures, and quite often, special investigative measures are applied in the cases of organized crime. This is in order to gather evidence of the suspects' criminal behavior when such could not be obtained by other means (Malish Sazdovska, 2005). These measures are integral part of the law enforcement tactics that encompasses all measures and activities needed to find out about the existence of a crime, the evidence and to clarify it. There are special criminalistics methods for each type of crime. They make a set of measures and activities aimed at discovering only one type of crime and combat successfully the crime (Angeleski, 2007).

However, development of new sophisticated ways of committing crimes by offenders and organized criminal groups, which use modern technical equipment and facilities, necessitates modernization of criminalistics tools and methods for its detection. Namely, there are numerous ways to use computers, satellite systems, software solutions and other systems to commit modern crimes in the domain of the cyber crime, money laundering, forgery and others.

[240] PhD Marina Malish Sazdovska, Associate Professor, Faculty of Security-Skopje, e-mail: mmsazdovska@gmail.com

This has been a challenge for the law enforcement authorities in order to find adequate modern technical and software solutions which are on par with the perpetrators and if possible to reduce this kind of crime, as well as to work on its suppression in the future.

2. NEW TECHNOLOGIES FOR DETECTION OF CRIME

Various methods and techniques can be used within the scope of the criminalistics analysis. Such are: statistical analysis of crime; analysis of patterns of crime to identify the criminal hotspots (mostly related to the use of geographic information system - GIS); network analysis (tactical analysis); analysis of telephone contacts (by using sophisticated software such as the Analytical program I2 or Watson); analysis of financial transactions; analysis of time series; analysis of criminal markets; risk analysis and many other (Stefanovska & Gogov, 2015).

Also, of particular importance in these and other methods is the use of Geographic Information System (GIS) in creating, maintenance and storage of digital geographic data with computer equipment (hardware and software) enabling processing, analysis and visualization of geographic and tabular data (Stefanovska, Gogov, 2015).

Application of GIS systems for combating crime is related to police actions and improvement of police work. To be more specific, certain legal solutions in Serbia treat the electronic devices for locating and tracking the results of their application as evidence in criminal proceedings. Moreover, special investigative measures: controlled delivery and locating and tracking people geospatially are evidence related techniques realized by use of modern electronic devices for global positioning, i.e. devices for automatic tracking of persons and objects. They can be used to find stolen vehicles by locating the position of the vehicle, with precision of 2 to 5 meters (MilojkovIc & Marinkovic, 2007).

Modern software solutions can be also used to manage major accidents caused while transporting dangerous goods. Namely, incidents can happen when hazardous materials are transported. Thus, in order to select the optimal routes for transportation of dangerous goods and implement preventive measures to minimize the risk, some forms of simulation can be exercised. Numerous models for selection of optimal routes can be used. Such is the Geographic Information System (GIS) to address the problem of routing and accurate prediction of the spatial consequences from disposal of hazardous substances. In addition, “Kovers” project which performs Multifactor optimization of the transport of dangerous goods can also be used, as well as the software for managing and planning routes CAMEO (Computer-aided Management of Emergency Operations) comprised of two modules: dispersion of toxic gases ALLOHA and program for electronic cartographic support MARPLOT (Ristic, Indjic & Karkalic, 2014).

Other effective tools besides the GIS systems to detect certain crimes, especially theft are also the alarm systems. To be more specific, alarms fitted to certain facilities, vehicles and so on are the electronic devices signaling at the moment of a break in, a sign for a police or private security agencies action. In this way, the use of alarm systems helps in the actions to detect perpetrators of crimes. Hence, thefts in apartments, vehicles, industrial equipment and any other place, which is protected with an alarm device, can be easily exposed.

Drones are also the new effective technology solutions, which are enabling intelligence gathering (www.bbc.com). Namely, during wartime, they provide intelligence by gathering information about certain actions of the opponent and the current situation on the ground at the war hot spots under control of insurgents and terrorists (www.telegram.hr). Examples of warfare when drones are used are pointed out because in such cases the risk of casualties is excluded due to the unmanned bombers that can be controlled from a secure location, which is several miles away. Establishment of the first drone squadron "Grenada" serving for terrain reconnaissance is also pointed out (www. infomax.mk). In addition to the security authorities that use drones for intelligence gathering, individual criminals and terrorists as well as similar organizations can also use drones for their activities. For example, when searching for the terrorists in Paris and gathering information about their communication it was concluded that there was a threat of a drone - bomb to be used. This possibility was related to the port area in Marseille-Fos, and data were obtained by the method of prediction analysis, based on the data from the intercepted conversations of people who were monitored and tapped (www.sitel.com).

Other experts who are warning about the criminal use of drones confirm this. The research, led by Sir David Omand, a former head of the UK's intelligence centre, GCHQ, highlighted the risk of the devices used in terrorist attack. They believe the crowds at sporting events or rallies could be vulnerable in a similar way if a future terrorist group were to look for means of dispersing chemical or biological agents (www.bbc.com).

Drones can also be used for committing crimes or gathering information about specific objects and people in order to create conditions for theft. Namely, drones are highly-maneuverable and - depending on the model - can carry advanced, high definition cameras which can capture video and still images. The technology allows thieves to explore properties from the air and will be used to identify security weak spots, such as older-style patio or French doors, which can be easily forced. Police have confirmed that unmanned drones are being piloted over private homes by burglars in a bid to identify potential targets (www.telegraph.co.uk).

3. NEW TECHNOLOGIES FOR DETECTION OF CRIME IN MACEDONIA

State authorities responsible for detection and suppression of crime in the Republic of Macedonia have realized the need for application of new modern solutions for actions against contemporary forms of crime. Mostly it is about using modern software solutions for data processing, filtering and their use to suppress certain kinds of crime.

Financial Intelligence Directorate considers introducing powerful software system in its work. It should provide data for each reported or suspected person or data collection, automatic processing, case analysis and would generate reports. The system would have extensive and accurate database pertinent to dealing with this type of crime. In addition, it would have a module for visual data analysis. The system should more effectively coordinate the activities of the competent authorities for combating crime: Ministry of Interior, Public Prosecutor, the Financial Intelligence Directorate, the Financial Police, the Customs Administration and the Public Revenue Office,. By it, these authorities would be connected

for communication, which is targeted to data and information exchange as well as effective suppression of financial crime. A special feature would also be the module, which is generating final intelligence reports in the domain of financial intelligence that would be further sent to the competent authorities that are combating the crime (www.ufr.gov.mk).

In this way, a full system is introduced in all phases and steps of the process of possible unlawful conduct as well as a system to combat effectively the crime. A system that is set in such a manner would minimize the possibility of money laundering and financing terrorism. In addition, it is planned to use an interactive web application through which banks, lawyers, savings houses, bailiffs, notaries and other entities under the Law would submit data, and request examination of suspects and potentially dangerous persons intending to carry out financial crime. In addition, within the system a module for automatic generation and sending data or requests for further information to banks would also be installed (www.ufr.gov.mk).

Financial Intelligence Directorate in the Republic of Macedonia uses modern software applications for its analysis such as:

- Suscriptor (software for keeping electronic archive)
- DocuShare - Document Management System (software for managing documents)
- ICM - Investigation Case Management (Application for data processing and electronic case management)
- I2 -Analyst Notebook (software for automatic creation of graphic patterns of cases)
- Business Intelligence (software to create reports from data in the database)
- SPSS (software for statistical analysis of data from the database).
- These tools are very useful for the operational functioning of the Directorate, having regard to the fact that during one calendar year, they receive 200 reports about suspicious activities of the entities.

Certain software solutions that have been used like the one for analysis of data on accidents in the country play a significant role to predict the crime. To be exact, based on the entered data for a number of years, the software calculates and predicts the trends in the next 6 years (Babanoski, 2014) (Figure 1). As the most appropriate software package for this purpose from the multitude of computer software tools for predicting future events based on previously observed sets of data is GMDH Shell DS 3.5.2. It is software for predicting time series, which is developed by the research, group GEOS and is based on proven classic GMDH algorithm, by using heavily modified and improved version. GMDH Shell is software for predicting time series designed to solve tasks of modeling, simulation and predicting (Babanoski, 2014).

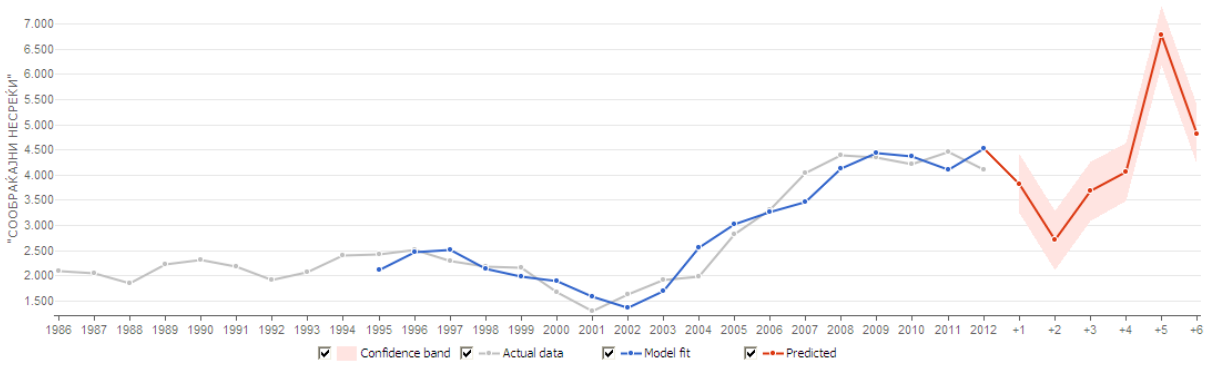


Figure 1: Predicting the timing of traffic accidents in the Republic of Macedonia for the period 2013-2018 (Babanoski, 2014)

Another feature is prediction for shorter intervals. Such example is prediction of the timing of traffic accidents in the country in the years 2013 and 2014 by months. In order to build its own model of prediction, the software took into account the last 3 years and gave the best possible accurate prediction for the year of 2013 and the year of 2014. The situation is such that significant changes and variations in the predicted years related to the last five monitored years are not expected, which means that in future, the seasonal schedule of accidents will not be changed. (Figure 2).

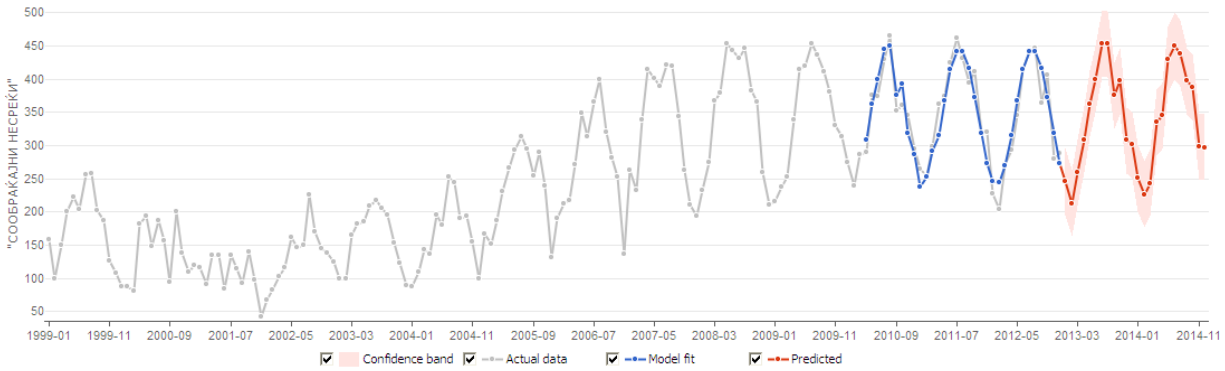


Figure 2. Predicted timing of traffic accidents in Macedonia in 2013 and 2014 by months (Babanoski, 2014)

This software could provide information even for the predicted traffic accidents by days or hours, based on the already entered data on the traffic accidents in the previous multi-year period. However, it should be mentioned that these solutions are not used within the framework of police work but only for research purposes.

The auditors when performing audits can also use modern software solutions. Namely, today's business is characterized with telecommunication data transfer. Therefore, in order to detect fraud in such case computer assisted audit techniques are applied. They are applied for obtaining and evaluating evidence related to reports on economic developments and operations in order to verify the extent of correspondence between existing operational reports

and predetermined criteria and the communication of results to the interested parties. Therefore, auditors should have adequate knowledge of information technology and its proper application in practice. In order to facilitate the implementation of the audit procedure in modern information environment, auditors are increasingly using computer-assisted audit techniques (Stojanova & Blazeska, 2013).

One of the best tools and techniques to reduce the risk and threats is the computer technology. Technology is often used to protect and defend computers and financial resources from damage of any kind, including fraud. These include computer techniques such as computer assisted audit techniques - CAATs, which enable efficient automated data review. In fact, they are directed to the likely risks to transactions and data, and are part of the audit strategy.

The advantages of using these programs are: auditors can test program controls and general internal controls related to computers; auditors can faster and accurately test a larger number of points than they can otherwise; auditors to test transaction instead of printed records of transactions that could be misleading; programs are cost effective in the long run, if the client does not change its systems; results can be compared with the results of the traditional test - if the results match, then it increases the overall reliability (Stojanova & Blazeska, 2013).

Audit software performs such data controls that otherwise the auditor should have conducted manually. By using these software auditors could carry out tests on computer files and databases, such as reading and extracting data from the systems of the client for further testing, selecting information, making arithmetic calculations, ease of selecting sample and creating data files.

Examples of such software are ACT and IDEA. Other examples of audit software to be mentioned are: verification software that accesses the data files of the client; programs for comparison that enable comparison of the versions of one program; interactive software for testing of online systems and integrated software for checking transactions in their processing.

By applying these software solutions, a quick analysis of the data is performed by the auditors and certain patterns are revealed. Because of it, the fraud is detected.

4. CRIME MAPPING

One of the ways for applying new technologies for crime investigation is also the crime mapping. There are different ways of crime mapping, which are used in the daily police work and the work of other law enforcement agencies. One of the ways is the use of Geographic Information Systems (GIS) as a method of crime analysis. It is a relatively new analytical method, where geographical maps present an integral part of the crime analysis. The geographical maps, showing the distribution of crime in a given environment, are an integral part of crime analysis, which plays an extremely important role in the crime management (Eman, Gyorkos, Lukman & Mesko, 2013).

Crime mapping is used for forensic analysis of the crime that happens in a certain area. Namely, by creating maps an accurate picture of crime hot spots where specific criminal activities occur is developed. In addition to its official purposes, the public could also use this method. For example, the website of Los Angeles Police Department enables access to

persons who are not authorized officials in order to get up-to-date crime statistics for the neighborhoods throughout Los Angeles. In such way, the users of the maps are informed about the crime in the community, as the first step for preventing future occurrences of the crime in the community (www.lapdonline.org). Thus, citizens can obtain information related to crime maps for the following crimes: homicide, rape, burglary, aggravated assault, robbery, burglary/ theft from vehicle, personal/other theft and auto theft.

Image 1: Crime Mapping in Los Angeles (www.lapdonline.org)

Based on the crime mapping additional analyzes of the crime are possible to be performed. In addition, the trends could also be determined. Therefore, London police (as well as other modern police) has a special section on the official web site. Metropolitan Police Service Crime Mapping Website provides data for crime types, police station locations and comparison of crime levels in a specific borough. This site has been created to help show us what crime has been committed in neighborhoods across the capital. Crime information can be shown on a map shaded to show crime rates in each area compared to the average across London.

By analyzing the data from the web site, a monthly comparative analysis can be produced (Figure 2), but also the annual trends (Figure 3) (www.maps.met.police.uk).

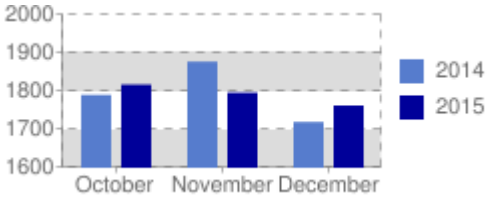


Image 2: Monthly trends (www.maps.met.police.uk, 2015)

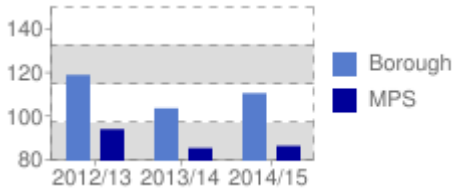


Image 3. Annual trends (www.maps.met.police.uk, 2015)

The website also provides information about certain types of crime for a certain period of time and the number of crimes well as the crime rate in the given area. Therefore, the site for the month of December 2015, in Shepherd, s Bush Green provides the data given below.

Table 1: Statistics for December in the area Shepherd's Bush GreenT (www.maps.met.police.uk, 2015)

Crime type	Crime count	Crime rate
Total notifiable offences	302	24.80
Residential burglary	13	1.07
Burglary other	3	0.25
Theft of motor vehicle	6	0.49
Theft from motor vehicle	4	0.33
Robbery business	1	0.08
Robbery personal	4	0.33
Violence against the person	88	7.23
Most serious violence	15	1.23
Anti-social behavior	75	6.16

The website also displays the location in London (www. maps.met.police.uk).

Image 4: Area for which data on crime is provided (www. maps.met.police.uk)

Data provided by mapping give opportunities for multiple actions against the crimes to be taken. Additional feature for the use of data for crimes' analysis and defining the crime rates in certain areas is that the criminogenic hot spots in a particular territory are determined with grater precision. Therefore, the new technologies are used as an integral part and are important tool for criminalistics analysis, which is performed by the police and other security services in a country. More exactly, these data are very useful for further planning of the actions of the authorities to combat crime, but also for strategic planning of future measures and activities in a certain area. Given the need for strategic, tactical and operational planning for the suppression of certain types of crime, the authorities need to implement fully crime mapping to successfully plan at all levels, but also to conduct effective actions in the field (Malish Sazdovska & Dujovski, 2009).

In addition to the use of crime maps to improve the work of the police, application of this method is also a positive feature because the citizens and the public have free access to

information on crime and crime rates in a certain area. This is useful for citizens in order to create a sense of security in a particular territory, by considering the location and the kind of crime. This refers to the immediate environment where they live and the city in general. In this way, conditions are created to apply the concept of community policing which is a situation when the police and citizens share information about criminal events and collaborate to combat the crime in a certain area.

For efficient use of information technology and in order to suppress a certain type of crime that in this case is the cybercrime, Microsoft has announced the opening of MCC (Microsoft Cybercrime Center), which will lead the global fight against Internet crime (www.smartportal.mk). The center will combine the legal and technical expertise of Microsoft with the most advanced tools and technologies to combat this type of crime. Cybercrime has been hurting millions of users worldwide. The Microsoft Center for Combating Cybercrime would deal with these criminal activities, including those related to malware, theft of intellectual property, exploitation of minors via the Internet and the like. In this way, the work of the center would help to protect people around the world and they would use their computers and internet services with confidence. The Centre for Cybercrime is located within the Microsoft campus located in Redmond, Washington. The facility features cutting-edge technologies that enable identification of global Internet threats. SitePrint technology enables online mapping of the networks of organized crime, while PhotoDNA is one of the leading technologies to combat Internet child pornography. Cyberforensics technology offers advanced features to detect global Internet crime including online fraud and identity theft (www. smartportal.mk).

The police work involves analyzes of a range of collected information. This information should be examined, systematized, classified and analyzed. Without adequate analysis, such data can be useless. By analyzing data, the result called *analytical information* became achieved. It is the most important factor for decision-making and effective police action. To accomplish that, analytics and modern methods and techniques are used. The method of computer mapping is very important because the geographical components of crime and other security events are also very important. Namely, almost all police work is related to some position, address or location. Each call for police intervention has certain geographic qualifier i.e. crime happens at a certain place in the geographical space. Therefore, in order to improve the police activity to combat crime it is important to connect the locations with the people and the events by using information technology (Tadic, 2009)

4.1. New technologies for crime mapping in Macedonia

Criminalistics mapping is use of the spatial analysis within the criminal analysis. Criminal analyst must have knowledge of maps and mapping, and basic understanding of techniques that enable visualization and understanding of police data. One of the most popular techniques in criminalistics mapping is converting tabular data into mapped data: matching of an address. This is the method of designating spatial locations with events or geo-coding or matching of an address in order to record certain events. At the same time, general maps, diagrams and thematic maps are developed (Brus, Hic & Kuper, 2009).

The mapping and descriptive labeling of crime can be carried out by recording the following: with one symbol; buffer zones; progressive mapping; graphical mapping and interactive mapping of crime. Also, raster data representing a grouping of coordinated network or screen dots (pixels) that are covered on the surface and designated with attribute data (mostly numeric value) are used. Raster files are commonly used to store satellite images and remote surveys and are usually presented in color (Boba, 2010).

In order to apply such and similar methods for crime mapping, some efforts are made in Macedonia too. Namely, the website of the Ministry of Interior (unlike other worldwide modern police) contains neither data nor there is software to map the crime in the country.

Still, in Macedonia there is a system, which is used for crime mapping. More precisely, it is a system consisting of two parts: analysis of events and filling the database and display of the data from the database on a map. The event data is read automatically from the website of Ministry of Interior from the daily e-newsletter and it is released in unstructured form and in natural language. The first part of the system analyzes each event and records it in a structured form in a database. However, due to the poor way of publishing bulletins, some events can be missed and the location of the event may not be the location of the event, but the name of street, which is published in the newsletter. This system in its database has information on the location and the type of event. The entire database can be downloaded from the website and freely used. The second part of the system displays the events on a map, which can be viewed as a map with signs or a heat map. The initial display shows the events of the last 30 days. One of the features of the system is that the events could be seen or could be filtered on various grounds, such as city, type of event, etc. (www crimemap.finki.ukim.mk).

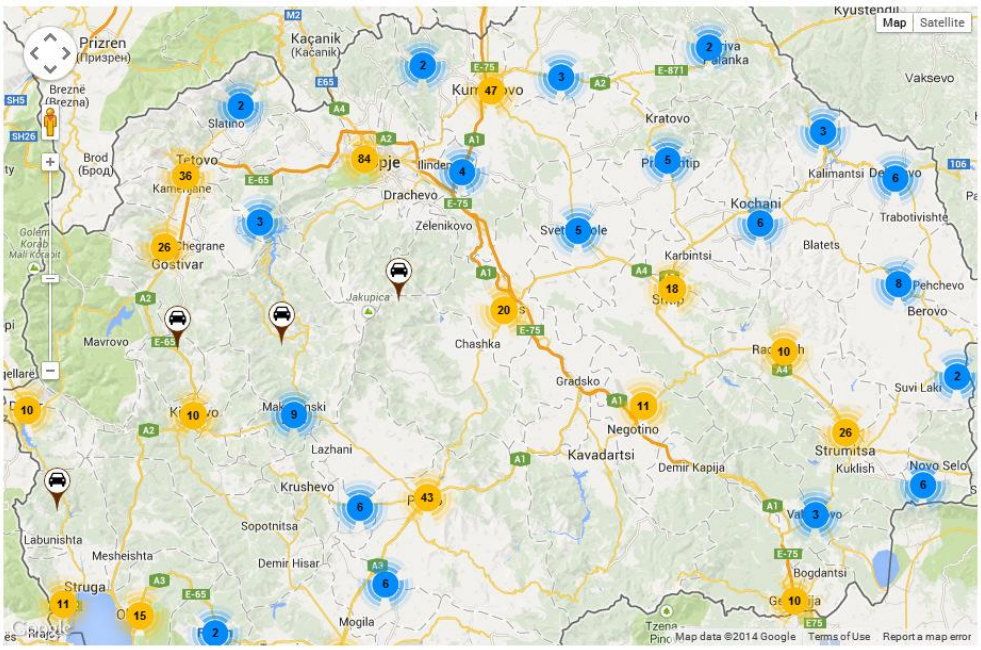


Image 5: Map of the Republic of Macedonia listing the accidents (www crimemap.finki.ukim.mk)

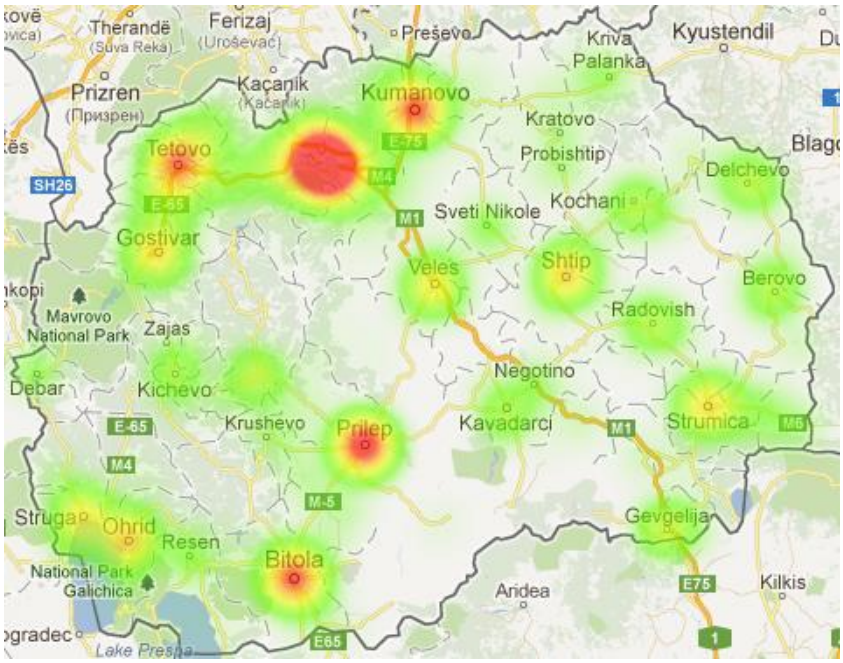


Image 6: Heat Map of the Republic of Macedonia (www crimemap.finki.ukim.mk)

This system is based on the use of available data on certain events and this website is the first to have an interactive map of the crime in the country. The system reads the data on the events from the daily electronic newsletter published on the official website of the Ministry of Interior, and then performs analysis and coding on the map from Google Maps. The events can be filtered by city, type of event, date of event, day of the week when they have occurred, and subsets of these parameters could be made. Although this system is not a fully complete map of crime in the country, it still shows valuable statistical information that could be used for analysis of criminal patterns. It could also be a preventive tool for reducing and combating of crime in the country. This system uses free data (open data), but it is data from officially confirmed data taken from the web site of the Ministry. This system of crime mapping is a result of an inspiration by several other similar projects in other countries in the world, most notably: Police.uk, CrimeMapping.com, PolicyMap.

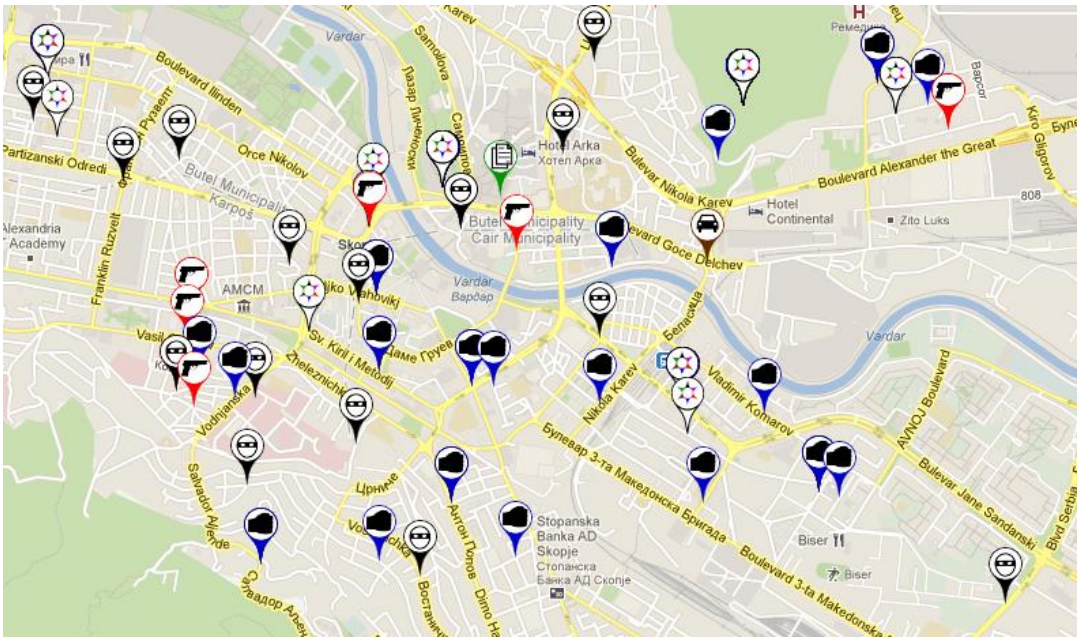


Image 7. Crime Mapping in Skopje (www crimemap.finki.ukim.mk)

Image 8. Crime Mapping in Skopje (www crimemap.finki.ukim.mk)

There is another system for crime mapping in the country, but it refers to the city of Skopje, and uses information obtained from the population (crowdsourcing). This system aims to collect a range of data on harassment and violence faced by women in public places in Skopje. These events are often not reported and are not registered. This website enables reporting of any harassment on the street, a park, a bus or any other public location or just information about occurred recent incidents and safety of public places and paths. These data refer to all types of violence from whistling, vulgar comments to touching, following someone, sexual assault or harassment and insults that are a daily reality for women but are rarely reported. In this way, a social network dedicated to the prevention and eradication of gender-based harassment in public places is created (www.reagiraj-bidibezbedna.mk).

In this way, data are collected and are presented later in a form of statistics, news, maps of reported events, diagrams etc. To analyze the data it is possible to filter it on different grounds. The website displays accounts of events with the description, the location, the date, and there is an explanation of the manner of how to report events.

It could be said that the Open Data initiative is starting to develop in Macedonia, but there is much more room for improvement and at least the computer science community wants to see it happening. In addition, crime mapping is a very useful tool in crime analysis and in fighting crime, but these maps can also be connected and overlaid with open data from education, income salaries, etc., in order to pinpoint the major cause for high percentage of crime in some regions. Another benefit is that the citizens can take into consideration the crime percentage of the region where they plan to buy their future home, where their children will go to school, or where their work is situated (Temelkovski, Jovanovic, Mishkovski & Trajanov, 2012).

5. CONCLUSION

This paper cited a number of new technological solutions that improve the work of the police and other security authorities. In fact, several software tools enable crime mapping, as well as criminalistics analysis and defining the trends of crime by which criminalistics could make the predictions. There are also numerous technical assets, equipment and instruments which are used for gathering intelligence, and surveillance of persons, events and conditions. In this way, an effective police action aimed at preventing certain criminal activities is enabled. In addition, there is also quick and timely detection of already committed crimes. This is especially important for the sophisticated ways of committing crimes, which require application of new technological solutions to detect the perpetrators of the acts.

The overall conclusion is that unlike the modern police forces worldwide, Macedonian police does not apply these new methods within its daily operations. Entire technological advancement of certain processes and application of new technological equipment for effective action on the ground is needed. It is unacceptable that the methods which have a decade long history of use abroad, while in the country, the need for their application is not considered yet. Processing of these methods is applied only for scientific purposes, teaching at the higher-level institutions, or only because of enthusiasts who are not directly involved in the security sector.

REFERENCES

Angeleski, M. (2007). *Kriminalisticka taktika 2.* Grafos, Kumanovo.
Babanoski, K. (2014). *Bezbednost I odgovornost na ucesnicite na patniot soobrakaj vo Republika Makedonija.* Doktorska disertacija. Skopje: Fakultet za bezbednost,
Boba, R. (2010). *Kriminalisticko istrazuvanje, mapiranje na kriminalot.* Skopje: Nampres.
Bruce, C., Cooper, J., Hick, S. (2008). *Exploring Crime Analysis*. Overland Park, KS: IACA.
Eman, K., Györkös J., Lukman, K., Meško. G. (2013). Crime Mapping for the Purpose of Policing in Slovenia - Recent Developments. *Revija za kriminalistiko in kriminologijo,* 64(3), 287-308.
Malis Sazdovska, M., Dujovski, N., (2009). *Bezbednosen menadjment.* Skopje: Fakultet za bezbednost.

Malis Sazdovska, M. (2013). *Priracnik za istragi kaj ekoloski krivicni dela.* Skopje: Fakultet za bezbednost.
Malis Sazdovska, M. (2005). *Priracnik za razuznavacki ciklus.* Skopje: Jofisken.
Milojkovic, B., Marinkovic, D. (2007). *Sistemi za globalno pozicioniranje i njihov znacaj u otktrivanju i dokazivanju krivicnih dela.* Beograd: NBP Nauka, Bezbednost, Policija, Kriminalisticko policijska akademija Beograd.
Ristic, S., Indjic, K., Karkalic, R. (2014). Primena savremenih softverskih resenja u procesu upravljanja hemijskim akcidentima izazvanih transportom opasnih materija. *Vojno delo*, 3, 160-184.
Stefanovska, V., Gogov, B. (2015). *Ulogata na zaednicata i na policijata vo prevencija na kriminalitetot: sostojbi vo gradot Skopje.* Istrazivacki izvestaj. Skopje: Fakultet za bezbednost.
Stojanova, P., Blazeska, D. (2013). *Primenata na kompjuterski potpomognati revizorski tehniki vo revizijata na izmami kako prodobivka od razvojot na informaciskata tehnologija.* Prva megunarodna naucna konferencija. Skopje: Univerzitet Evro Balkan.
Tadić, N. (2009). Kompjutersko mapiranje bezbjednosnih događaja u fumkciji veće efikasnosti policije. *Policijski glasnik*, 5(2), 16-17.
Temelkovski, D., Jovanovik, M., Mishkovski, I., Trajanov D. (2012). *Towards open data in Macedonia: crime map based on Ministry of internal affairs' bulletins.* The 9th Conference for Informatics and Information Technology (CIIT)

Internet sources

http://smartportal.mk/internet/microsoft-otvori-centar-za-borba-protiv-internet-kriminalot/
http://www.lapdonline.org/crime_mapping_and_compstat
http://www.lapdonline.org/crime_mapping_and_compstat
http://maps.met.police.uk/
www.ufr.gov.mk
http://www.bbc.com/news/uk-29717771
http://www.telegram.hr/politika-kriminal/snimka-iz-drona-prikazuje-potpuno-razoreni-sirijski-grad-homs/
http://infomax.mk/wp/?p=19562
http://sitel.com.mk/identifikuvani-mozhni-celi-na-teroristite-vo-francija
http://www.bbc.com/news/uk-29717771
http://www.telegraph.co.uk/news/uknews/crime/11613568/Burglars-use-drone-helicopters-to-identify-targe-homes.html
https://www.reagiraj-bidibezbedna.mk/main
http://crimemap.finki.ukim.mk/home/mk

REVIEW PAPER

Robert Eberherr[241]

E-LEARNING IN THE BAVARIAN POLICE - THE PERSPECTIVE OF FURTHER EDUCATION

Summary

Since 2001, the Bavarian Police have tried out new ways of learning. During the years, the Bavarian Police have had to deal with an increasing number of students included into further education programme. Considering this, the police were forced to come up with new ways of conveying all the topics of further education to every single officer. Presence education is a direct way to teach important issues, but its feasibility is not without restrictions, bearing in mind a larger number of officers. It turned out that it was necessary to introduce the e-learning system into the further education programme. The Bavarian Police opted for blended-learning. By the use of the e-learning programmes in combination with the presence education, each officer is going to become prepared for his/her demanding and versatile job. The basics are going to be conveyed via the e-learning, whereas specialized knowledge would be taught by teachers in the institute of further education. Since the introduction of the e-earning system, the requirements of learning processes have been increasing. Moreover, every student also needs to experience some achievements, so the check-ups for courses intended for the preparation for seminars have been introduced additionally. Experimenting with new ways of learning is deemed very important so that the police actually work with podcasts and in virtual classrooms that offer different types of students' multifunctional methods to prepare themselves for their everyday worklife.

Key words: *LP-Po, ILIAS, operating agreement, blended learning*

1. HISTORY OF E-LEARNING IN THE BAVARIAN POLICE

The first programs (from the 70s) started without a didactic or methodical structure, guiding the user through the program without any possibility to influence it (Wendt, 2003). In 2001, the first learning programs were used as CBTs.[242] During the years the programs have gotten more interactive. The importance lies in the intention of the product. Of course, there could be a program for every topic, but essential is the competence, which should be amplified.
First plans for a new program with the topic laser speed control instruments started in 2002. For this programing instructions for a Learning Management System (LMS) were developed as well as a concept, including a didactic model, for the tutorial laser velocimetry. This program is still in use, of course with updates and annual controls on the timeliness of the contents. This monitoring lies on the shoulders of the teacher for the respective topic, who

[241] PHK Robert Eberherr, Fortbildungsinstitut der Bayerischen Polizei, Ainring e-mail: robert.eberherr@polizei.bayern.de
[242] CBT: computer based training, first programs were published in the middle of the 70s.

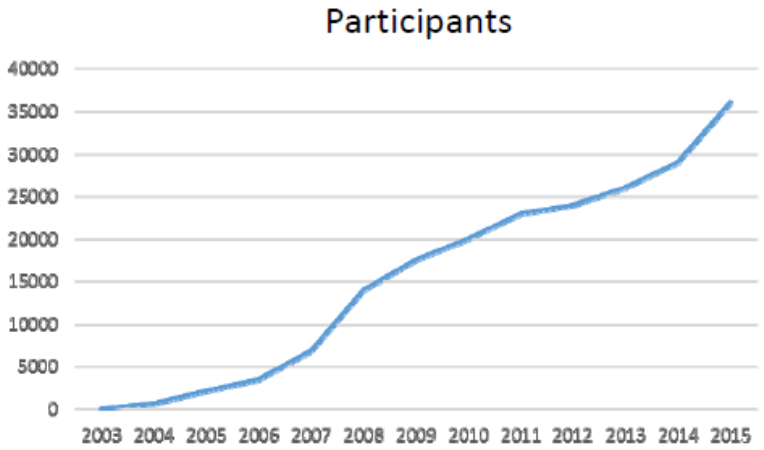
works at the institute of further education. He is also the contact person for questions on the matter.

The demand for e-learning programs has increased and the Bavarian Police decided to introduce a learning platform (LP-Pol[243]). At the beginning, it was accessible for a limited group of users, who tested the platform online. One year later, the LP-Pol was generally approved for training in order of the Ministry of the Interior and the employee committee.

In 2011 the e-learning course for digital radio was published and is also an example for the cooperation of different institutions in Germany. The program was developed by the federal state of Baden-Württemberg and given to the Bavarian Police. Every officer in the field needs to know how to use the digital radio. So the count of users has risen and a migration to a new learning platform was necessary. ILIAS was chosen as replacement system. In 2013 it was introduced and is still in use. Over the years the team of e-learning has grown and tested new authoring tools. At the moment IDEA7 Professionell, Articulate Storyline2 and ILIAS software are in use to establish learning programs. To be up to date, a weekly data synchronizing process from the employee's database is performed. A new high-performance server architecture ensures a smooth implementation.

Counted at 2015, there are more than 36.000 active users on the platform. This year, 2016, 38,000 users were counted, which means that about 90% of all employees of the Bavarian Police are active on the platform.

The graph below shows the increase of user numbers since 2003.



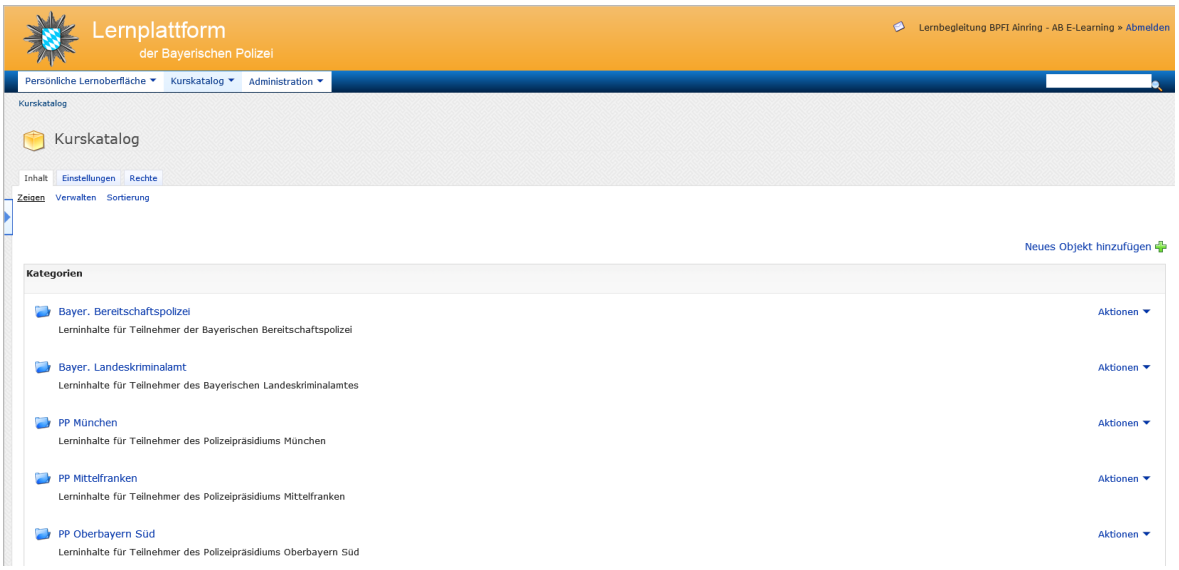
Graph 1: Development of the number of the participants in e-learning

Latest data is from 2015 (Graph 1). However, it is clear that the number of participants rises continuously. All of the 36.000 registrated users successfully completed at least one course. At peak times there are more than 300 participants with simultaneous access.

After working through a program, every user receives a test certificate or a certificate of attendance automated via e-mail and it is also automatically listed in the electronic personal file of every user.

[243] LMS of the Bavarian Police called „Lernplattform der Bayerischen Polizei“ shortened LP-Pol

The platform is structured into different Bavarian-wide categories (Graph 2). The administrative rights belong to the BPFI Ainring, the institute of further education. Every category includes courses that are used across Bavaria and are necessary for the daily work, for example Windows 8.1 or Office 2013.
Every regional Police headquarter has its own area with own groups. Administrative rights and the view on their users are given to them. Different ways to acquire knowledge is offered, for example, knowledge base, additional information or wikis. To contact other users or to ask question on a topic, there is the possibility to use asynchrony communication such as forum or platform-mail.
Depending on the position of an officer, she/he is able to choose her/his programs. There are programs which every user has to work through, no matter her/his position, for example, some modules concerning cybercrime. After that, every user decides on further modules that are fitting to her/his sector of work. Investigators in the sector of sexual crime need to work through this learning program. They receive basic knowledge and then they have to successfully complete a test, before they come to the institute of further education to deepen their knowledge on that topic in cooperation with the local teacher. The basis for this seminar is the processing of the basic module and the passed test. The structure of the platform (homepage) is presented on the Graph 2.



Graph 2: The homepage of the platform for e-learning

Overall, 27 products (contents) of the e-learning can be used on this platform. The offered products are shown in the Table 1.

Table 1: Offered products of e-learning for Bavarian police

Title	Modules
Laser speed control Instruments	**8**
Exam Laser speed control Instrument	**1**
Cybercrime: • **New Media** • **Social networks**	 **8** **5**
First verification (tracing) of sexual crime	**2**
Fundamentals on transporting dangerous good	**2**
First aid in forensic technology laboratories	**1**

In 2016, the institute is planning to compile programs for digital photography, preparation for the police boatmasters certificate and IT Security training. EPSweb, an operation reporting system, is still in the process of finalizing. For the first time, the team is working with screen recordings to establish the program in cooperation with the subject matter expert (specialized teacher).
Of course, there are external developments in use, as is pictured in the Table 2.

Table 2: External developments of the e-learning for Bavarian police

Title	Modules
Corruption prevention	2
Windows migration: • Windows 8.1 • Office 2013	 2 7
Digital radio	2
Public service law	5
Digital tachograph	1
Document search (manhut): • Document check • Falsification of documents	 1 1

2. FRAME CONDITIONS AND RULES OF ACTION

The operating agreement defines that electronically information- and communication technology should be used in all three phases of learning, preparation and post processing. e-learning and presence education should be combined in blended learning. It is also determined to save the data of each user as well as give the requirements to use the platform in the right manner. Everyone should have two hours without disturbance per day while working through a program. Every user is asked to take a break after 20 minutes of learning. To make sure that all these requirements lead to success, it is reasonable to arrange special rooms and workplaces with computers. Headphones are going to ensure that the user learns on every possible channel. Some courses work with voluntary tests to check their knowledge after doing the basic module. But there are also compulsory tests when the user is going to take part in a presence seminar.

Supervision is central in Ainring. Four colleagues work on programs, answer questions of users and they care for the timeliness of the contents. Together they ensure that every user gets help to work through the program successfully. Some programs postulate supervision, but in a decentral manner. Every regional headquarter is able to appoint administrators, tutors and, of course, multiplicators. Especially Laser is conveyed by multiplicators, who have the ability to lead/guide through the examination.

3. BLENDED LEARNING

3.1. Definition

The Bavarian Police mostly uses blended-learning-concepts, a combination of e-learning courses and classroom trainings at the institute of further education. Advantages of e-learning are versatile. It is easy to integrate learning into the daily workflow without leaving work for a central presence education. Furthermore, it does not depend on a time or place. Every user is able to learn the contents in her/his time via mobile client or at the computer. The key is that the program fits to the purpose of the topic and is addressed to each learner type (Sauter/Sauter, 2002).

Learning processes are individual and they depend on the user. When talking about e-learning, the activity-oriented approach is in the focus. But as previously mentioned, e-learning with presence education is the better way to pass on knowledge to learners. Web-based trainings in combination with classroom training show a much higher success of learning.

Three learner types are known when it comes to e-learning (Sauter/Sauter, 2002):

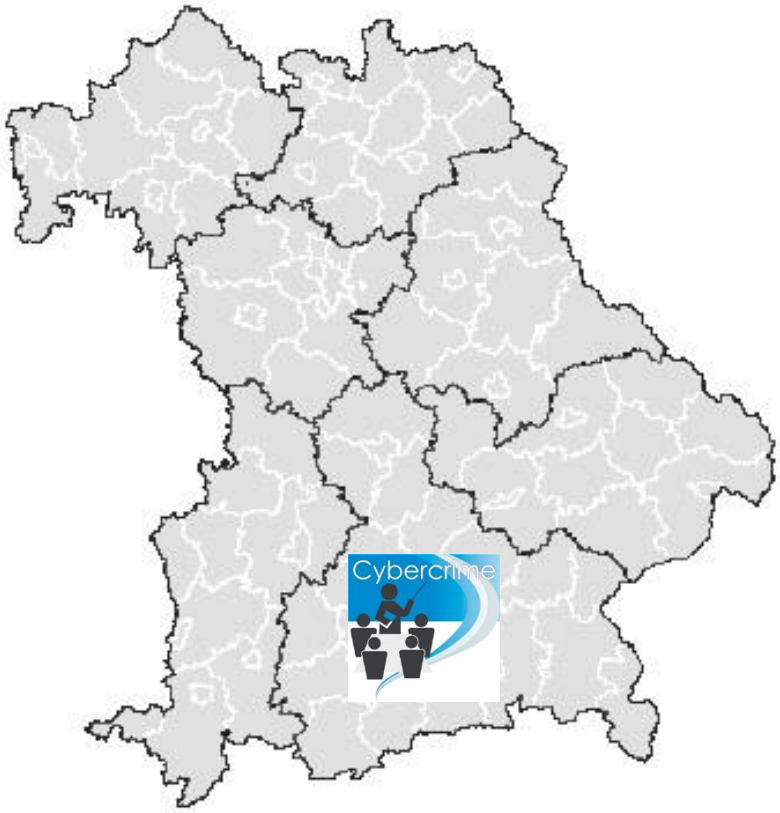
Explorative:

The audience consists of the informed learner with high competences. The procedural method shows a case to the scholar, maybe with some further information, but then the user has to work through the problem on her/his own. She/he is responsible for the solutions. Aim of this way is to discuss the results and to design a prototype. In this case, e-learning gives necessary information and material.

Inductive:
Scholars with background on the topic are the audience. While working with different cases on the topic, the user develops rules for this procedure. Aim is to establish rules, which can be used in such cases. eLearning in this way of learning presents the cases und the analytic methods.

Deductive:
The audience has a general education but no specialized knowledge on the topic. The scholar developes the base, rules and questions to get the solution for a case. Aim is to learn different strategies for the solution of a problem. Therefore, the program gives basic knowledge and shows different approaches.
One successful example for blended learning is the topic of cybercrime.

3.2. Implementation: cybercrime

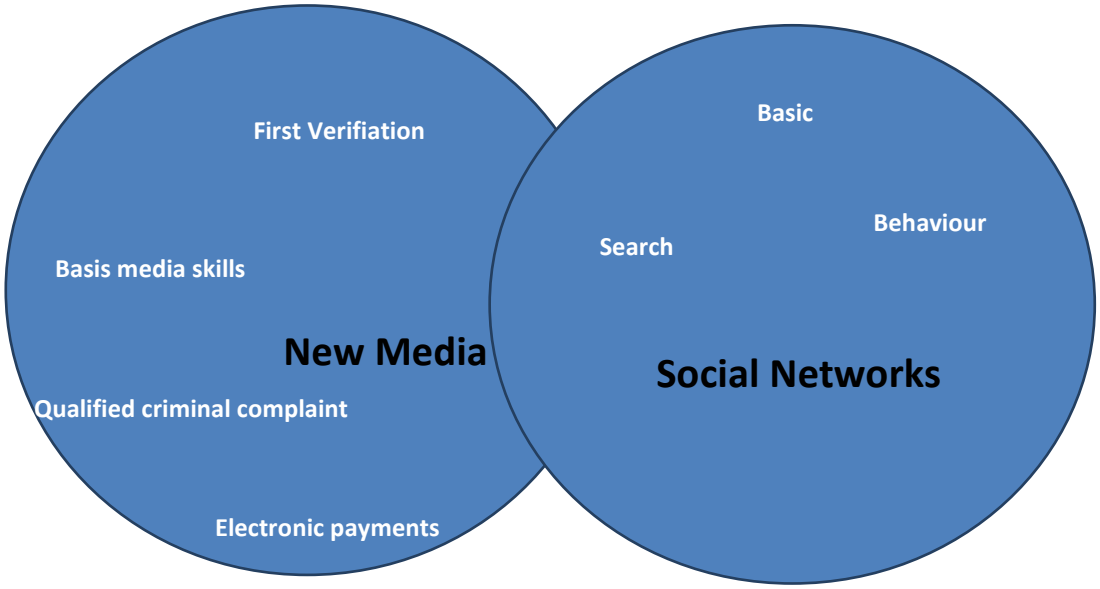


Graph 3: Bavaria

The fast and often intransparent progress of crime in cyberspace is one of the biggest challenges for the Bavarian police (Graph 3). The intense rise of crime shows that this topic needs to be in the spotlight/needs to be focused on. Daily changes mean new defiance and all police officers need to be prepared for such crimes. In 2013, a concept was designed and the institute of further education was commissioned with the realisation.

Of course, there are different levels of knowledge and different target groups. This is why different training groups were introduced. Every officer has to work through three different levels starting with introducing e-learning courses, presence trainings and ending with subsequent Intranet information pages (cybercrime portal) to learn more about the phenomenon.

Following that concept, there are two big topics that belong together as you can see in the Graph 4.



Graph 4: Levels of knowledge and target groups

Both topics have very much in common and because of this, they cannot be separated from each other. Four programs are going to be worked through in the sector „New Media“. Sector „Social Networks“ includes three programs. Basic SN and Behavior SN are obligatory for every employee of the Bavarian Police. For every learner who is actually in schooling there is no need for these two modules. The shown topics are part of the basic education in the police schools (Graph 4).

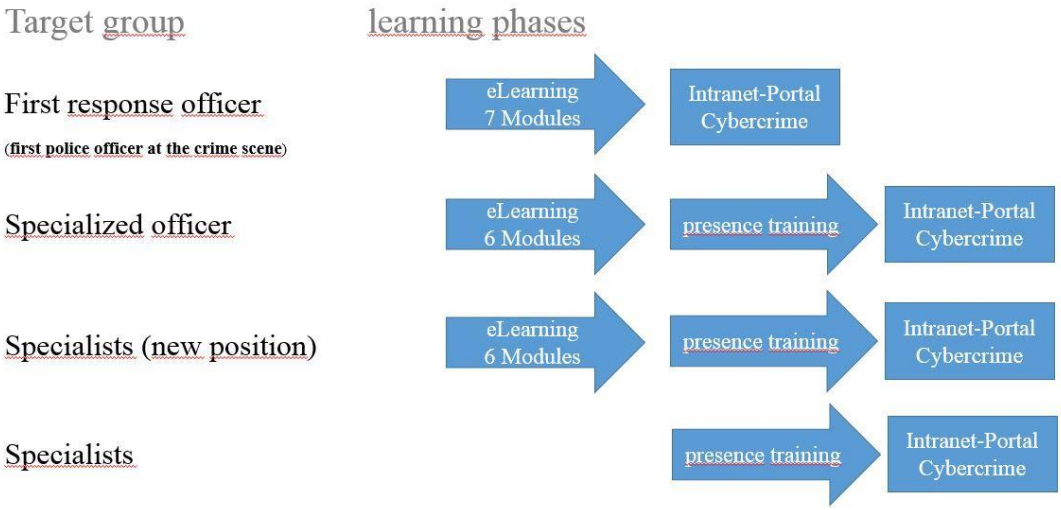
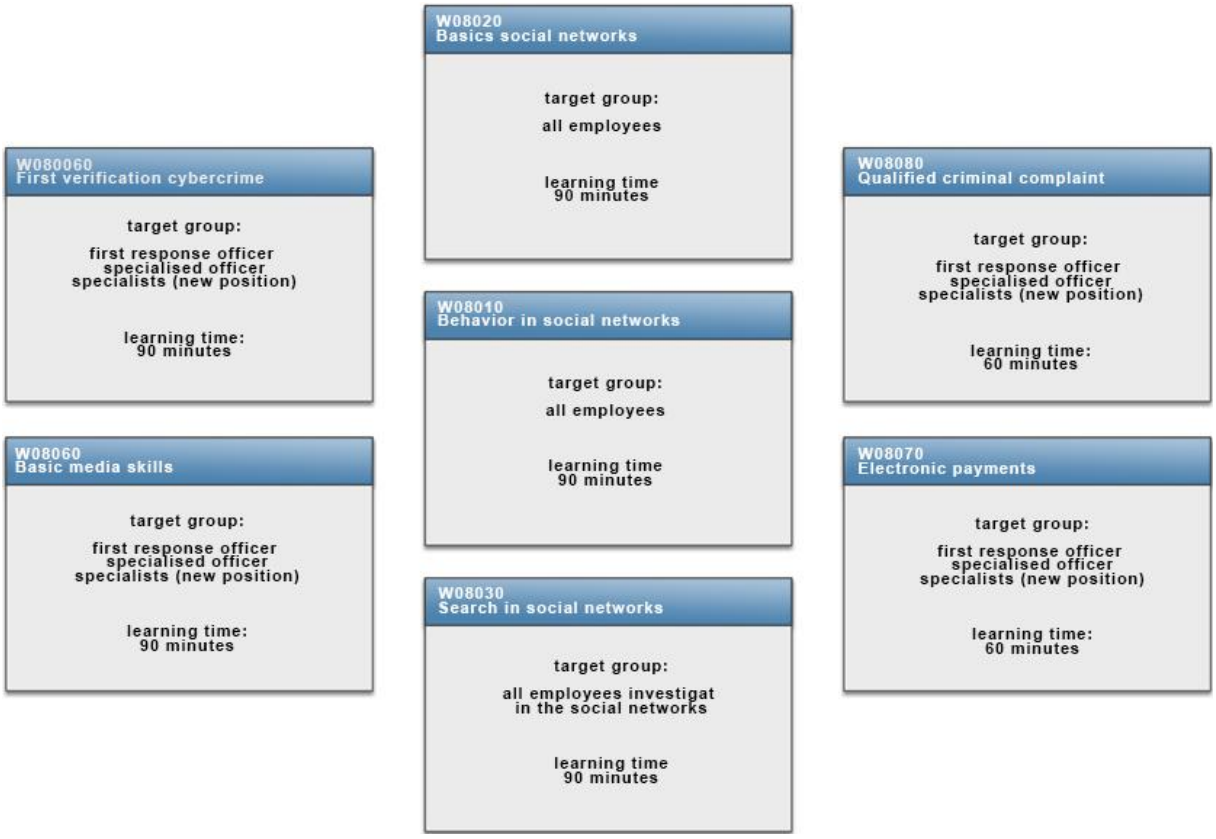


Figure 1: The learning phase for each target group

The learning phases for each target group is shown in the Figure 1.
The Graph 5 clarifies the different e-learning programs with the audience.



Graph 5: Target groups with e-learning (dichtl, 2015)

Of course, every program has its own learning time and target group, which is illustrated in the next graph. There is a program with 45 minutes working time, but also times of about 90 minutes, especially for specialized trainings.

4. EVALUATION RESULTS

PR Christian Dichtl conducted an evaluation on acceptance of e-learning in the further education of Bavarian police officers. He wanted to find out, which factors have influence on the acceptance of e-learning.

Following Goodhues Task-Technology Fit Model (Goodhue/Thompson, 1995), there is a direct connection between task, technology and the individual. These three factors matter to achieve acceptance (Bürg/Mandl, 2004). Hence, e-learning needs to give clear tasks, a technology which is easy to handle, and of course every single officer who has to work with the program needs to be able to handle e-learning. Evaluations should give a feedback on how the programs could be improved. Christian Dichtl even asked, whether the user thought that e-learning was the right way to do further education (Dichtl, 2015). The results are shown in the Table 3.

Table 3: The age groups that are preferring e-learning (Dichtl, 2015)

		On which form of continuing education you would participate in the future most likely again?			
		E-Learning	Blended Learning	Presence training	total
Age group	Up to 30 years	22,4%	56,2%	21,4%	100,0%
	31 to 40 years	21,3%	52,2%	26,5%	100,0%
	41 to 50 years	12,0%	51,6%	36,4%	100,0%
	Over 50 years	17,6%	46,9%	35,5%	100,0%
total		17,9%	51,0%	31,1%	100,0%

It is also interesting how the methodic and didactic system was evaluated (Table 4).

Table 4: Methodic and didactic evaluation 1 (dichtl, 2015)

Single item	trifft voll zu 1	trifft über-wiegend zu 2	trifft weniger zu 3	trifft nicht zu 4	MW	SD	N
The course contents were efficiently explained previously	34,1 420	49,7 613	12,4 153	3,8 47	1,86	0,77	1233
The learning objectives of the eLearning modules were clearly defined at the beginning	43,1 530	44,8 552	11,0 136	1,1 13	1,70	0,70	1231
The graphic design of the eLearning modules has appealed to me	18,9 233	53,0 653	23,1 285	5,0 62	2,14	0,77	1233
The learning contents were presented with various media (video, audio, images, text)	49,1 607	43,7 540	6,2 76	1,0 12	1,59	0,65	1235
The curriculum was built understandable and structured	28,4 351	56,5 698	13,3 164	1,8 22	1,88	0,68	1235
The questions was phrased clearly and unambiguously	19,9 246	55,3 685	21,6 268	3,2 39	2,08	0,73	1238

One very interesting result is that the design of the program is obviously an individual term. It depends on personal taste (Table 5).

Table 5: Methodic and didactic evaluation 2 (dichtl, 2015)

I could always track my learning progress	34,3 422	45,3 558	17,1 211	3,2 40	1,89	0,79	1231
The tutorial was well matched to my prior knowledge	16,8 199	47,2 558	27,1 321	8,9 105	2,28	0,84	1183
Through the tutorial I could expand my expert knowledge	34,1 422	49,0 607	14,0 173	2,9 36	1,86	0,76	1238
My personal learning objectives have been achieved	36,1 441	47,7 582	12,8 156	3,4 41	1,83	0,77	1220
I was able to adjust the pace of learning to my individual needs	55,1 676	35,8 439	6,8 84	2,3 28	1,56	0,72	1227
The acquired knowledge can be very well transposed in practical application	16,9 197	52,3 611	23,4 273	7,4 87	2,21	0,80	1168

The last two items declare that on the one side the user is able to learn and combine this learning with her/his individual needs, but on the other side, the users are not completely content with using the acquired knowledge in their worklife. This is something we need to work on.

In general, the evaluation shows a high acceptance of e-learning, of course there are a few differences shown in the results of the various age groups. Aged between 40 and 50 years, the users prefer classroom trainings at the institute of further education in Ainring. 75% of all the participants would like to change more courses with e-learning.

The fact that the asynchrony communication possibilities were used very little has proven to be a problem. The users do not require it any more. Maybe this result depends on the fear of showing weakness or ignorance on some of the shown topics. They do not want their superior to see this.

5. CONCLUSION

Seeing all these matters, it is clear that e-learning seems to be one of the preferred ways to learn, but always in combination with presence learning. The evaluation has proven this opinion. To become even more variable and multifunctional, the Bavarian Police also works together with other federal states and institutions. Aim is to use resources better and more precisely.

In 2016, the Bavarian Police starts to work with podcasts and virtual classrooms, which is going to be a step that pictures the Bavarian Police as modern and future trend-oriented employer. Of course these steps can only be done with a didactic and methodic concept, but in focus is the learning process of each officer and how it can be individualized furthermore.

REFERENCES

Bürg, O./Rösch, S./Mandl, H. (2005). *Die Bedeitung von Merkmalen des Individuums und Merkmalen der Lernumgebung für die Akzeptanz von E-Learning in Unternehmen*. Forschungsbericht 137. https://epub.ub.uni-muenchen.de/561/1/FB_173.pdf (March 08, 2016).

Dichtl, C. (2015). *Akzeptanz von E-Learning. Eine empirische Untersuchung erfolgskritischer Akzeptanzfaktoren in der polizeilichen Fortbildung.* Tiefenbach.

Goodhue, D./Thompson, R. (1995). *Task-Technology Fit and Individual Performance*. Publication MIS Quarterly (last call: March 18, 2016) http://aisel.aisnet.org/misq/vol19/iss2/5

Sauter, A./Sauter, W. (2002). *Blended Learning. Effiziente Integration von E-Learning und Präsenztraining*. Neuwied, Kriftel: Luchterhand.

Wendt, M. (2003). *CBT und WBT. Konzipieren, entwickeln, gestalten*. München: Carl Hanser Verlag.

PROFESSIONAL PAPER

Vesna Trajkovska[244]

USE OF EU LEGAL ACTS ON COMBATING CYBERCRIME IN TEACHING ENGLISH VOCABULARY TO LAW ENFORCEMENT STUDENTS

Summary

The paper deals with the use of authentic EU documents as didactic resources in teaching English to law enforcement students. It draws on the idea that the use of authentic documents is an important segment in the process of designing materials for teaching English for specific purposes, which also includes English for law enforcement purposes. This type of documents abounds in specialized vocabulary and can be used in numerous ways for creating classroom activities, aimed at enhancing students' lexical knowledge in a respective field. The paper focuses on the presentation of several options for designing vocabulary exercises based on the texts of several EU legal acts addressing the issue of cybercrime. These exercises are specifically designed for law enforcement students and they should help them enrich their vocabulary in the field of cybercrime and information systems, which is of great importance for their future profession. Although the exercises are designed on the basis of a limited number of EU documents, they provide solid ground for one to realize the multitude of possibilities for using this type of authentic documents in an English class.

Key words: *vocabulary, EU legal acts, English for specific purposes, cybercrime.*

1. INTRODUCTION

Acquisition of English lexical knowledge is a very important aspect in educating law enforcement students. In order to be able to perform their duties within their prospective profession with greater success, they should acquire a high proficiency level of English which would enable them to communicate effectively in English in certain situations, depending on the specificity of the tasks and duties in question. This can be achieved through English language syllabus which is comprised of subject-based lessons, covering specific contents relevant to their profession, whose aim is to enhance students' communicative competence.

As far as cyber security is concerned, it is more than evident that in recent years it has become a very important issue, closely linked to the possession of English lexical skills. Namely, as a relatively recent phenomenon, it abounds with concepts which are mainly lexicalized in English and then imported into other languages, either in the form of lexical borrowings, calques i.e. direct translations, or very rarely in the form of newly coined words within the lexical corpus of the target language. Within the context of European Union, these concepts

[244] Assistant Professor Vesna Trajkovska, PhD, email: trajkovska_vesna@yahoo.com, Faculty of Security, Skopje, Idrizovo bb

are often defined in official documents which are originally drafted in English and then translated and incorporated in the national legislations of the member countries or the countries aspiring for EU membership.

Bearing this in mind, it is essential for professionals in the area of security and law enforcement to become familiar with the contents of these type of texts, both in their original form and the corresponding translated versions. Therefore, the inclusion of official EU documents in the law enforcement English classroom makes them a very helpful resource for teaching specialized vocabulary in the field of cyber security as used in an authentic, real life context. For the purpose of this paper, in the sections that follow, we will present several options for designing classroom activities containing contents of official EU documents, which are based on the principles of communicative teaching within English for Specific Purposes (ESP) instruction. We will limit our paper on three EU documents, namely: *DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*, and *COUNCIL FRAMEWORK DECISION of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment*[245]. These documents will be used as the basis for designing classroom activities with the main focus on students' lexical knowledge. We will present several techniques for transforming specialized texts into interactive classroom activities within the context of communicative language teaching, as the most widely used approach in foreign language instruction in the last few decades.

2. COMMUNICATIVE LANGUAGE TEACHING IN THE "ESP" CLASSROOM

The emergence of English for Specific Purposes (ESP) is considered one of the greatest novelties which were introduced in teaching English as a foreign language in the second half of the 20th century. According to Hutchinson and Waters (1987:8) its emergence is based on three key factors. The first factor was linked to the status of economic power of the USA and the promotion of English as the language of technology and commerce, which led to the creation of "a new generation of learners who knew specifically why they were learning a language" (ibid: 6). The second factor was related to the emergence of new ideas in linguistics, and the shift of focus towards discovering how language was used in real communication (ibid:7). Therefore, the language that learners needed "could be identified by the linguistic characteristics of their specialist area of work or study" (ibid: 8). Finally, ESP teaching was encouraged by the developments in educational psychology, characterized by the shift of focus on the learners' interests which would have influence on "their motivation to learn and therefore on the effectiveness on their learning" (ibid: 8). This could be achieved by

[245] The texts were selected on the basis of the list of EU legislative actions in the fight against cybercrime on European Commission's website: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm (February 21, 2016.)

taking texts from their areas of study, which would "improve the learners' motivation and thereby make learning better and faster" (ibid).

What distinguishes ESP instruction is the specific role of the teacher who acts both as course instructor and course designer. Based on learners' needs analysis, the ESP teacher "needs to find out what the language-based objectives of the students are in the target occupation or academic discipline and ensure that the content of the ESP course works towards them" (Basturkmen, 2010:8). On the other hand, the emphasis on real communication use of English in a specific discipline implies that the lessons should be organized in a manner which would meet the communicative needs of the learners, thus increasing their motivation to learn the language.

The enhancement of students' communicative skills within ESP context can best be achieved through classroom activities based on communicative language teaching. The emergence of this approach coincides with the emergence of English for specific purposes as a separate branch of teaching English as a foreign language. It dates back to the 1970s when Hymes introduced the concept of communicative competence, which was also proposed by Campbel and Wales. It actually refers to the knowledge of language use in specific contexts and communicative situations. Apart from grammatical competence, communicative competence should also include contextual or sociolinguistic competence (Canale & Swain, 1980:4). This practically means that when communicating, besides the linguistic forms, students should be aware of the context of the communicative act, the environment, the interlocutors, the goals they want to achieve, i.e. the specific function of the utterance etc. This is the reason why the communicative syllabus focuses on exposing students to the language as it is used by native speakers, by simulating real life situations, often supported by real life authentic oral and written materials.

Within the context of communicative language teaching, classroom work revolves around fluency-oriented activities, including inter alia, information-gap activities, jigsaw activities, task-completion activities, information-gathering activities, opinion-sharing activities etc. with emphasis on pair and group work as well as authenticity (Richards, 2006: 14-21). This type of activities should foster students' interaction and enable them to enhance their speaking, writing, reading and listening skills as a whole, since "effective teaching of language as communication calls for an integrated approach which represents different skills and abilities as aspects of a singly underlying activity" (Widdowson, 1978:142). The aim of these activities is to bring the authenticity of real life language use in the classroom and to prepare students for functional use of the language in contexts and communicative settings relevant to their future profession, through role-plays, games, simulations, problem-solving activities etc.

3. THE USE OF AUTHENTIC MATERIALS IN THE "ESP" CLASSROOM

As we could see from the introductory sections, the tendency towards authenticity in terms of language use plays an important role in the communicative ESP classroom. Bearing this in mind, one can clearly conclude that the selection of relevant content to be included in the ESP syllabus is a very important aspect in the material development process. This importance arises from the ESP learners' needs for exposure to specialized content belonging to their specific area of interest, which will help them improve their lexical skills in the respective area. It can also be referred to as "carrier content, informative content, discipline-based knowledge, specific content, specialist knowledge or expert knowledge" (Bocanegra-Valle, 2010:142-43) meaning "information which is specific to a particular discipline and which people, like students and future experts, possess in their mother tongue." (ibid: 143). The inclusion of this type of knowledge into the ESP classroom can best be achieved through the use of authentic materials from the specific area which can be used either in their integral form, or with certain modification and adaptation based on the learners' proficiency level. Authentic material actually refers to "any kind of material taken from the real world and not specifically created for the purpose of language teaching." (Ellis & Johnson, 2003:157). In other words, it practically means that these texts were not primarily written for language learners, and their contents was not tailored so as to meet the learners' educational needs. Within ESP context, authentic texts from the specific area can be used as helpful teaching resources, since "non-authentic texts cannot represent real-world language use, that simplified materials often lose some meaning with simplification and that the real-world situations learners will face or are already facing are best prepared for with authentic texts." (Flowerdew & Peacock, 2001:182). As Nunan (2004:50) puts it "specially written texts and dialogues do not adequately prepare learners for the challenge of coping with the language they hear and read in the real world outside the classroom – nor is that their purpose."

Authentic materials are often written by specialists in a given area and they are primarily intended for such specialists. Having this in mind, they can logically be considered as useful resources containing words and expressions which are typically used by specialists in the respective area. These words and expressions are used in the forms and manner in which they are naturally used by their speakers in real life contexts, which can make it difficult for other language users to follow and to understand them without the help of a dictionary, or without being given the wider context in which they occur. Taking into consideration the characteristics of subject-bound authentic texts, it becomes clear that their inclusion in the ESP syllabus is crucial, when aimed at preparing ESP students for the functional use of the language with high level of proficiency and communicative competence. Depending on the type of text and the didactic goal which is to be achieved, these texts can be used in their original form, or modified, i.e. transformed into didactic exercises which will raise the motivation of the learners and will engage them in interactive communicative activities.

As far as teaching English for law enforcement is concerned, we can agree that course instructors have at their disposal a wide range of written and oral materials, which can be taken as the basis around which classroom activities can be organized. This includes, inter

area, the more specific segment of cyber security. Being a relatively new phenomenon, it is the subject of various documents, which address it from different perspectives. Its specific vocabulary is used, through which new concepts in the "cyber" area are lexicalized. At the level of European Union, the issue of cybercrime or the wider concept of cyber security are addressed by a number of legal documents, whose contents is used as the basis for the harmonization of the legislations of the existing and prospective member states. Taking this into account, it would be very useful for students to be exposed to the contents of such documents in their English classes, preparing them for their future profession. As cyber security professionals, they will inevitably deal with this type of texts which address a rapidly growing phenomenon of the 21st century.

In order to show the applicability of EU legal documents in ESP instruction for advanced students at tertiary level, in the section that follows we will present several strategies for developing interactive classroom activities aimed at enhancing students' lexical skills in the area of cybercrime and cyber security in general.

4. EU LEGAL TEXTS AS THE BASIS FOR DESIGNING COLLOCATION EXERCISES

Collocational competence is a very important aspect in foreign language acquisition process. In order to be able to express their thoughts clearly, particularly when using specialized language, speakers should possess good knowledge of the combinations in which various words co-occur. This applies equally to lexical collocations and grammatical collocations. A lexical collocation is typically composed of nouns, adjectives, verbs, and adverbs (Benson, Benson & Ilson, 2010: 31), while a typical grammatical collocation is composed of a dominant word, such as noun, verb or adjective and a preposition or other grammatical structure (ibid: xix). When it comes to the acquisition of a foreign language in a specific area, we can agree that collocations play a very important role, since specialized language used by professionals in a particular area consists of a wide variety of specific word combinations which have established a specific semantic relation. Authentic written documents in the area of cyber security abound in both grammatical and lexical collocations, which makes them a very useful resource for developing classroom activities for law enforcement students.
Taking this into account, for the purpose of this paper, we will present several techniques for using EU documents as the basis for designing communicative exercises aimed at acquisition of collocational knowledge. For the acquisition of knowledge of lexical collocations, we propose a game activity where students work in groups, and each group is given a different document. They are given a list of two or three prepositions, and they should read the document and find grammatical collocation with the specific preposition. They may have a limit of 10 collocations. When they find the collocations, they they create a gap filling exercise, where they take the original sentence from the text and delete the nouns or verbs collocating with the respective preposition. The students from the other groups work together and try to guess the missing collocation. For each guess they gain a point, and the group with the highest number of guesses at the end wins the game. This type of activity is very useful since it makes the learning of technical, specialized vocabulary more interesting for students.

Working in groups helps them develop their team work skills, and it allows for the inclusion and participation of both strong and weak students who help each other in negotiation of meaning while competing with the other teams.

The following is a list of sentences containing collocations with the prepositions "against" and "to", taken from *DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*[246]:

NOUN + "AGAINST" Collocations

"Providing information can facilitate a better understanding of present and future threats and thus contribute to more appropriate and targeted decision-making on combating and preventing _____information systems." (Key: ***attacks AGAINST****)*

"Member States are encouraged to provide for relevant measures incurring liabilities in the context of their national law in cases where a legal person has clearly not provided an appropriate level of _____ cyber attacks." (Key: ***protection AGAINST****)*

"Improved cooperation between the competent law enforcement bodies and judicial authorities across the Union is essential in an effective _____ cybercrime." (Key: ***fight AGAINST****)*

"The liability of legal persons under paragraphs 1 and 2 shall not exclude criminal _____ natural persons who are perpetrators or inciters of, or accessories to, any of the offences referred to in Articles 3 to 8." (Key: ***proceedings AGAINST****)*

"_____ legal persons" (Key: ***sanctions AGAINST****)*

NOUN + "TO" Collocations:

*"Ensuring an appropriate level of protection of information systems should form part of an effective comprehensive framework of prevention measures accompanying criminal law _____ cybercrime." (****responses TO****)*

*"This constitutes a _____ the achievement of a safer information society and of an area of freedom, security, and justice, and therefore requires a response at Union level and improved cooperation and coordination at international level." (****threat TO****)*

*"This tendency is accompanied by the development of increasingly sophisticated methods, such as the creation and use of so-called 'botnets', which involves several stages of a criminal act, where each stage alone could pose a serious _____ public interests." (****risk TO****)*

*"Particular attention should be paid to raising the awareness of innovative small and medium-sized enterprises to threats relating to such attacks and their _____ such attacks, due to their increased dependence on the proper functioning and availability of information systems and often limited resources for information security." (****vulnerability TO****)*

*"There is a need to achieve a common approach to the constituent elements of criminal offences by introducing common offences of illegal _____ an information system, illegal system interference, illegal data interference, and illegal interception." (****access TO****)*

*"A case may be considered minor, for example, where the damage caused by the offence and/or the _____ public or private interests, such as to the integrity of a computer system or to computer data, or to the integrity, rights or other interests of a person, is insignificant or is of such a nature that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary." (****risk TO****)*

[246] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF (February 21, 2016.)

Games can also be used within the context of the acquisition of lexical collocations. As the basis of this game, we propose the same Directive which was used for the practice of grammatical collocations. This time, the activity is centered around error correction. Namely, students are divided into two groups and they are given sentences from the Directive, each sentence containing a wrongly used collocation. They are also given a list with the correct collocates, with several extra words which are supposed to puzzle the students, thus making the task more complicated for them. The teacher chooses one sentence and the groups should spot the mistake and replace the wrong word with the correct collocate from the list. They have the right to give one answer only, and if the answer is correct they earn 10 points. If the answer is incorrect, they lose 20 points. They change turns, and the group with more points wins the game.
In order to illustrate this activity, we will present several sample sentences with wrongly used collocates, and their corrected counterparts as they are authentically used in the Directive.
The following is the list with the correct collocates, which should be inserted on the place of the wrong ones:

approximate alter damage cause launch constitute impose introduce

These collocates should be inserted in the appropriate place in the following sentences taken from *DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*[247]:

"Once created, the infected network of computers that ***~~form~~*** *the botnet (Key:* ***constitute****) can be activated without the computer users' knowledge in order to* ***~~start~~*** *a large-scale cyber attack (Key:* ***launch****), which usually has the capacity to cause serious damage, as referred to in this Directive."*
"Large-scale cyber attacks can ***~~provoke~~*** *substantial economic damage (Key:* ***cause****) both through the interruption of information systems and communication and through the loss or alteration of commercially important confidential information or other data."*
"The objectives of this Directive are to ***~~modify~~*** *the criminal law (Key:* ***approximate****) of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities, including the police and other specialized law enforcement services of the Member States, as well as the competent specialized Union agencies and bodies, such as Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA)."*
"This Directive aims, inter alia, to ***~~involve~~*** *criminal penalties (Key:* ***introduce****) for the creation of botnets, namely, the act of establishing remote control over a significant number of computers by infecting them with malicious software through targeted cyber-attacks."*

[247] ibid

5. USING EU DOCUMENTS FOR TEACHING CONCEPTS RELATED TO CYBERCRIME AND CYBER SECURITY

For successfully performing their prospective professional duties, it is important for law enforcement officers to be able to make a clear distinction between various types of crimes and offences. This is particularly important in those cases when the different types of crimes/offences share certain similarities, and their proper identification can be of crucial importance when practically dealing with the crimes/offences in question. For this reason, in this section we will offer an exercise where the students will be presented with offences related to child sexual abuse on the one hand, and offences related to child sexual exploitation, on the other hand. This classroom activity is carried out with two group of students working together as part of a team. They are given several jumbled paragraphs defining activities which constitute offences considered as either sexual abuse or sexual exploitation. Students from the first group work on identifying the activities related to sexual abuse, while the students from the second group work on identifying the activities related to sexual exploitation. They work together, discussing the key notions defined by the paragraphs. After they finish with this task, a representative from each group shares the results and the whole class infers the difference between these two groups of offences. For the purpose of this exercise, we chose the definitions provided in *DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*[248].
The following is an excerpt from the sample exercise:

"Causing, for sexual purposes, a child who has not reached the age of sexual consent to witness sexual activities, even without having to participate, shall be punishable by a maximum term of imprisonment of at least 1 year." (Key: ***Article 3****,* ***Offences concerning sexual abuse, Group 1)***

"Causing or recruiting a child to participate in child prostitution, or profiting from or otherwise exploiting a child for such purposes shall be punishable by a maximum term of imprisonment of at least 8 years if the child has not reached the age of sexual consent, and of at least 5 years of imprisonment if the child is over that age." (Key: ***Article 4, Offences concerning sexual exploitation, Group 2)***

"Causing, for sexual purposes, a child who has not reached the age of sexual consent to witness sexual activities, even without having to participate, shall be punishable by a maximum term of imprisonment of at least 1 year." (Key: ***Article 3, Offences concerning sexual abuse, Group 1)***

"Causing or recruiting a child to participate in pornographic performances, or profiting from or otherwise exploiting a child for such purposes shall be punishable by a maximum term of imprisonment of at least 5 years if the child has not reached the age of sexual consent and of at least 2 years of imprisonment if the child is over that age." (Key: ***Article 4, Offences concerning sexual exploitation, Group 2)***

[248] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN (February 21, 2016.)

Apart from these two types of offences, the above-mentioned EU Directive distinguishes a third group of offences which belong to the group of offences concerning child pornography. This group covers various activities related to child pornography, and for the purpose of our paper we propose a classroom activity where students practice word formation through suffixation. Through pair work, they should guess the appropriate suffix and fill in the gaps in the missing words. By participating in this activity, students raise their awareness related to the lexical productivity of English, and the suffixes which are used by English speakers for derivation of different parts of speech.

In the following excerpts, students are specifically focused on the derivation of nouns and adjectives, based on the definitions contained in *DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*[249]:

Article 5
Offences concerning child pornography

1. Member States shall take the necessary measures to ensure that the ***intent*** *(Key:* ***intentional****) conduct, when committed without right, referred to in paragraphs 2 to 6 is punishable.*
2. ***Acquire*** *(Key:* ***Acquisition****) or* ***possess*** *(Key:* ***possession****) of child pornography shall be punishable by a maximum term of imprisonment of at least 1 year.*
'3. Knowingly obtaining access, by means of ***inform*** *(Key:* ***information****) and* ***communicate*** *(Key:* ***communication****) technology, to child pornography shall be punishable by a maximum term of imprisonment of at least 1 year.*
4. ***Distribute*** *(Key:* ***Distribution****),* ***disseminate*** *(Key:* ***dissemination****) or* ***transmit*** *(Key:* ***transmission****) of child pornography shall be punishable by a maximum term of imprisonment of at least 2 years…*

In order to practice contextual use of theoretically acquired knowledge, as a follow-up, students may continue with a listening comprehension exercise, where they will hear several recorded audio stories about child sexual abuse, child sexual exploitation and child pornography. Based on the information about these three types of offences contained in the EU Directive on Combatting the Sexual Exploitation of Children Online and Child Pornography, they should identify the type of offence described in each case.

Sample case 1

After a police raid in a local night club, the police officers arrested several traffickers, and in the cellar of the club, among other prostitutes, they found a 10-year-old girl who was forced into giving sexual services to adult men, and was also involved in virtual prostitution via Internet. (Type of offence: ***Child Sexual Exploitation****)*

[249] ibid

Sample case 2

In a local elementary school, a maths teacher was arrested, when he was caught in flagranti having sex with a 13-year-old schoolgirl who had low grades in maths. (Type of offence: ***Child Sexual Abuse****)*

Sample case 3

The coach of a junior handball team stored in his personal computer pictures of naked 11-year-old handball players taken in the dressing room. The conversation log on his profiles on several social networks revealed that he sent these pictures to his virtual friends in exchange for pictures of other girls. (Type of Offence: ***Child Pornography****)*

The acquisition of new concepts in this area can also be achieved through gap-filling exercises, in the form of pair work. To illustrate this, we will use the same Directive, but this time we will deal with different concepts. Namely, they are given the definitions of "a child", "age of sexual consent", "child pornography" and "child prostitution", taken from the above-mentioned Directive. Both students working in pair have the same definitions with different pieces of information deleted. Their task is to ask each other questions and fill in the gaps with the missing information that their partners have.
The following is an excerpt from this activity, with the definitions given to the students, and the possible questions they may ask each other in order to complete the sentences in their original form as they are found in the Directive[250]:

'child' means any person below the age of …….; (Key: ***18 years****)*
Sample question: ***Below what age is a person considered a child?***
'age of sexual consent' means the age below which, in accordance with ……. law, it is prohibited to engage in sexual activities with a child; (Key: ***national****)*
Sample question: ***Which law defines the age of sexual consent?***
(c) 'child pornography' means:
(i) any material that visually depicts a child engaged in real or simulated ……. ……. conduct; (Key: ***sexually explicit****)*
Sample question: ***What kind of conduct of a child is visually depicted in the material which constitutes child pornography?***
(ii) any depiction of the ……. organs of a child for primarily sexual purposes; (Key: ***sexual****)*
Sample question: ***Which organs of the child are depicted in child pornography materials?***
(iii) any material that visually depicts …… engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of ……, for primarily sexual purposes; or (Key: ***any person appearing to be a child (x 2)****)*
Sample question: ***Whose engagement in real or simulated sexually explicit conduct, and whose sexual organs are depicted in the material which is considered child pornography?***
(iv) …… images of a child engaged in sexually explicit conduct or ……

[250] ibid

*images of the sexual organs of a child, for primarily sexual purposes; Key: (**realistic (x 2)**)*
*Sample question: **What kind of images of a child engaged in sexually explicit conduct and of the sexual organs of a child are considered child pornography?***
*(d) 'child prostitution' means the use of a child for sexual activities where ……. is given or promised as payment in exchange for the child engaging in sexual activities, regardless of whether that payment, promise or consideration is made to the child or to a third party; (Key: **money or any other form of remuneration or consideration)***
*Sample question: **What is the child given or promised in exchange for engagement in sexual activities?***
(e) 'pornographic performance' means *a live exhibition aimed at ……..., including by means of information and communication technology*, of: (Key: ***an audience***)
*Sample question: **Who is the live exhibition in pornographic performance aimed at?***
a child engaged in real or simulated sexually implicit conduct; or
*the sexual organs of a child for …….; (Key: **primarily sexual purposes)***
*Sample question: **Why are the sexual organs of a child exhibited?***

Finally, we will present an excerpt from an interactive classroom activity, where students, working in pairs, try to infer the meanings of various concepts, based on their use in *COUNCIL FRAMEWORK DECISION of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment*[251] from the section addressing *Offences related to payment instruments*, *Offences related to computers*, and *Offences related to specifically adapted devices*. Since we are going to demonstrate a technique which involves student's participation in pair work, we will limit our exercise to the first two offences, namely *Offences related to payment instruments* and *Offences related to computers*. One of the students is given the text of Article 2, which refers to *Offences related to payment instruments*, while the other student is given a list with the explanations of a selected number of words from the text. Based on the explanations and the context in which they appear in the document, the first student should guess the hidden words. After they finish with Article 2, they should continue with Article 3. This time, they change their roles, i.e. the second student has the whole text, while the first one has the explanations for the selected words. They repeat the procedure and come up with their answers. The first pair to finish with the task presents the answers to the rest of the class and finally the students compare and discuss their answers as a whole class, drawing conclusions about the semantic nuances of the various words and the contexts in which they are used.'

Below are the texts of both articles, with the selected words and the explanations of their corresponding meanings:

Article 2[252]
Offences related to payment instruments
Each Member State shall take the necessary measures to ensure that the following conduct is a criminal offence when committed intentionally, at least in respect of credit cards, eurocheque cards, other cards issued by financial institutions, travelers cheques,

[251] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001F0413&from=EN (February 21, 2016.)
[252] ibid

eurocheques, other cheques and bills of exchange:
(a) theft or other unlawful ***appropriation*** *(Word meaning:* ***the act of taking something for your own use, usually without permission[253]****) of a payment instrument;*
(b) ***Counterfeiting*** *(Word meaning:* ***copying or imitating (coins, handwriting, etc.) in order to deceive***[254]*) or* ***falsification (****Word meaning:* ***changing something, such as a document, in order to deceive people[255]****) of a payment instrument in order for it to be used fraudulently;*
(c) receiving, obtaining, transporting, sale or transfer to another person or ***possession (****Word meaning:* ***the fact that you have or own something[256]****) of a stolen or otherwise unlawfully appropriated, or of a counterfeited or falsified payment instrument in order for it to be used fraudulently;*
(d) ***Fraudulent*** *(Word meaning:* ***obtained, done by, or involving deception, especially criminal deception[257]****) use of a stolen or otherwise unlawfully appropriated, or of a counterfeited or falsified payment instrument;*

Article 3[258]
Offences related to computers
Each Member State shall take the necessary measures to ensure that the following conduct is a criminal offence when committed intentionally:
performing or causing a transfer of money or monetary value and thereby causing an ***unauthorized*** *(Word meaning:* ***not having official permission or approval[259]****) loss of* ***property*** *(Word meaning:* ***a thing or things belonging to someone[260]****) for another person, with the intention of procuring an unauthorized economic* ***benefit*** *(Word meaning:* ***an advantage or profit gained from something[261]****) for the person committing the offence or for a third party, by:*
— without right introducing, ***altering*** *(Word meaning:* ***changing or making different***[262]), ***deleting*** *(Word meaning:* ***removing from a document or record[263]****) or* ***suppressing*** *(Word meaning:* ***preventing something from being seen[264]****) computer data, in particular identification data, or*
— without right ***interfering with*** *(Word meaning:* ***preventing (a process or activity) from continuing or being carried out properly[265]****) the functioning of a computer program or system.*

---

[253] http://dictionary.cambridge.org/dictionary/english/appropriation#translations (February 21, 2016.)
[254] Based on the definition of counterfeit (v.) in Hornby, A.S. (1993). *Oxford Advanced Learner's Dictionary of Current English, fourth edition, seventh impression*. Oxford: Oxford University Press, p.271.
[255] Based on the definition of falsify (v.) on http://dictionary.cambridge.org/dictionary/english/falsify (February 21, 2016.)
[256] http://dictionary.cambridge.org/dictionary/english/possession (February 21, 2016.)
[257] http://www.oxforddictionaries.com/definition/english/fraudulent (February 21, 2016.)
[258] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001F0413&from=EN (February 21, 2016.)
[259] http://www.oxforddictionaries.com/definition/english/unauthorized?q=unauthorised (February 21, 2016.)
[260] http://www.oxforddictionaries.com/definition/english/property (February 21, 2016.)
[261] http://www.oxforddictionaries.com/definition/english/benefit (February 21, 2016.)
[262] Based on definition of *alter (v.)* on http://www.thefreedictionary.com/alter (February 21, 2016.)
[263] Based on the definition of *delete (v.)* on http://www.thefreedictionary.com/delete (February 21, 2016.)
[264] Based on the definition of *suppress (v.)* on http://dictionary.cambridge.org/dictionary/english/suppress (February 21, 2016.)
[265] Based on the definition of *interfere with* on http://www.oxforddictionaries.com/definition/english/interfere (February 21, 2016.)

6. CONCLUSION

Taking into consideration the sample exercises presented in this paper, we can draw a logical conclusion that it is possible to use EU legal acts as the basis for designing classroom activities for the acquisition of English vocabulary in the area of law enforcement. This specific paper was focused on EU documents – legislative actions are aimed at the fight against cybercrime, and the proposed activities revolved around vocabulary addressing this issue. Through the exercises presented in the paper we showed that specialized vocabulary from texts based on highly formal style can be presented to the students in the form of communicative classroom activities, which are aimed at fostering students' communicative competence.

The limitations of the paper can be found in the fact that only three EU documents related to the fight against cybercrime were selected as the basis for the selection of the excerpts which were included in the exercises. This practically means that the proposed activities represent only a small portion of the ideas which can possibly be developed into didactic materials for teaching English vocabulary to law enforcement students. The paper can serve as motivation for other authors who can explore other teaching ideas, based on the documents used in this paper and also including other documents addressing the issue of cybercrime. In this paper, we focused mainly on the development of students' lexical skills, but the selected documents can equally be useful for designing classroom activities for enhancing students' grammar skills, which can be a challenge for other papers that can be written in the future. Apart from the topic of cybercrime, this type of exercises which are developed on the basis of authentic texts within communicative language teaching, can also be useful when addressing other topics belonging to other areas within ESP instruction. Their transformation into didactic classroom materials can be an exhausting task for English teachers and course designers, but the results can be of great benefit for their end-users who will simultaneously acquire both content and linguistic knowledge.

REFERENCES

Basturkmen, H. (2010). *Developing Courses in English for Specific Purposes*. Basingstoke: Palgrave Macmillan.

Benson, M., Benson, E. & Ilson, R. (2010). *The BBI Combinatory Dictionary of English. Your guide to Collocations and Grammar, third edition revised by Robert Ilson*. Amsterdam/Philadelphia: John Benjamins Publishing Company.

Bocanegra-Valle, A. (2010). Evaluating and designing materials for the ESP classroom. In Ruiz-Garrido, M, Palmar-Silveira, J.C. & Fortanet-Gomez, I. (eds) *English for Professional and Academic Purposes*. Amsterdam/New York: Editions Rodopi B.V. (141-165).

Canale, M., Swain, M. (1980). Theoretical Bases of Communicative Approaches to Second Language Teaching and Testing. *Applied Linguistics*, (1), 1-47., http://ibatefl.com/wp-content/uploads/2012/08/CLT-Canale-Swain.pdf(February 21, 2016.)

Ellis, M & Johnson, C. (2003). *Teaching Business English*. Oxford: Oxford University Press.

Flowerdew, J. & Peacock, M. (2001). *Research Perspectives on English for Academic Purposes*. Cambridge: Cambridge University Press.

Hornby, A.S. (1993). *Oxford Advanced Learner's Dictionary of Current English, fourth edition, seventh impression*. Oxford: Oxford University Press.

Hutchinson, T. & Waters, A. (1987). *English for Specific Purposes: a learning-centered approach*. Cambridge: Cambridge University Press.
Nunan, D. (2004). *Task-based Language Learning*. Cambridge: Cambridge University Press.
Richards, J. (2006). *Communicative Language Teaching Today*. Cambridge: Cambridge University Press.
Widdowson, H.G. (1978). *Teaching Language as Communication*. Oxford: Oxford University Press.

Internet sources

COUNCIL FRAMEWORK DECISION of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001F0413&from=EN (February 21, 2016.)
DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN (February 21, 2016.)
DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF (February 21, 2016.)
http://dictionary.cambridge.org/dictionary/english/appropriation#translations (February 21, 2016.)
http://dictionary.cambridge.org/dictionary/english/falsify (February 21, 2016.)
http://dictionary.cambridge.org/dictionary/english/possession (February 21, 2016.)
http://dictionary.cambridge.org/dictionary/english/suppress (February 21, 2016.)
http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm (February 21, 2016.)
http://www.oxforddictionaries.com/definition/english/benefit (February 21, 2016.)
http://www.oxforddictionaries.com/definition/english/fraudulent (February 21, 2016.)
http://www.oxforddictionaries.com/definition/english/interfere (February 21, 2016.)
http://www.oxforddictionaries.com/definition/english/property (February 21, 2016.)
http://www.oxforddictionaries.com/definition/english/unauthorized?q=unauthorised (February 21, 2016.)
http://www.thefreedictionary.com/alter (February 21, 2016.)
http://www.thefreedictionary.com/delete (February 21, 2016.)

Gabor Kovacs[266]

COMMON PUBLIC SERVICE EXERCISE AT NATIONAL UNIVERSITY OF PUBLIC SERVICE

Summary

The training and education system of future Hungarian public service specialists are cost-effective and exercise oriented. In most of the European countries, the public service administration, military and law enforcement organizations, work together both in peace, during the wartime and during different types of disasters. The National University of Public Service (NUPS) is a special institution in Hungary and in the European Higher Education Area. At the end of each academic year, NUPS organizes The Common Public Service Exercise involving graduate students, Hungarian military and law enforcement organizations as well as public service organizations. This two days' practice oriented activity is unique in the European and Hungarian Higher Education Area. The heads of the University agree that future experts must be trained together and that they should learn the same basic knowledge, to be able to carry out joint activities more easily. The exercise of the past three years has been very useful and successful, according to the participants and the highest-level decision makers. A reader will have a full insight into the preparatory work and the course of the exercise and would gain the experience, which could be successfully adapted to his own work.

Key words: *law enforcement training and education, leadership methods, military education, policing, practice oriented training, public service education*

1. INTRODUCTION

The National University of Public Service (NUPS) is one of the special institutions in Hungary and in the European Higher Education Area. In spite of the fact that NUPS is only a 5-year-old higher education institution - its predecessor institutions are the Zrínyi Miklós National Defence University, the Police College and the Faculty of Public Administration of Corvinus University of Budapest – it provides significant achievements in public service training. This heritage provides a stable ground to the future progress.

The objective behind the integration was to set up a University that strengthens national loyalty and professionalism within the Hungarian public service. This effort requires cooperation in the civil public administration, military and law enforcement.

NUPS belongs to the middle-sized universities in Hungary; we have roughly 6,500 students and 350 instructors.

The Act on the National University of Public Service[267] "*the objective of the National University of Public Service with administrative, law enforcement and military courses is to*

[266] Gabor Kovacs, *National University of Public Service – Hungary*, e-mail: *Kovacs.Gabor@uni-nke.hu*

[267] Act CXXXII of 2011 on the National University of Public Service http://en.uni-nke.hu/uploads/media_items/nups-academic-and-examination-regulations.original.pdf

train professionals carrying out administrative, defense and law enforcement activities, to provide the officer supply of the defense and law enforcement organizations and to create the interoperability among the unifying public service careers"

The university is tailored according to the Bologna Process, it provides undergraduate (bachelor, BA), graduate (master, MA) and PhD levels as well as special training programs, further training and re-training ones.[268]

The 'peaceful life of Hungarian citizens' is full of dangers and problems (natural dangers, crimes, illegal migration, dangerous industrial plants). The globalized impacts, the social and natural dangers all threaten our citizens' lives. The task of the law enforcement organizations and other state organizations is to manage these dangerous situations.[269] In order to manage these situations, the law enforcement, the military and the public service organizations have to work together.[270] One of the good examples is the annual common exercise, which is carried out at NUPS.

2. THE COMMON PUBLIC SERVICE MODULE

The basic task of the University is to change the training and education structure in order to provide the interoperability among the different professions.

The Common Public Service Module – the 15 subjects are different and cover the completely public administration basic knowledge materials. *(Constitutional Law, General Political Science, General Sociology, The State's Structure, Security Sciences, Military Theory and Military Operation, Disaster Management, Public Service Function,* ***Common Public Service Exercise****, Public Financial Affairs, Public Service Careers, Public Service Logistics, National Security Sciences, Theory of Law Enforcement, Management and Organization Theory*[271]*).*[272]

According to the accepted curricula, students prove the level of their knowledge summarized in the common module: in the common public service exercise. During this exercise, the students carry out tasks related to a specific and complex problem. All of the students work as if they were in their own future profession in order to be able to solve different situations.

In the past 3 years, NUPS organized the following exercises.

3. THE 2013 YEAR'S EXERCISE "WHITE-WATER 2013" (VADVIZ 2013)

The topic of the 2013-year's exercise was the task required from the public service organizations during the flood emergency in the homeland *(to maintain the public order, to handle the illegal immigration, the relocation of citizens and the relocation of a prison).* The military students in the framework of the exercise focused on another topic. That was the

[268] Common Core Curriculum Master Education, NUPS Faculty of Law Enforcement, Law Enforcement Management Theory Department 2013. Budapest, Ludovika tér 2.

[269] János Varga: Some relationship between border security, public safety, public security and personal safety In: Eva Kunovská (szerk.). Police Theory and Practice. Bratislava: Akadémia Policajného zboru, 2010. pp. 135-142.

[270] „International Perspectives on Police Education and Training." Editor: Perry Stanislas, Pulitzer: Routledge Taylor and Francis Group, 2014. London, Chapter 11., Fórizs Sándor: Police training and education in Hungary, p. 175-192. ISBN: 978-0-415-63218-8 (hbk), ISBN: 978-0-203-09589-8 (ebk).

[271] Czuprak Otto, Kovacs Gabor: Management and Organization Theory, Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., 2013. 326 p.(ISBN:978-615-5344-36-7)

[272] Common Core Curriculum Bachelor Education NUPS Faculty of Law Enforcement, Law Enforcement Management Theory Department 2013. Budapest, Ludovika tér 2.

preparation of the peacekeeping mission of the special units of the Hungarian Army and the preparation during the emergency caused by the flood.[273]

Throughout the exercise, the Disaster Management Organizations began the process as if it had been a normal situation. They started the preparation process in order to avoid the flood at the area of the - second largest river of Hungary - the river Tisza. The local municipalities and the Disaster Management Organizations started their joint activity. Through the emergency, the National Emergency Management Centre directed and organized the activity of different organizations involved in the activity. During the emergency, the law enforcement students practiced the collection process of illegal immigrants at the borders and the control of rescue forces at the border checkpoints.

The organizations practiced the management tasks according to the competences of different levels. They planned, organized, implemented and controlled joint activities, developed cooperation among the following units: the European and other national and international organizations, the authorities of neighboring countries, the homeland law enforcement, the public service and military organizations, the non-governmental and charity organizations that took part in the clearing process of the emergency. All of the students practiced the duties of Hungary related to the UN, NATO, EU and Schengen membership. The number of participants was approximately 700 students. Some parts of the Hungarian Army provided some sub-tasks in a peacekeeping mission. The military staff prepared the relocation of different subunits to the crisis zone, the coordination and managing the peacekeeping mission, the activity at the demilitarized zone, and the cooperation with the governmental and non-governmental organizations. This exercise was the first exercise in the life of NUPS – it was successful.

4. THE IMPLEMENTATION OF COMMON PUBLIC SERVICE EXERCISE "LAST FORT 2014" ("VÉGVÁR 2014")

The scenario of the Common Public Service Exercise in 2014 was different, illegal migration problem, homeland terror attack etc. During the preparation period, the staff prepared a detailed fictional basic situation. The drafting group led by the vice rector for education prepared a very detailed basic mission for all participants. The number of participants that year increased, it was more than 1,100 students and approximately 100 teachers and other personnel. The virtual scene of the exercise was a designated area of Hungary. The real scene of the exercise was the assembly room of the Law Enforcement Campus and the Military and Officer Training Campus. One university campus could not provide enough working place for the participants, so the leaders decided to use parallel working method during the exercise. The same exercise was to be run at two different campuses so the umpires could handle the coordination and monitor the students.

In order to make the exercise successful the staff prepared a special mission for each profession and it was tailored for the police (the following specializations: border guard,

273 Gabor Kovacs The new challenges and approach at the law enforcement master education programme at the National University of Public Service In: Ksenija Butorac 4th International Scientific and Professional Conference: POLICE COLLEGE RESEARCH DAYS IN ZAGREB. 886 p., 2015.04.23-2015.04.24. Ministry of the Interior of the Republic of Croatia, Police Academy, 2015. pp. 226-239. (ISBN:978-953-161-291-6)

criminal investigation, public order), the military (artillery, tank unit, etc.) and the public administration students.[274]

During the exercise, the students used the computer labs and the different special operation rooms.

In order to make the exercise lifelike the different movements were carried out in real time on the training field. The continuous connection with the participants on the training field was provided by a video conference system and a satellite link.

The students at local, county and national levels created different organizations. The graduating students acted as the organization leaders and the staff as well. Each participant carried out their task according to the competences of their respective organization. They used the forces and the cooperative organizations in order to solve the different situations.

In 2015, the topic of the Common Public Service Exercise was the same like in the year of 2014.

5. THE IMPLEMENTATION PLAN OF COMMON PUBLIC SERVICE EXERCISE "STORM 2016" ("VIHAR 2016")

The basis of the 2016 exercise was provided by the freezing rain and hailstorms along with their consequences in Hungary in early December 2014. Similar emergencies due to extreme weather conditions may occur at any time. The prevention, management and recovery procedures through the cooperation of public service branches as well as the international cooperation with partner organizations comprised the main events of the exercise. Students acquire the necessary knowledge for the performance of these tasks throughout their training and the preparation phase of the exercise. Incoming groups from invited international partner institutions participate in the exercise, contributors, and spectators.

Countless alerts have been sent from the Visegrad Mountains, Gödöllő Hills to the Disaster Management and the Hungarian National Police. According to these reports, the falling tree branches have also cut the power lines and have damaged many electric posts, hence in some places electric power supply has stalled or ceased. Professional and volunteer firefighters of the county and the local governments are working in Gödöllő, Balassagyarmat, Vác, and Rétság as well as at various places along connecting roads. The units continuously arrive at the areas of damage and work on the recovery. On Main Road 21, a tree has fallen on the overpass thereby blocking the traffic. The M3 Highway has a big car accident; more than 15 cars have had a serious accident. According to the announcement, there is an increased risk of accidents on the roads in the Mátra Mountains in the evening and at the night; therefore citizens are requested not to set forth.

The involved organizations are dealing with disaster management: fire departments, industry safety, operational services of disaster management; police (public transport, public order, public security); defense forces (peace support forces, operators of the defense forces' technical equipment); national/county/local headquarters of prison service; National Medical

274 Gábor Kovács the problem solving management process and the best practise of the national university of public service in: ghiță bărsan, gheorge udeanu, vasile căruțașu (szerk.) the complex physiognomy of the international security environments. 251 p. sibiu: "Nicolae Balcescu" land forces academy, 2015. pp. 104-113.(isbn:978-973-153-215-8)

Officer; National Veterinary Officer; organizations on private security; charity and social organizations; local services of the National Ambulance Service; National Metrological Service; General Directorate of Water Management; National Transport Authority; General Environmental, Nature Conservational and Water Inspectorate; Office of Migration and Nationality; civil and national security services; National Tax and Customs Administration; National Institute for Environment.

5.1. The main components of the exercise

5.1.1. Law enforcement, public administration and international component

The students primarily take the roles of the leaders and officers of organizations responsible for the fulfilment of tasks at national, county and especially local levels[275]; the members of organizations consisting of officers/officials delegated by cooperative and potentially involved organs. Each participating organization fulfils the tasks in accordance with its respective competences, and realizes the appropriate leadership and directorship[276.] The contact groups and staffs comprising students with law enforcement specialization will perform tasks in practice as well.[277]

Due to the large number of participants (approximately 900 students, 100 teachers and staff), it is preferred to duplicate the exercising organizations of the regional/local level. Throughout the exercise, there will be two organizations operating parallel, with the same structure and system of tasks. In accordance with the initial situation, the complex exercise will take place in the designated areas of Hungary (Balassagyarmat and surroundings, Nógrád and Pest County) as well as in Slovakia, in areas near the border with Hungary.

As part of the international aspect of the workshop, students of the Faculty of International and European Studies as well as participants delegated from the respective institutions in neighboring countries will act as organizations fulfilling the tasks of the relevant countries' respective ministries of foreign affairs. International students and their companions will be observers within the staffs of their respective public service professions.

5.1.2. Defense component

The activities of the defence forces during peacetime are highly limited. Despite this fact, the defence forces cooperate with law enforcement and public administration bodies by fulfilling partial tasks during the emergency situation. Due to the extreme weather conditions, the deployment of the defence forces is expected to be necessary. The exercise includes the preparation for the tasks to be fulfilled in states of emergency, and the modelling of tasks to be performed by the defence forces (security and of technical equipment, winter maintenance and the participation in rescue missions)

---

[275] Kovacs (2014). *The police staff's management practice.* 225 p. Budapest: Hungarian Association of Police Science, *pp. 141-151.*(ISBN:9786155305511)

[276] Kovacs-Schweickhardt (2014). Organization and management system of law enforcement agencies Budapest: National University of Public Service, pp. 17-56. (ISBN:978-615-5305-79-5)

[277] Kovacs-Horvath (2014). Management and organization theory of law enforcement agencies. 240 p Budapest: National University of Public Service, pp. 57-92. (ISBN:9786155305412)

5.2. The main phases of conducting the exercise

The Zero Phase

Substance: Tasks performed during peacetime. Issues dealt with: reports of domestic and international meteorological services; fine-tuning of local resources; activity of national and county organizations; fine-tuning of preparedness plans.

The 1st Phase

Substance: Tasks related to states of emergency

Issues dealt with: holding professional and staff orientations; proposal of the Interdepartmental Committee on Disaster Management to the Government on the declaration of the state of emergency; introducing the bill to Parliament, decision-making and formation of decree; the Government of Hungary declares the state of emergency in the territory of Nógrád and Pest counties; meetings of the Interdepartmental Committee on Disaster Management.

The 2nd Phase

Substance: Tasks related to states of emergency

Issues dealt with: performing the preparation (and preparation related tasks) of the appointed forces; continuous introduction of the dynamic impacts; leading the tasks of public administration in the state of emergency; proposing international cooperation related to the areas on the border; performing law enforcement tasks, evacuation of penitentiaries and jails.

3rd Phase

Substance: Performance of tasks, leadership in dynamic situations

Issues dealt with leading public administration tasks in state of emergency; realizing international cooperation in relation to the settlements and areas near the state border; performing law enforcement activity; performing tasks of recovery from the consequences disaster.

4th Phase

Substance: Returning to peacetime

Issues dealt with staff orientation on the changes in the weather conditions and on the new situation; preparing the necessary steps for the system of public administration; returning the organizations into normal state; collecting official documents, concluding the exercise.

The exercise applies a dual chronology – real-time and operational time. For the sake of performance, the participants of the exercise fulfil the tasks according to “operational time”. The various events follow each other with various timeframes.

5.3. The goals and values of the university common public service exercise

The common public service exercise is an important event in the life of NUPS. The goals of the Common University Public Service Exercise are:

- Contribution to the harmonization of the various sub-systems in public service approach.
- Establishment of the consonance and communality training system of the university.
- Students (full-time and Bachelor level students as well as final year Master students in military and law enforcement training) gaining experience (civil students gaining knowledge) regarding fulfilment of complex professional tasks within integrated operative staffs.
- Students' practicing leading functions and staff work while carrying out certain tasks in practice. The utilization of theoretical knowledge on leadership training in practice, the development of leadership competences.
- The new element is the workshop for the invited international participants. The workshop also serves as an excellent opportunity to harmonize the cooperation of law enforcement, defense forces and public administration organizations during states of emergency. In the light of internationalization, realizing the exercise with the involvement of students and lecturers from international educational institutes. International students delegated from partner institutions as well as invited colleagues from international partners will – by sending country – present the system of activities aimed at solving problematic situations in the given scenario.
- The enhancement of the relationship between the university training and the timely tasks and activities of public service organizations, as well as the application of new methods in the training. The mutual utilization of the lessons learned, joint development of the approved plans, operating systems and procedures in both theory and practice.
- Strengthening links between the different faculties and professions for the university students, the common work and cooperation. Application of new theoretical and practical methods in different situations. Contribution to the harmonization of the different subsystems, the unified view of the common public service sector.
- The application of theoretical and practical knowledge of the management and organization science in practice. The development of the leadership competence of the different university students. The joint application of military, law enforcement and civil support management and information systems.
- During the cooperation process, the common utilization of the new experience. The implementation of approved plans, improving the operating systems and procedures in theory and in practice.
- Common Public Service Exercise is a kind of commitment to the harmony and interdependence of university training system. The material produced by participating nations as well as the own realization will serve as a basis for a comparative study that will be applicable during the future preparation of students at NUPS and for the modernization of current domestic procedures.

6. SOME EXPERIENCE OF THE COMMON PUBLIC SERVICE EXERCISES

Some experience in the preparation part:

- The preparation of the exercise should start before November. It is necessary to launch a conference on the Exercise at the end of September. At the beginning, a basic mission is needed to be prepared, and then it is necessary to prepare the detailed missions for each profession.
- The two days' exercise is necessary, the first day serves as the day of the preparation – the technical connection (internet, radio, telephone) is vital between the different workplaces.
- During the exercise there's no need to demonstrate the organizations at national level because the students are not able to handle the decision making process at this level.
- The preparation lessons are very useful for the participants; however, not only the students but also all the teachers involved in the exercise should take part in these lessons.
- If it is possible, the students have to go to the scene of the activity, in order to study the present situation (landscape, forests, rivers, mountains etc.) and the effects of different decisions.
- The conduct of the exercise:
- All of the main activities must be divided: the students must know the main steps of the exercise. Very often jumps in time are necessary. Not too many different situations are needed, it is necessary to finalize the leading process.
- One part of the exercise must be the international press conference. The leaders prepare the press conference in Hungarian and in English languages.
- Some positions were not necessary – for example a 'veterinarian' – the umpires can play this role.

The activity of the students:

- The parallel leading level system is useful. All the working groups do their own work during the exercise.
- 8-10 students in one working group is too many, one working group has to consist of maximum 4-5 students.
- All of the information must be taken simultaneously when some events happen in real situations (fax, e-mail, telephone, letter, etc.).
- The activity of the teachers:
- The preparation group must pay attention to the information flow between the groups. The basic scenario and the additional scenario must be built on each other.
- The teachers must take part in the whole preparation event, the accurate and profound preparation is necessary to make the exercise successful.
- The supervisor teachers must evaluate the performance of the students –an evaluation form before the exercise needs to be prepared.

The logistic support:

- Someone must be appointed responsible for the entire logistic support of the exercise.
- The budget is approximately € 1000. The staff needs the following items: T-shirts in different colors (the students who have a uniform for being a career officer wear their uniform, however, it is necessary to recognize the different civilian groups.)
- Lunch for the staff and the students, cold beverages, and buffet are needed.

The communication:

- Someone must be appointed responsible for the technical equipment, the internet and intranet connection, the projectors, the laptops are vital for the success of the exercise.
- The video conference system worked efficiently during the exercises, the satellite system was useful. A special email inbox has to be created for the exercise. The special knowledge basis and all the training material have to be made available digitally, a digital event log is necessary for the students and teachers.
- It is necessary to appoint a person who is responsible for the communication. The local media must be invited.

Others:

- The final evaluation report is necessary as soon as possible.
- Students, except for the military cadets, had problems with working with paper-based maps. Applying foil is effective.

7. CONCLUSIONS

The structure of NUPS is special, to train the future military, law enforcement and public service experts in basic, master and PhD level in one organization. The colleagues of NUPS have been working effectively in the past five years. The Hungarian military, law enforcement and public service organizations are satisfied with the graduated university students in bachelor and master level.

The special module – Common Public Service Module provides common knowledge for all the university students during the bachelor education. This knowledge is necessary for the well-organized work of the future experts. The Common Public Service Exercise is a vital part of the bachelor education. It helps the teachers to provide practice oriented education. During the exercise, the teachers realize the strengths and the weaknesses of the education process; they can effectively improve the curriculum and the training methods. They have a direct impression of the students' works. It helps the students, because they use their theoretical knowledge in order to solve the different practical problems.

During the common exercise the ability of the communication, the cooperation and coordination of the students are evolving. In the different positions, the students' work together; during the teamwork, they realize the different problems and they find the common solutions.

This knowledge is necessary for the well-organized work of the future experts. The planning, organizing and leading of the exercises were smooth; the experiences were useful and acceptable for the public service organizations.

According to the best Hungarian practice, the staff of NUPS is ready to invite some foreign university teachers and students in order to collect deep impression for the Common Public Exercise.

REFERENCES

Act CXXXII of 2011 on the National University of Public Service (2016). http://en.uni-nke.hu/uploads/media_items/nups-academic-and-examination-regulations.original.pdf (retrieved 12/03/2016)

Common Core Curriculum Master Education (2013). NUPS Faculty of Law Enforcement. Budapest: Law Enforcement Management Theory Department.

Varga, J. (2010). Some relationship between border security, public safety, public security and personal safety In: Kunovská, E. (ed.). *Police Theory and Practice*. Bratislava: Akadémia Policajného zboru, pp. 135-142.

„International Perspectives on Police Education and Training." Editor: Perry Stanislas, Pulitzer: Routledge Taylor and Francis Group, 2014. London, Chapter 11., Fórizs: Police training and education in Hungary, p. 175-192. ISBN: 978-0-415-63218-8 (hbk), ISBN: 978-0-203-09589-8 (ebk).

Czuprak Otto, Kovacs Gabor: *Management and Organization Theory*, Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., 2013. *326 p.*(ISBN:978-615-5344-36-7)

*Common Core Curriculum Bachelor Education NUPS Faculty of Law Enforcement (*2013). Budapest: Law Enforcement Management Theory Department.

Kovacs, G. (2015). The new challenges and approach at the law enforcement master education programme at the National University of Public Service. In: Butorac, K. *4th International Scientific and Professional Conference: Police College Research Days.* Zagreb: Ministry of the Interior of the Republic of Croatia, Police Academy, pp. 226-239.

Kovács, G. (2015). The Problem Solving Management Process and the Best Practise of the National University of Public Service. In: Bărsan, G., Udeanu, G., Căruțaşu, V. (ed.) *The Complex Physiognomy of the International Security Environments*. Sibiu: "Nicolae Balcescu" Land Forces Academy, pp. 104-113.

Kovacs, G. (2014). *The police staff's management practice.* Budapest: Hungarian Association of Police Science.

Kovacs, G., Schweickhardt, G. (2014). *Organization and management system of law enforcement agencies.* Budapest: National University of Public Service.

Kovacs, J., Horvath, G. (2014). *Management and organization theory of law enforcement agencies.* Budapest: National University of Public Service.

IZVORNI ZNANSTVENI RAD

Ivica Labazan[278]
Ivančica Varjačić[279]
Joško Sindik[280]
Martin Kolonić[281]
Dejan Pastorčić[282]

STAVOVI POLICIJSKIH SLUŽBENIKA – STUDENATA O STRUČNOSTI, KONTROLI, ODLUČIVANJU I RUKOVODITELJIMA

Sažetak

U ispitivanju stavova policijskih službenika – studenata o svojoj pripremljenosti za poslove koje obavljaju, količini odluka koje samostalno donose i njihovoj važnosti, učestalosti kontrola od nadređenih te o karakteristikama rukovoditelja, prigodni uzorak sačinjavalo je 76 (od mogućih 91) studenata druge godine specijalističkog diplomskog stručnog studija Kriminalistika, Visoke policijske škole u Zagrebu, upisanih na taj studij 2010. godine. Konstruirani je upitnik stavova pokazao zadovoljavajuće metrijske karakteristike. Opći ciljevi istraživanja bili su ispitati stavove studenata vezane uz vlastitu pripremljenost za poslove koje obavljaju te poželjnost zaštitničkog stava rukovoditelja, kao i o količini i stupnju važnosti odluka koje ispitanici samostalno donose i podatke o učestalosti kontrola od nadređenih. Problemi istraživanja bili su utvrditi postoje li razlike u stavovima studenata s obzirom na: spol, dob i godine radnog staža. Nakon provedenog istraživanja možemo konstatirati da s obzirom na na spol, dob i godine staža (nezavisne varijable) policijskih službenika – studenata nisu utvrđene značajne razlike prema niti jednoj od ispitivanih zavisnih varijabli.

Ključne riječi: *pripremljenost, odlučivanje, samostalnost, važnost odluka, dobar rukovoditelj.*

---

[278] Ivica Labazan, bacc. crim., viši stručni referent, Područni carinski ured Zagreb.
[279] Ivančica Varjačić, bacc. crim., policijski službenik za obradu kriminaliteta, PU zagrebačka.
[280] dr. sc. Joško Sindik, znanstveni suradnik, Institut za antropologiju, Zagreb.
[281] Martin Kolonić, stuč. spec. crim., policijski službenik za aerodromsku policiju i graničnu kontrolu u zračnim lukama, Ravnateljstvo policije, Uprava za granicu, Služba pomorske i aerodromske policije.
[282] Dejan Pastorčić, struč. spec. crim., pomoćnik načelnika PP za policiju, PU sisačko-moslavačka, PP Dvor.

1. UVOD

Posebnosti poslova policijskog službenika

Policijski posao[283] zakonski je reguliran i određen Zakonom o policijskim poslovima i ovlastima i drugim zakonima, a obavlja se primjenom policijskih ovlasti. Policijski poslovi su posebni u odnosu na ostale vrste poslova koje obavljaju državni službenici, a specifičnost se odražava u više karakteristika, od kojih je možda najznačajnija ovlast primjene sredstava prisile prema drugim osobama (uključujući i vatreno oružje) te ograničavanje slobode kretanja ljudi (uhićenje, zadržavanje). Posebnost poslova se ogleda i u činjenici da to javnost uvijek zanima, ali na neformalni način i nadzire primjenu policijskih ovlasti kojima se nerijetko zadire u osobna prava i slobode čovjeka i građanina. Ovisno o sredini u kojoj radi te opisa poslova koje ima u nadležnosti, policijski službenik je izložen nadzoru i kritici javnosti i kada je u službi i kada je izvan službe. Naglasak je uvijek na društvenoj i socijalnoj ulozi koju ima policijski službenik u određenoj sredini (radnoj organizaciji, obiteljskom i socijalnom okruženju) te se pred njega postavlja zadatak da svoje ponašanje u službi i izvan službe prilagodi društveno prihvatljivim, ali i očekivanim normama ponašanja. Posebnost policijskih poslova se ogleda i u tome što su policijski službenici uvijek obvezni i dužni vršiti stručnu edukaciju i održavati razinu znanja potrebnog za obavljanje policijskih poslova, uz korak sa svakodnevnom i učestalom promjenom zakonske regulative kojom se uređuje obavljanje policijskih poslova i primjena policijskih ovlasti.

Glavina i Vukosav (2011) navode da su policijski službenici izloženi stresorima vezanim uz prirodu posla (uporaba sile, donošenje kritičnih odluka, prisustvovanje raznim oblicima nasilja itd.), interpersonalnim stresorima, organizacijskim stresorima (smjenski rad, rad vikendom i praznicima, male plaće, loši odnosi s nadređenima, opremljenost za rad itd.) i obiteljskim stresorima odnosno loši odnosi u obitelji zbog policijskog posla[284].

Menadžment u policiji

Orlović i Pušeljić (2010) navode kako je bit menadžerstva upravljanje organizacijama i sustavima na način da se zajednički i koordinirano postignu unaprijed razrađeni ciljevi. Između policijskih službenika prevladava mišljenje kako značajan i pretežiti udio stresa u obavljanju policijskih poslova predstavlja odnos rukovoditelja prema niže rangiranom službeniku i međusobna komunikacija te način svakodnevnog ophođenja. Menadžeri nisu samo rukovoditelji i njihova uloga je nešto šira u odnosu na postojeći sustav i rukovoditelje u policijskoj hijerarhiji. Policijski menadžment predstavlja uvođenje novog sustava vrijednosti unutar policijske organizacije, gdje menadžer preuzima ulogu vođe (prvi među jednakima) te se mijenja kompletna strategija odnosa unutar organizacije, ali i između organizacije i javnosti.

Jedan od primarnih ciljeva menadžmenta u policiji bi bio uspostava takvih odnosa gdje bi došlo do optimalnog korištenja ljudskih potencijala te svrhovitog i učinkovitog upravljanja organizacijom, kako bi se postigao pozitivan učinak na sve zaposlenika (porast motivacije za

[283] Zakon o policijskim poslovima i ovlastima, Narodne novine 76/2009.
[284] Vidi detaljnije u: Glavina, I., Vukosav, J. *Stres u policijskoj profesiji.* Policija i sigurnost. (20)1:32-44.

obavljanje policijskih poslova, smanjenje razine stresa koji dopire iz organizacije, porast učinkovitosti i ekonomičnosti u radu državne uprave – javnih službenika).

Donošenje odluka

Policijski službenici nerijetko moraju donositi odluke kojima se zadire u nečija prava i tada se subjektivni osjećaj građana (izazvan tom odlukom) u određenoj mjeri reflektira i prenosi na policijskog službenika koji je takvu odluku i donio. Za ispravno i zakonito donošenje odluka policijski službenici moraju biti stručno osposobljeni i educirani, kako bi se izbjegao negativni učinak pogrešne odluke i moguće sankcije za nju. Koliko se policijski službenici smatraju osposobljenima za poslove koje obavljaju, pitanje je čiji odgovor ovisi o više objektivnih i subjektivnih faktora. Međutim, ponekad subjektivni osjećaj nadilazi objektivne okolnosti i argumente te se nerijetko precjenjuje razina vlastite osposobljenosti za donošenje odluka. Sadašnji sustav poznaje i oslanja se na hijerarhijsku strukturu i odnose subordinacije, što ponekad znatno otežava donošenje odluka i samostalnost prilikom primjene policijskih ovlasti. Proces donošenja odluka mora se zasnivati na jasno postavljenim odnosima i kriterijima te mora postojati interni sustav procjene učinkovitosti i analize pojedinih odluka, a posebice onih koje su odnose na temeljna prava i slobode.

Utjecaj rukovoditelja

Cajner Mraović (2009) i Cajner, Faber i Volarević (2003) navode kako se policijski rukovoditelji nalaze u situaciji vrlo teškog izbora. Naime u opisanim okolnostima oni se mogu odrediti da ništa ne mijenjaju u načinu rada što ih, s jedne strane lišava izlaganja novim rizicima, ali s druge strane, postupno vodi u daljnje pogoršavanje stanja. Utjecaj rukovoditelja na međusobne odnose u policijskoj organizaciji je iznimno velik, ovisno o strukturi organizacije i njegovom položaju. Taj bi utjecaj trebao biti pozitivan na učinkovitost u obavljanju policijskih poslova, ali i međusobne odnose između zaposlenika. Rukovoditelji moraju imati svijest o tome da je njihov utjecaj na radnu kvalitetu službenika značajan i predstavlja uteg s kojim treba vješto "balansirati" između zadovoljavanja potrebe za učinkovitošću i potrebe da se u tome zadovolje pojedinačni interesi i stavovi pojedinca u toj organizaciji. Novim Zakonom o policiji [285] uvedena je obveza stručnog osposobljavanja rukovoditelja za poslove rukovođenja u policijskoj organizaciji, što je značajan iskorak u odnosu na prethodno zakonsko uređenje i radno-pravni status rukovoditelja u policijskoj organizaciji.

Opći ciljevi istraživanja bili su ispitati stavove studenata vezane uz vlastitu pripremljenost za poslove koje obavljaju. koje su poželjne karakteristike rukovoditelja i o količini i stupnju važnosti odluka koje ispitanici samostalno donose te podatke o učestalosti kontrola od nadređenih. U skladu s općim ciljevima, formulirali smo i konkretnije sljedeće probleme istraživanja te pripadne hipoteze:

Istraživački problemi:

1. Utvrditi deskriptivne karakteristike (aritmetička sredina, standardno raspršenje, normalitet distribucije) za glavne (zavisne) varijable istraživanja.

[285] Zakon o policiji je donesen 11. ožujka 2011.

2. Utvrditi povezanost između svih glavnih varijabli istraživanja.

Pretpostavljeno je da postoji pozitivna povezanost između radnog iskustva i pojedinih karakteristika posla koja se odnose na samostalnost donošenja odluka te da postoji pozitivna povezanost između pojedinih karakteristika posla koje se odnose na samostalnost donošenja odluka (prve dvije hipoteze).

1. Utvrditi postoje li spolne razlike između svih glavnih varijabli istraživanja.

Pretpostavljeno je da ne postoje spolne razlike koje se odnose na samostalnost donošenja odluka niti koje se odnose na stav ispitanika o poželjnim karakteristikama rukovoditelja, niti u učestalosti kontrole, a također niti u važnosti donesenih odluka (treća hipoteza).

Ciljevi istraživanja su sljedeći:

1. Utvrditi postoje li razlike između svih glavnih varijabli istraživanja u odnosu na dobnu skupinu (stariji mlađi).
2. Utvrditi postoje li razlike u duljini radnog staža između svih glavnih varijabli istraživanja.

Pretpostavljeno je da postoje razlike prema zavisnoj varijabli duljina radnog staža u odnosu na adekvatnu pripremljenost za poslove koje obavljaju, u smislu bolje pripremljenosti kod radno iskusnijih djelatnika (peta hipoteza).

2. METODA

2.1. Ispitanici

U istraživanju je ispitan prigodni uzorak studenata Visoke policijske škole u Zagrebu, II. godine specijalističkog diplomskog stručnog studija Kriminalistika. Ukupan broj ispitanika koji su sudjelovali u istraživanju je 76, od kojih je 58 studenata i 18 studentica službenika Ministarstva unutarnjih poslova. Za potrebe analize razlika kreirane su dihotomne varijable dobna grupa te radno-iskustvena grupa (s po 38 ispitanika), na temelju medijana za dob (stariji=2 / mlađi=1) odnosno radno iskustvo (iskusniji=2 / neiskusniji=1).

2.2. Instrumentarij

U ovom istraživanju primijenjen je upitnik (Pušeljić, 2011.)[286] iz kojeg smo koristili samo ciljano određena pitanja potrebna za ovo istraživanje.

I. Dio ankete sadrži opće podatke o ispitaniku, i to varijable: *spol* (muški=1 ili ženski=2), kontinuiranu varijablu *dob* (svaki ispitanik odgovarajućom brojkom navodi svoje godine), kontinuiranu varijablu *godine staža u policiji* (svaki ispitanik odgovarajućom brojkom navodi svoje godine radnog staža u policiji).

II. Dio ankete se sastoji od 5 pitanja:

a) ***Adekvatna pripremljenost za posao.*** Rezultat na ovoj skali daje nam subjektivni dojam ispitanika o pripremljenosti za posao koji obavlja. Sastoji se od pitanja: "Smatrate li se adekvatno pripremljenim za posao koji obavljate?", na koje

[286] Upitnik iz područja organizacije i menadžmenta, Visoka policijska škola – neobjavljeni.

ispitanik odgovara zaokruživanjem odgovarajućeg slova na skali Likertovog tipa sa 4 stupnja (a – uopće nisam pripremljen/a=1, b – nedovoljno sam pripremljen/a=2, c – djelomično sam pripremljen/a=3, d – da, potpuno sam pripremljen/a=4).

b) ***Samostalnost u donošenju odluka.*** Rezultat na ovoj skali mjeri samostalnost ispitanika u donošenju odluka u poslu koji obavlja. Sastoji se od pitanja: "Koliko odluka povezanih s obavljanjem poslova donosite samostalno, bez konzultacija s nadređenim rukovoditeljem?", na koje ispitanik odgovara zaokruživanjem odgovarajućeg slova na skali Likertovog tipa sa 4 stupnja (a – niti jednu odluku ne mogu donijeti samostalno=1, b – malo odluka donosim samostalno=2, c – odlučujem sam/a, a samo u rijetkom slučajevima se konzultiram s nadređenim=3, d – isključivo samostalno donosim odluke=4).

c) ***Važnost odluka koje ispitanici u obavljanju svojeg posla samostalno donose.*** Sastoji se od pitanja: "Kakva je važnost odluka u taktičkom i operativnom smislu koje samostalno donosite?", na koje ispitanik odgovara zaokruživanjem odgovarajućeg slova na skali Likertovog tipa sa 3 stupnja (a – radi se uglavnom o nevažnim odlukama=1, b – radi se o odlukama manje važnosti koje su operativne naravi=2, c – radi se o odlukama čija je važnost taktičke i operativne naravi=3).

d) ***Izloženost kontroli nad ispitanicima u obavljanju svojeg posla.*** Rezultat na ovoj skali mjeri izloženost ispitanika kontroli u poslu. Sastoji se od pitanja: "Koliko ste često izloženi kontroliranju nadređenih?", na koje ispitanik odgovara zaokruživanjem odgovarajućeg slova na skali Likertovog tipa sa 3 stupnja (a – nisam podložan kontroli=1, b – kontrole su povremene i rijetke=2, c – kontrole su česte i stalne=3).

e) ***Subjektivni doživljaj podrške rukovoditelja.*** Rezultat na ovoj skali mjeri subjektivni doživljaj o tome smatraju li ispitanici da je dobar rukovoditelj onaj koji će zaštiti svoje suradnike. Sastoji se od pitanja: "Dobar rukovoditelj u svakoj prilici će svojim autoritetom i osobnošću zaštititi svoje suradnike!", na koje ispitanik odgovara zaokruživanjem odgovarajućeg slova na skali Likertovog tipa sa 5 stupnja (a – uopće se ne slažem=1, b – uglavnom se ne slažem=2, c – nisam siguran=3, d – uglavnom se slažem=4, e – potpuno se slažem=5).

2.3. Postupak

Ispitanicima je dana uputa da se radi o anonimnoj anketi čiji će rezultati biti korišteni isključivo za pisanje seminarskog rada te se mole da iskreno odgovaraju na navedena pitanja. Dobiveni podaci su obrađeni računalno – statističkim programom IBM SPSS – verzija 10.0. Uz deskriptivnu statistiku koristili smo Spearmanov koeficijent korelacije te Mann Whitney U test za testiranje razlika između dva nezavisna uzorka (Petz, 1994).

3. REZULTATI I RASPRAVA

U **tablici 1** dani su deskriptivni podaci o rezultatima istraživanja. Prosječna dob ispitanika je 33,5 godina, s time da najmlađi ispitanik ima 27, dok je najstariji starosti 52 godine. Prosječne godine radnog staža ispitanika su 10,9 godina, a minimalno 4 godine i maksimalno 32 godine radnog staža. Veći dio ispitanika smatra da je adekvatno pripremljen za posao koji obavljaju te da su samostalni u donošenju odluka u obavljanju posla koje su po svojoj važnosti manje važne i operativnog karaktera. Izloženost kontroli ispitanika od strane rukovoditelja je većinom povremena i rijetka te ispitanici smatraju da će dobar rukovoditelj uvijek zaštiti svoje suradnike. Od normalne distribucije statistički značajno odstupaju rezultati za sve varijable, s asimetrijom prema većim vrijednostima. Uočljivo je da je posljednja tvrdnja (koja se odnosi na mišljenje ispitanika o poželjnim karakteristikama rukovoditelja) izrazito malo diskriminativna jer je prosječni rezultat previsok, što se kasnije reflektiralo i na nepostojanje statističkih značajnih razlika u odnosu na sve nezavisne varijable u istraživanju. Ovo bi pitanje u budućim istraživanjima trebalo preformulirati ili ga parcijalizirati i pretvoriti u dva ili više pitanja kojima ćemo pogoditi u "srž" problematike.

Tablica 1: Deskriptivna statistika upitnika stavova studenata

	Minimum	Maximum	Aritmetička sredina	Standardno raspršenje	Kolmogorov-Smirnov Z	Značajnost
Dob	27,00	52,00	33,553	4,533	1,570	p<0,05
Radni staž	4,00	32,00	10,921	5,706	1,412	p<0,05
Smatrate li se adekvatno pripremljenim/nom za poslove koje obavljate	1,00	4,00	3,500	0,663	3,081	p<0,01
Koliko odluka povezanih s obavljanjem poslova donosite samostalno, bez konzultacija s nadređenim rukovoditeljem	1,00	4,00	2,645	0,534	3,415	p<0,01
Kakva je važnost odluka u taktičkom i operativnom smislu koje samostalno donosite	1,00	3,00	2,382	0,610	2,545	p<0,01
Koliko ste često izloženi kontroliranju nadređenih	1,00	3,00	2,408	0,570	2,751	p<0,01
Dobar rukovoditelj u svakoj prilici će svojim autoritetom i osobnošću zaštititi svoje suradnike	1,00	5,00	4,250	0,569	3,087	p<0,01

Legenda: Kolmogorov-Smirnov Z= test normaliteta distribucije

U **tablici 2** prikazane su međusobne korelacije varijabli upitnika. Od ukupnog broja korelacija (21), statistički značajnih je pet i sve su bile pozitivnog smjera. Statistički značajne korelacije pronađene su između nezavisnih varijabli životna dob i godine radnog staža,

između nezavisne varijable duljina radnog staža i zavisne varijable adekvatna pripremljenost za posao. Kod zavisnih varijabli, međusobno su pronađene statistički značajne korelacije između adekvatne pripremljenosti za posao i samostalnog odlučivanja te važnosti donesenih odluka i na kraju, postoji statistički značajna korelacija i između samostalnosti odlučivanja i stupnja važnosti donesenih odluka.

Tablica 2: Međusobne korelacije kontinuiranih varijabli upitnika (zavisnih i nezavisnih)

Varijable	Dob	Radni staž	Smatrate li se adekvatno pripremljenim/nom za poslove koje obavljate	Koliko odluka povezanih s obavljanjem poslova donosite samostalno, bez konzultacija s nadređenim rukovoditeljem	Kakva je važnost odluka u taktičkom i operativnom smislu koje samostalno donosite	Koliko ste često izloženi kontroliranju nadređenih	Dobar rukovoditelj u svakoj prilici će svojim autoritetom i osobnošću zaštititi svoje suradnike
Dob	1	,685**	,115	,005	,000	,072	-,147
Radni staž		1	,278*	,104	,158	-,064	-,055
Smatrate li se adekvatno pripremljenim/nom za poslove koje obavljate			1	,357**	,313**	-,123	-,053
Koliko odluka povezanih s obavljanjem poslova donosite samostalno, bez konzultacija s nadređenim rukovoditeljem				1	,421**	-,087	-,099
Kakva je važnost odluka u taktičkom i operativnom smislu koje samostalno donosite					1	-,185	,029
Koliko ste često izloženi kontroliranju nadređenih						1	,093
Dobar rukovoditelj u svakoj prilici će svojim autoritetom i osobnošću zaštititi svoje suradnike							1

*** korelacija je značajna uz p<0.01 (2-smjerno);*
** korelacija je značajna uz p<0.05 (2-smjerno)*

U **tablici 3** prikazane su razlike u odnosu na varijablu spol te dobiveni rezultati pokazuju da od svih varijabli postoji značajna razlika jedino u varijabli staž.

Tablica 3: Razlike u stavovima u odnosu na varijablu spol

	SPOL	Aritmetička sredina	Standardno raspršenje	Mann Whitney U test (p)
Kronološka dob	muškarci (58)	33,690	4,477	p>0,20
	žene(18)	33,111	4,812	
Duljina radnog staža	muškarci(58)	12,190	5,430	**p<0,01**
	žene(18)	6,833	4,643	
Smatrate li se adekvatno pripremljenim/nom za poslove koje obavljate	muškarci (58)	3,535	0,558	p>0,20
	žene (18)	3,389	0,762	
Koliko odluka povezanih s obavljanjem poslova donosite samostalno, bez konzultacija s nadređenim rukovoditeljem	muškarci (58)	2,672	0,534	p>0,20
	žene (18)	2,556	0,541	
Kakva je važnost odluka u taktičkom i operativnom smislu koje samostalno donosite	muškarci (58)	2,431	0,565	p>0,20
	žene (18)	2,222	0,732	
Koliko ste često izloženi kontroliranju nadređenih	muškarci (58)	2,362	0,541	p>0,20
	žene (18)	2,556	0,602	
Dobar rukovoditelj u svakoj prilici će svojim autoritetom i osobnošću zaštititi svoje suradnike	muškarci (58)	4,293	0,554	p>0,20
	žene (18)	4,111	0,590	

U **tablici 4** prikazane su razlike u odnosu na varijablu dob, iz čega je vidljivo da ne postoji statistički značajna razlika ni u jednoj varijabli u odnosu na dob ispitanika, što je vjerojatno zbog velike homogenosti uzorka ispitanika (ne postoje velike međusobne razlike u starosnoj dobi).

Tablica 4: Razlike u stavovima u odnosu na varijablu dobna skupina

Zavisne varijable	Dob	Aritmetička sredina	Standardno raspršenje	Mann Whitney U test (p)
Smatrate li se adekvatno pripremljenim/nom za poslove koje obavljate	mlađi (38)	3,500	0,558	p>0,20
	stariji (38)	3,500	0,762	
Koliko odluka povezanih sa obavljanjem poslova donosite samostalno, bez konzultacija s nadređenim rukovoditeljem	mlađi (38)	2,658	0,534	p>0,20
	stariji (38)	2,632	0,541	
Kakva je važnost odluka u taktičkom i operativnom smislu koje samostalno donosite	mlađi (38)	2,316	0,574	p>0,20
	stariji (38)	2,447	0,645	
Koliko ste često izloženi kontroliranju nadređenih	mlađi (38)	2,368	0,541	p>0,20
	stariji (38)	2,447	0,602	
Dobar rukovoditelj u svakoj prilici će svojim autoritetom i osobnošću zaštititi svoje suradnike	mlađi (38)	4,263	0,554	p>0,20
	stariji (38)	4,237	0,590	

U **tablici 5** prikazane su razlike u varijabli radnog staža ispitanika iz čega je vidljivo da je statistički značajna razlika samo u odnosu na adekvatnu pripremljenost za posao, a s obzirom na to da se radi o sličnim karakteristikama posla koji obavljaju ispitanici bitan faktor stoga je i radni staž, tako da se ispitanici s kratkotrajnijim radnim stažom (manjim od 10 godina) smatraju manje pripremljenijim za posao koji obavljaju. U odnosu na druge rezultate koji odstupaju moguće je da je zbog drugačijeg posla koji obavljaju.

Tablica 5: Razlike u stavovima u odnosu na varijablu radnog staža

Zavisne varijable	Staž	Aritmetička sredina	Standardno raspršenje	Mann Whitney U test (p)
Smatrate li se adekvatno pripremljenim/nom za poslove koje obavljate	kratkotrajniji (35)	3,257	0,741	**p<0,01**
	dugotrajniji (41)	3,707	0,512	
Koliko odluka povezanih s obavljanjem poslova donosite samostalno, bez konzultacija s nadređenim rukovoditeljem	kratkotrajniji (35)	2,571	0,608	p>0,20
	dugotrajniji (41)	2,707	0,461	
Kakva je važnost odluka u taktičkom i operativnom smislu koje samostalno donosite	kratkotrajniji (35)	2,257	0,657	p>0,10
	dugotrajniji (41)	2,488	0,553	
Koliko ste često izloženi kontroliranju nadređenih	kratkotrajniji (35)	2,429	0,608	p>0,20
	dugotrajniji (41)	2,390	0,542	
Dobar rukovoditelj u svakoj prilici će svojim autoritetom i osobnošću zaštititi svoje suradnike	kratkotrajniji (35)	4,257	0,561	p>0,20
	dugotrajniji (41)	4,244	0,582	

Kad sagledamo odnose između zavisnih i nezavisnih varijabli, vidimo da u većini slučajeva nismo pronašli razlike u zavisnim varijablama u odnosu na nezavisne. Jedina iznimka je postojanje razlike prema varijabli duljina radnog staža, u odnosu na adekvatnu pripremljenost, u smislu bolje pripremljenosti za obavljanje poslova kod radno iskusnijih djelatnika. Objašnjenje nepostojanja razlika u dobivenim rezultatima pripisujemo pretpostavci

da vrsta posla vjerojatno uvjetuje slične stavove prema istraživanim zavisnim varijablama bez obzira na dob i spol. Konačno, možda je riječ i o društveno poželjnom odgovaranju na upitnik (djelomično) premda je bila naglašena znanstvena svrha istraživanja (Fastić-Pajk, 2005). Kao nedostatke ovog istraživanja mogli bismo navesti premaleni i homogeni uzorak (sličnost radnog mjesta, sličnost poslova koje ispitanici obavljaju). Primjerice, kada bismo istraživali sve studente Visoke policijske škole ili sve organizacijske jedinice MUP-a, vjerojatno bismo dobili bitno drugačije rezultate. Budući da je ovo po našim saznanjima prvo istraživanje policijskih službenika takvog tipa, za buduća istraživanja predlažemo instrumente s više pitanja, korištenje većeg broja varijabli, veće i reprezentativnije uzorke, po mogućnosti slučajne te provođenje istraživanja i u drugim organizacijskim jedinicama MUP-a.

4. ZAKLJUČAK

Utvrđene su deskriptivne karakteristike (aritmetička sredina, standardno raspršenje, normalitet distribucije) za glavne varijable istraživanja. Utvrđena je povezanost između svih glavnih varijabli istraživanja i sve su pozitivnog smjera. Utvrđeno je da postoji pozitivna povezanost između radnog iskustva i pojedinih karakteristika posla koja se odnose na samostalnost donošenja odluka te da postoji pozitivna povezanost između pojedinih karakteristika posla koje se odnose na samostalnost donošenja odluka. Utvrđeno je da ne postoje spolne razlike koje se odnose na:

- vlastiti stav o pripremljenosti za poslove koje službenici i službenice obavljaju
- samostalnost donošenja odluka
- učestalost kontrola
- važnost donesenih odluka.
- stav o zaštitničkom odnosu rukovoditelja spram podređenih.

Međutim, u odnosu između nezavisnih varijabli spol i godine radnog staža, postoji statistički značajna razlika u korist muških službenika koji prosječno imaju gotovo dvostruko dulji radni staž. Pretpostavlja se da dobiveni rezultat proizlazi iz činjenice da se žene u značajnijem udjelu počinju primati u službu tek 10-ak godina unazad. Utvrđeno je da u odnosu na dobnu grupu također ne postoje razlike između glavnih varijabli istraživanja. Međutim, kao što je i pretpostavljeno, potvrđeno je da postoje razlike prema nezavisnoj varijabli duljina radnog staža u odnosu na adekvatnu pripremljenost za posao, u smislu bolje pripremljenosti za posao kod radno iskusnijih djelatnika.

LITERATURA

Cajner Mraović, I. (2009). *Prevencija kriminaliteta u lokalnoj zajednici. Strategija primjene znanosti i iskustva dobre prakse.* Zagreb: MUP RH.
Cajner, M., Faber, V., Volarević, G. (2003). *Strategija djelovanja policija u zajednici.* Zagreb: Ministarstvo unutarnjih poslova.
Fastić-Pajk, I. (2005). *Socijalno poželjno odgovaranje u različitim modalitetima prezentacija čestica i njegova povezanost s osobinama ličnosti*. Zagreb: Filozofski fakultet.
Glavina, I., Vukosav, J. (2011). *Stres u policijskoj profesiji,* Policija i sigurnost. 20 (1), 32-47.
Orlović, A., Pušeljić, M. (2010). *Operativni menadžment ljudskih potencijala (SWOT analiza policije first – line menadžera u kriminalističkoj policiji*. Policija i sigurnost 19 (1), 67-68.
Pušeljić, M. (2011). *Upitnik iz područja organizacije i menadžmenta. Radni materijal s predavanja (neobjavljen)*. Zagreb: Visoka policijska škola.
Petz, B. (1994). *Statistika za praksu*. Zagreb: Ministarstvo unutrašnjih poslova.
Zakon o policijskim poslovima i ovlastima. Narodne novine 76/09.

Ivica Labazan
Ivančica Varjačić
Joško Sindik
Martin Kolonić
Dejan Pastorčić

ATTITUDES OF POLICE OFFICERS – STUDENTS TOWARDS COMPETENCE, CONTROL, DECISION MAKING AND MANAGERS

Summary
For the examination of the attitude of police officers – students about their preparedness for the tasks they perform, the amount of decisions they make independently and about the importance of the decisions, the frequency of the control exercised by their supervisors as well as about the characteristics of their supervisors, the sample encompassed 76 (out of potentially 91) of second year students of the Specialist Graduate Professional Studies of Criminal Investigation (enrolled in 2010) at the Police College in Zagreb. The designed questionnaire about their attitude demonstrated satisfactory psychometric properties. The general objective of this study was to examine the attitudes of students regarding their own preparedness for the tasks they perform, the desirability of a protective attitude on the part of their supervisors, the amount of decisions made by respondents individually, the degree of the significance of these decisions and the data on the frequency of the control by their superiors. The challenges of the research were to determine whether there were any differences in the attitude of students with regard to gender, age or the years of service. Upon the completion of the study we may conclude that with respect to gender, age and the years of service (independent variables) of police officers - students, no significant differences by any of the examined dependent variables have been established.

Key words: *preparedness, decision-making, independence, importance of decisions, good manager.*

PRILOG

OPĆI PODACI:

SPOL : M Ž

DOB : _____

GODINE STAŽA U POLICIJI: _____

Molim Vas da pažljivo pročitate pitanje te da zaokružite samo jedan od ponuđenih odgovora.

1. Smatrate li se adekvatno pripremljenim/nom za poslove koje obavljate?

a) Uopće nisam pripremljen/a.

b) Nisam dovoljno pripremljen/a.

c) Djelomično sam pripremljen/a.

d) Da, potpuno sam pripremljen/a.

2. Koliko odluka povezanih s obavljanjem poslova donosite samostalno, bez konzultacija s nadređenim rukovoditeljem?

a) Niti jednu odluku ne mogu donijeti samostalno.

b) Malo odluka donosim samostalno.

c) Odlučujem sam/a, a samo u rijetkom slučajevima se konzultiram s nadređenim.

d) Isključivo samostalno donosim odluke.

3. Kakva je važnost odluka u taktičkom i operativnom smislu koje samostalno donosite?

a) Radi se uglavnom o nevažnim odlukama.

b) Radi se o odlukama manje važnosti, koje su operativne naravi.

c) Radi se o odlukama čija je važnost taktičke i operativne naravi.

4. Koliko ste često izloženi kontroliranju nadređenih?

a) Nisam podložan kontroli.

b) Kontrole su povremene i rijetke.

c) Kontrole su česte i stalne.

5. Dobar rukovoditelj u svakoj prilici će svojim autoritetom i osobnošću zaštititi svoje suradnike!

a) Uopće se ne slažem.

b) Uglavnom se ne slažem.

c) Nisam siguran.

d) Uglavnom se slažem.

e) Potpuno se slažem.

PROFFESIONAL PAPER

Snežana Mojsoska[287]
Nikola Dujovski[288]
Elena Dimovska[289]

CONCEPT OF E-POLICE AND E-POLICING SERVICES AS A PART OF E-GOVERNMENT: FUTURE DEVELOPMENT IN THE REPUBLIC OF MACEDONIA

Summary

In terms of globalization and the development of technology, crime takes new positions, worldwide. According to the World Bank definition, "E-government refers to the use by government agencies of information technologies (such as Wide Area Network, the Internet and mobile computing) that have the ability to transform relations with citizens, businesses and other arms of government." This paper aims at examining the role of the e-police as a segment in an e-government and its future setting up in a country. Setting up of the e-police, like a segment in an e-government has many benefits especially in the fight against crime for both parties, victims as well as police management. The e-police system is not a new concept in developed countries but it is a completely new concept in developing countries. The e-police is based on the principles of communication and coordination that will lead to an improvement in the implementation of police policy and reduction of crime rate. Macedonia does not have such a platform. The statistics show for the fact 60% improvement of the functioning of the police and in the reporting of cases. The establishment of the e-police system in the country requires a project as a future reference that would include the procurement of the software, hardware, data entry, linking system, server, training etc.

Key words: *e-government, e-policing, e-police, crime, internet.*

1. INTRODUCTION

E-Government (EG) is a permanent commitment made by government, aimed to improve the relationship between the private citizen and the public sector, through enhanced, cost-effective, and efficient delivery of services, information, and knowledge. Broadly defined, EG includes the use of all information and communication technologies, in the range from fax machines to the wireless palm pilots. EG is aimed to facilitate the daily administration of the government, exclusively as an internet-driven activity that improves citizen's access to the government information, services and expertise, in order to ensure citizen's participation in government process, and satisfaction with this process (UN & ASPA, 2004).

E-policing (EPG) is a part of e-government. It is delivering services from police to citizens, using information and communication technology. According to the European Commission,

[287] Snezana Mojsoska, Associate prof., Faculty of security, st.1 Kolonija Idrizovo no.2a, Skopje
e-mail: smojsoska@gmail.com

[288] Nikola Dujovski, Asistant prof., Faculty of security, st.1 Kolonija Idrizovo no.2a,Skopje, e-mail: smojsoska@gmail.com

[289] Elena Dimovska, Msc. Candidate, Faculty of security, st.1 Kolonija Idrizovo no.2a,Skopjee-mail: elena.dimovska90@gmail.com

there are about 20 services defined that EG has provided to the citizens. Availability of these services enables to the European Commission to evaluate and make a ranking of certain country. Measurement is made for tax personal income, social contributions (job, corporate tax, benefits from social security, VAT, personal documents, registration of a new company, submission of the vehicle data in the Statistical Office, building permits, custom the declarations to the police, allowing environmental public libraries, public procurement, certificates, applying for higher education, Publication of change of residence, Health services. The connection between EG and EPG is very close. E-police (EP) is only one of 20 services that EG offers to the citizens.

This paper has analyzed EPG as the part of EG, benefits, their development in developed countries and possibility of implementing EG in Macedonia. Macedonia has already EG, but not all sectors are still developed.

2. E-GOVERNMENT AND E-POLICE

E-government (EG) refers to the using of information-communication technologies from the government for the purposes as follows: better communication with citizens and business, enabling better access to the services provided better access to the information, in other words - more effective and more transparent government. Determining the index of e-government is complex. This index is derived from several indexes: Web index, The infrastructure index, Human capital index and E-participation.

EG (or Electronic government) can be defined as the "use of information and communication technologies to offer citizens and businesses the opportunity to interact and conduct business with government by using different electronic media such as telephone, touch pad, fax, smart cards, self-service kiosks, e-mail/ Internet, and EDI" (Almarabeh and AbuAli, 2010: 30). In its simplest form, EG is the application of information and communication technologies (ICTs) to deliver public services (Holmes, 2001). Hence, EG can be viewed as the administration, rules, regulations and frameworks, organized by a government for service delivery as well as to communicate, co-ordinate and integrate processes within itself (Almarabeh and AbuAli, 2010).

On the other side EPG is the transaction of services and information between the police and citizens via the Internet. A recent review of the police service models and call management suggested that use of the Internet to report calls for service was an emerging trend.[290]

The Internet is increasingly central to public access and information. Secure reporting of non-urgent incidents is one of the Internet applications that is already proved useful. Online crime reporting allows the public to file police reports for some incidents and crimes via the Internet, 24 hours a day, and seven days a week. Police departments can retrieve these reports when police resources are available. This frees up patrol officers who would otherwise spend time tracking down these incidents.[291]

---

[290] E-Policing in Police Services, Definitions, Issues and Current Experiences, http://www.rcmp-grc.gc.ca/pubs/ccaps-spcca/e-policing-police-eng.htm(accessed 17.12.2015)

[291] Ibid

E-police (EP) is intended to provide total computerized information system support for the work of the police. EP system registers the complaints from the people through the online tools, and it is helpful to the police department for further process. The aim of EP is to develop an E-police reporting and management system, which is easily accessible to the public, police department and to the administrative department. EP would also help to provide division heads and senior officers with the management information about crime control, as well as about administration and support services, such as accounting and personnel management. This helps to the higher authorities of the police to have an overview about the progress of the investigation. This feature is made available to the public, for the purpose of the interaction with police indirectly[292].

EP expands our channels of communication through the Internet, but it is not able to replace completely the telephone or face-to-face contact, which already remained important. Developing of an EPG initiative requires:

- development of a strategic vision and direction
- evaluating impacts of related legislation
- evaluation of technology options
- projection of all costs, including planning, implementation and operation
- identifying such barriers to success as lack of strategy, resistance and delays in requirements.

Identified Benefits of E-policing are multiple.

For the community, EPG is important for several purposes:

- Reporting incidents does not require face-to-face contact with the police
- Better access for those in rural or remote areas
- Ability to ask questions and get answers when convenient
- Ability to exit the process at any time without difficulty or repercussions.

For the police, EPG is important for several purposes:

- Online forms assure that identical-screening questions are asked
- Ability to schedule work more evenly through the day
- Ability to deliver 24/7 police services conveniently and cost effectively without a physical presence (possibly establishing a virtual police station in crime spots and remote areas)
- Improved linkages with local organizations and partners.[293]

EP depends of development of EG in countries, internet users, and internet broadband. In the developed countries, EG technologies have a potential to improve the life of 80% of the world's population. The developed countries, such as the U.S., Canada, UK and Australia are the leaders in EG so far (Annual Global Accenture Study, 2002), reaping the vast majority of initial gains of e-government implementation. Actually, the gap between developed and

[292] Sumit R., Shreyas B. Kene , Prof. V. V. Bhujade E-Police Police Record Management System, Farsole Department of Computer Sci. and Engg. International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, Volume: 2 Issue: 3

[293] E-Policing in Police Services, http://www.rcmp-grc.gc.ca/pubs/ccaps-spcca/e-policing-police-eng.htm(accessed 03.12.2015)

developing countries in Internet technological infrastructures, practices, and usage has been wider rather than narrower over recent years. Besides the lack of sufficient capital to build up expensive national information infrastructure (NII), on which EG is based, the developing countries also lack the sufficient knowledge and skills to develop suitable and effective strategies for establishing and promoting EG. An estimated 500 EG-programs were launched in the year 2001 by governments worldwide (Palmer, 2002).

3. E-POLICE FUTURE IN MACEDONIA

The beginning of the concept of development of EG in the Macedonia lasts from 2000. In 2001, the Law on Electronic Data and Electronic Signature was adopted. At the national level, strategic approach to build information society started with the "e-Macedonia for all". E-Declaration from 2002 includes twenty experts from all sectors concerned. The Declaration adopted by the Parliament lays the institutional foundations for further activities towards the development of information society in Macedonia. Parliament declaration was adopted as a proposal by MPs from both major parties under this umbrella. Following the recommendations, the Government established the CIT (Information Technology Commission), as a body, which powers have been engaged towards the development of ICT and information society in the country. CIT created the National ICT task force composed of experts from all sectors. Macedonian implementation of EP started with a National strategy. This Strategy predicts electronic alarm to the police, with the possibility of standard procedure for reporting criminal activity (theft of car theft in the home, etc.), where in the regional unit of the Ministry of Interior should be conducted electronically. The service will be implemented by the Ministry of the Interior, with the stakeholders. Ministry of Information Society implemented strategic objective, operationalized in the development of information society services expected results: 24x7 availability of electronic service without the need for physically walking into a branch of MI; reducing costs associated with submission alarm implementation period (2009-2010); performance indicators (number of occurrences obtained electronically compared with the number of occurrences obtained default); risks (non-usage due to distrust of citizens to the service); Misuse Service.

According to the Strategy, the electronic alarm has not been implemented yet. Using EP is related to the use of internet service. If we compare with developed countries in 2005, about 16.8 million Canadian adults, or 68% of them, used the internet for personal non-business reasons. Only 58% of the residents who are living in rural and remote areas have the access to the internet (Statistic Canada, 2006). In 2003, internet use was lower among household outside the 15 most populous census metropolitan areas, but 85 percent of rural youth reported almost daily computer use at libraries, as compared with 4 percent of students in cities (Public Works and Government Services Canada, 2005). Therefore, it means that rural Canadians have improved their situation regarding the internet. The internet was used at home for the e-mail (91% compared to 32.2% in 2003), general web browsing (84 percent, 48.5% in 2003) and electronic banking (58%, 30.8% in 2003), to name just a few activities. The categories of crime prevention, public security or crime, were not included in the 2003 survey, but searching the information about the governments could somehow fit around 52% (Statistic Canada, 2006; 2004). Davies (2004) notes that 53% of households in the UK are connected to

the Internet and about 70 percent of people use it occasionally. Davies (2004) compared the internet to a new community with rules that resemble to the democratic constitutions.

The precondition for the development of EP in Macedonia is internet literacy, handling with ICT on a satisfactory level and almost close to the level of the use in highly developed countries, which have already established the system of EPG. According to the data of the State Statistical Office, in the first quarter of 2015, 69.4% of the households had access to the Internet at home, which is one percentage point more in comparison with the same period in 2014. The participation of households with broadband connection in the total number of households increased from 67.7% in 2014 to 69.0% in 2015. Almost all (99.5%) of the households with internet access had broadband (fixed or mobile) connection to the Internet. In the first quarter of 2015, 69.2% of the total population aged 15-74 used a computer, while 70.4% used the internet. Internet was most used by pupils and students, i.e. 94.7%. 71.2% of the Internet users in the first quarter of 2015 used a mobile phone or a smart phone for accessing the Internet away from home or work. Of the persons to have ever used the Internet, 15.4% ordered/bought goods or services over the Internet in the last 12 months, and the majority of them (66.9%) bought clothes or sports goods, and user of internet banking were 7%. Almost 80% of the persons that did not buy over the internet in the last 12 months prefer to go in shopping personally. Namely, they like to see product, force of habit or similar, and 28% did not buy over the internet because of their worries about payment security or privacy concerns, e.g. giving credit card details or personal details over the Internet.[294]

Macedonia has lots preconditions for development of EP. There is a need to establish EP because of several benefits: improvement of the effectiveness for the policy performance; to improve the efficiency of police procedures (for example, by eliminating redundant processes in the registration of criminal cases); to improve the quality of management information provided for senior policy decision-making, particularly through integration of previously separate information systems.[295] EPG opens new ways of performing jobs for the police, not only through newly available tools, but also by creating an interactive flow of information between the police and the citizens. EPG fosters two-way communication, providing better access for both, the public and the police.
EPG enables that the initial public contacts can be handled electronically. This delivers information to the police, when it is “fresh”, decreasing public inconvenience of waiting on the telephone or in line at the police station to report in person. E-policing signals that police are in synch with current technology[296].

It is also need to be set up a “Third Eye” software in the special branches of the police department so that it helps the police supervisors to monitor crime and criminal records. An electronic database has to be set, with an interactive website, which will contain daily press

[294] www.stat.gov.mk
[295] Sumit R., Shreyas B. Kene , Prof. V. V. Bhujade *E-Police Police Record Management System*, Farsole Department of Computer Sci. and Engg. International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, Volume: 2 Issue: 3
[296] *E-Policing in Police Services, Definitions, Issues and Current Experiences*, http://www.rcmp-grc.gc.ca/pubs/ccaps-spcca/e-policing-police-eng.htm(accessed 17.12.2015)

releases, supplement, list of top terrorists and criminals, lists of people under police custody and people injured in road or other accidents, etc.[297]

4. CONCLUSIONS

The growth of science and technology made development of society. Internet use has become an important in the functioning of the system. Highly developed countries have already established e-government (EG) with all its elements defined by the European Commission. One of these sub-systems is the e-police (EP). Good examples of the established systems of EP from developed countries have England, Canada, USA, Estonia, Singapore, Japan, China, etc. The basic prerequisite for setting up the EP are the networks of broadband Internet, as well as the confidence in using of the electronic systems, media and ICT literacy.

Although Macedonia still has numerous internet users, the strategy developed from the Ministry of Informatics and Administration to use EP is still not established, within coherent system.

Undoubtedly, the police should remain to have face-to-face communication, but also the electronic communication appears as extremely important. EPG as communication system has two-way direction, as police to citizen and vice versa. According researches many participants saw that e- policing could be more effective at the level of service delivery. Expectations are that online reporting could reduce the demand on front line officers, switchboard and front counter staff. Macedonia should realize the planned project for the introduction of EP, having in mind the benefits and advantages that EP offers.

REFERENCES

Almarabeh, T., & AbuAli, A. (2010). A General Framework for E-Government: Definition Maturity Challenges, Opportunities, and Success. *European Journal of Scientific Research*, 39(1), 29-42.

E-Policing in Police Services, Definitions, Issues and Current Experiences (2015). http://www.rcmp-grc.gc.ca/pubs/ccaps-spcca/e-policing-police-eng.htm (accessed 17/12/2015)

International Conference on UN Global E-government Readiness Report (2004). Towards Access for Opportunity. New York: United Nations.

Mollah, M.B., Islam, S.S., Ullah, M.A. (2012). *Proposed e-police system for enhancement of e-government services of Bangladesh.* Informatics, Electronics & Vision (ICIEV). http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?arnumber=6317444 (accessed 12/3/2016)

Palmer, I. (2002). *State of the world: eGovernment implementation*. Faulkner Information Services (January), Docid 00018297. Annual Global Accenture (former Anderson Consulting: AC) Study Report.

Sumit R., Kene S.B., Bhujade, V.V. (2014). *E-Police Police Record Management System*, Farsole Department of Computer Sci. and Engg. *International Journal on Recent and Innovation Trends in Computing and Communication*, 2(3), 497-500.

[297] Mollah, M.B. Islam, S.S. ; Ullah, M.A.Proposed e-police system for enhancement of e-government services of BangladeshInformatics, Electronics & Vision (ICIEV), 2012 International Conference on

POLICIJSKI PROCESI – NOVE TEHNOLOGIJE, SIGURNOST I PRAVO/
POLICE WORK- NEW TECHNOLOGIES, SECURITY AND LAW

STRUČNI RAD

Stjepan Gluščić[298]
Lana Milivojević[299]

UREĐENJE INSTITUTA NEOVISNOSTI I UČINKOVITOSTI ISTRAGE I NEOVISNOSTI ISTRAŽITELJA U HRVATSKOM KAZNENOM POSTUPKU

Sažetak

U radu se analizira utjecaj odluka Ustavnog suda RH i odluka ESLJP na normativno uređenje i tumačenje ispunjenosti uvjeta u provedbi učinkovite i neovisne istrage i neovisnosti istražitelja u kaznenom postupku. U posljednjih nekoliko godina ESLJP i Ustavni sud RH donijeli su nekoliko značajnih presuda u kojima se utvrđuje da u pojedinim slučajevima nije provedena učinkovita i neovisna istraga sumnje u počinjenje kaznenog djela. Posljednjim izmjenama Zakona o kaznenom postupku, Zakona o državnom odvjetništvu, kao i Zakona o policijskim poslovima i ovlastima normirani su postupci i pravila kojima se nastoji ispuniti standarde nužne za neovisnu i učinkoviti istragu i neovisnost istražitelja.

Ključne riječi: *istraga, istražitelj, kazneni postupak, Ustavni sud.*

1. UVOD

Za kazneno procesno pravo u RH može se reći da se nalazi u kontinuiranoj reformi. Povijesno promatrano, dosadašnje značajnije zahvate reformskog karaktera možemo podijeliti u tri cjeline. Prva značajnija izmjena dogodila se donošenjem novog Zakona o kaznenom postupku (u daljnjem tekstu ZKP) 1997. godine, druga donošenjem, također, novog ZKP-a 2008. godine, te treća donošenjem odluke Ustavnog suda broj U-I-448/2009, U-I-602/2009, U-I-1710/2009, U-I-18153/2009, U-I-5813/2010, U-I-2871/2011 (NN 91/2012., u daljnjem tekstu Odluka).

Jedan od temeljnih ciljeva izrade ZKP/97. bilo je izraditi zakon koji odražava kriminalno-politički napora za uravnoteženjem težnje za zaštitom građana i težnje za učinkovitošću postupka. U tom nastojanju željelo se prihvatiti i razraditi temeljna prava i slobode građana kao i prava obrane u postupku koja proizlaze iz Ustava kao i međunarodnih dokumenata prvenstveno Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda od 4. studenog 1950. (NN-MU 18/97.), uvažiti nove pojavne oblike kriminaliteta te rasteretiti kazneni postupak (Krapac, str. 10., 2008.). Druga reformska izmjena dogodila se donošenjem ZKP/2008. Ovaj ZKP je, slijedeći dostignute promjene ZKP/97., prvenstveno reformirao prethodni kazneni postupak. Temeljna promjena odnosi se na ukidanje sudske istrage i njezino transformiranje u državnoodvjetničku istragu, gdje su uz stadij optuživanja izvršene najveće promjene. Promjene su učinjene i u podcjelinama kaznene prijave i izvida kaznenih

[298] Dr. sc. Stjepan Gluščić, prof. visoke škole, Visoka policijska škola, Zagreb, e-mail: sgluscic@fkz.hr
[299] Dr. sc. Lana Milivojević, prof. visoke škole, Visoka policijska škola, Zagreb, e-mail: lmilivojevic@fkz.hr

djela. Prethodni postupak u ZKP/2008. podijeljen je na podcjeline: kazneni progon, istraga, dokazne radnje i optuživanje. Državni odvjetnik postaje stožerna figura cjelokupnog prethodnog postupaka, nositelj funkcije progona u okviru koje planira i provodi aktivnosti predviđene zakonom. Dio radnji može prepustiti policiji ili istražitelju. Teoretičari, imajući u vidu nove odnose i zadaće u potpuno renomiranom i za nas novom postupku, navode da je za uspjeh ove reforme ključan odnos policije i državnog odvjetništva te da oni postaju odgovorni za uspjeh i provedbu kaznenog progona (usporedi Pavišić, str. 590., HLJKPP 2/2008.). Treća etapa razvoja označava se kao konstitucionalizacija, judicijalizacija i europeizacija hrvatskog kaznenog postupka (Đurđević, str. 315., HLJKPP br. 2/2013.) a značajno je uvjetovana donošenjem Odluke USRH 19. rujna 2012. godine kojom je utvrđeno kako Zakon o kaznenom postupku iz 2008. godine nije u skladu s 18 članaka Ustava RH i 6 članaka Europske konvencije o zaštiti temeljnih prava i sloboda, odnosno da su 43. članka ZKP/08. protivna Ustavu RH. Europeizacija proizlazi iz obveza usklađivanja kaznenog procesnog prava s pravom Europske unije. Direktive Europskog parlamenta i Vijeća od prihvaćanja Lisabonskog ugovora su temeljni propisi kojima se usklađuju kaznenopravni sustavi država članica EU. Judicijalizacija se odnosi na jačanje ovlasti suda u svim stadijima kaznenog postupka, te na uspostavljanje i jačanje sudske zaštite okrivljenika u kaznenom postupku (Đurđević, str 316., HLJKPP br. 2/2013.).

Ova posljednja etapa je višeznačna i međusobna isprepletena. Konstitucionalizacija kaznenog postupka rješava i određena pitanja koja se nameću prihvaćanjem direktiva kojima se uređuju pojedina pitanja koja su rješavana i Odlukom USRH, te se istodobno odnose i na judicijalizaciju, jer se rješavajući pitanje jačanje uloge suda u postupku rješava i pitanje kontrole nad ostvarivanjem prava okrivljenika.

U ovom radu se analizira utjecaj odluka USRH i odluka ESLJP na normativno uređenje i tumačenje ispunjenosti uvjeta u provedbi učinkovite i neovisne istrage i neovisnosti istražitelja u kaznenom postupku. U posljednjih nekoliko godina ESLJP je donio nekoliko značajnih presuda u kojima se utvrđuje da u pojedinim slučajevima nije provedena učinkovita i neovisna istraga sumnje u počinjenje kaznenog djela, dok je USRH temeljem tih presuda i odredbi samog Ustava RH ustanovio određene standarde za provedbu učinkovite istrage i neovisnosti istražitelja, što je rezultiralo i izmjenama Zakona o kaznenom postupku, Zakona o državnom odvjetništvu, kao i Zakona o policijskim poslovima i ovlastima. U navedenim zakonima normirani su postupci i pravila kojima se nastoji ispuniti standarde nužne za neovisnu i učinkoviti istragu i neovisnost istražitelja.

2. KAZNENI PROGON PREMA ZKP/08.

Ustavni sud u svojoj Odluci (točka 121. Odluke) zaključuje kako, „praksa Europskog suda jasno pokazuje“ da danas postoji minimum zajedničkih europskih pravnih standarda vezanih uz djelotvornost postupaka prije suđenja neovisno o njihovoj formalnoj nacionalnoj klasifikaciji. Kazneni progon i istraživanje moraju biti neovisni, nepristrani i djelotvorni tako da mogu dovesti do otkrivanja i kažnjavanja odgovornih.

Kazneni progon i istraživanje odnose na aktivnosti prethodnog postupka, a prema našem ZKP-u to su aktivnosti koje poduzima prvenstveno državno odvjetništvo i policija (moguće je i istražni sudac). Kazneni progon je funkcija državnog odvjetnika koja označava poduzimanje

aktivnosti usmjerenih na otkrivanje i procesuiranje kaznenih djela za koja se progon poduzima po službenoj dužnosti. Državno se odvjetništvo kao posebno državno tijelo za vršenje kaznenog progona pojavljuje početkom XIX. st., dakle u vrijeme nastanka mješovitog tipa kaznenog postupka. Uvođenje državnog odvjetnika u kazneni postupak, te utemeljenje državnog odvjetništva kao posebnog državnog tijela ima za cilj osigurati sustavni kazneni progon ali i nadzor države nad ovom funkcijom kaznenog postupanja (Tomašević, Krapac, Gluščić, str. 25., 2012.). Vršenje kaznenog progona najvažnija je zadaća državnog odvjetnika koja se sastoji od niza aktivnosti i zadaća, navedenih u čl. 38. ZKP-a. Policija je pak zadužena, prvenstveno, za otkrivanje (ali i dokazivanje) počinjenih kaznenih djela.

Prema ZKP/08., prije izmjena uvjetovanih Odlukom USRH, prethodni postupak sastojao se od četiri cjeline. 1. Kazneni progon (Kaznena prijava; Izvidi kaznenih djela; Odbacivanje kaznene prijave i odustajanje od kaznenog progona prema posebnom zakonu; Dokazne radnje prije početka postupka). 2. Istraga (Pokretanje, tijek i okončanje istrage; Dokazno ročište; Pouka o pravima). 3. Dokazne radnje: a) dokazne radnje: pretraga; privremeno oduzimanje predmeta; ispitivanje okrivljenika; ispitivanje svjedoka; prepoznavanje; očevid; uzimanje otisaka prstiju i otisaka drugih dijelova tijela; vještačenje; dokaz ispravom; dokaz snimkom; elektronički (digitalni dokaz); b) posebne dokazne radnje: nadzor i tehničko snimanje telefonskih razgovora i drugih komunikacija na daljinu; presretanje, prikupljanje i snimanje računalnih podataka; ulazak u prostorije radi provođenja nadzora i tehničko snimanje prostorija; tajno praćenje i tehničko snimanje osoba i predmeta; uporabu prikrivenih istražitelja i pouzdanika; simuliranu prodaju i otkup predmeta te simulirano davanje potkupnine i simulirano primanje potkupnine; pružanje simuliranih poslovnih usluga ili sklapanje simuliranih pravnih poslova; nadzirani prijevoz i isporuku predmeta kaznenog djela; privremeno oduzimanje poštanskih pošiljki; sravnjivanje računalnih podataka i 4. Optuživanje (podizanje, sadržaj i predaja optužnice; prethodno ispitivanje i odgovor na optužnicu; postupak pred optužnim vijećem; odlučivanje o potvrđivanju optužnice; očitovanje okrivljenika o krivnji i pregovaranje o sankciji; donošenje presude na temelju sporazuma stranaka; povlačenje i izmjena optužnice; upućivanje na suđenje).

Kazneni progon započinjao je upisom kaznene prijave u upisnik (čl. 205. st. 4. ZKP/08.) ili svakom radnjom ili mjerom ograničenja osobnih prava i sloboda koju poduzima nadležno tijelo, a usmjerena je razjašnjavanju sumnje da je određena osoba počinila kazneno djelo. Kazneni progon završavao je odustajanjem državnog odvjetnika ili drugog ovlaštenog tužitelja od progona ili sudskom odlukom (čl. 2. st. 5. ZKP/08.). U navedenom smislu početak kaznenog progona je vezan uz upis kaznene prijave u odgovarajući upisnik, odnosno uz kriterij ograničenja osobnih prava i sloboda neke osobe. Kazneni progon obuhvaća radnje poduzete u cilju razjašnjenja pitanja o postojanju uvjeta započinjanja kaznenog postupka ili odbacivanja kaznene prijave, a traje od upisa prijave u upisnik ili poduzimanje radnje ili mjere ograničenja osobnih prava pa do odluke suda. Za početak kaznenog progona nije potreban odluka suda već državnog odvjetnika, dok je za početak kaznenog postupka potrebna odluka suda. Kazneni postupak započinje: 1) potvrđivanjem optužnice, 2) određivanjem rasprave na temelju privatne tužbe, 3) donošenjem presude o izdavanju kaznenog naloga (čl. 17. st. 1. ZKP/08.). Od započinjanja kaznenog postupka, razlikujemo započinjanje kaznenog progona, koji može započeti upisom kaznene prijave u upisnik kaznenih prijava ili svakom radnjom ili mjerom ograničenja osobnih prava i sloboda koju poduzima nadležno tijelo (čl. 2. st. 5.).

Kazneni postupak završava donošenjem pravomoćne presude, obustavom istrage ili obustavom postupka. Kazneni progon završava odustajanjem od progona ili sudskom odlukom.
Prvenstveno je uloga državnog odvjetnika ustrajati na kaznenom progonu, te radi ostvarivanja njegove svrhe, pravodobno poduzimati radnje na koje je ovlašten zakonom. U uređenju kaznenog progona ZKP/08. naglasak stavlja na učinkovitost. Ona se promatra ne samo kao dužnost već i pravo tijela kaznenog progona, ali i pravo osumnjičenika da se odluči o sumnji koja ga opterećuje kao i pravu žrtve i oštećenika tijekom postupka bez obzira na činjenicu da se postupak vodi po službenoj dužnosti. Dio odredbi kojima se uređivao kazneni postupak Ustavni sud proglasio je neustavnim i naložio zakonodavcu njihovo usklađivanje s Ustavom. U svojoj Odluci, Ustavni sud poziva se i na standarde ESLJP i odluke u kojima se standardi definiraju te na taj način zapravo određuje okvire u kojima se normativno uređenje (navedenih instituta) i treba pridržavati.

3. STANDARDI KOJI OMOGUĆUJU PROVEDBU UČINKOVITE ISTRAGE PREMA ODLUCI USRH

A) Standardi učinkovite istrage

Navodeći da kazneni progon mora biti neovisan, nepristran i djelotvoran, USRH u Odluci navodi da to znači prihvaćanje standarda koji omogućavaju: a) adekvatnost istrage za utvrđivanje i kažnjavanje počinitelja, b) sveobuhvatnost istrage, c) neovisnost i nepristranost istražitelja, d) žurnost istrage, e) transparentnost, f) uključenost žrtve u istragu odnosno istraživanje i g) obvezu poduzimanja kaznenog progona kada na to ukazuje rezultat istrage.

Navedeni standardi u suštini znače provedbu i standarda koji proizlaze iz Konvencije (vidi Batistić Kos, str. 57. HLJKPP 1/08.) a artikulirani su kroz odluke ESLJP, pri čemu se ističe da je odgovornost države da izgradi sustav koji je sposoban prevenirati ali i istraživati kaznena djela što znači identifikaciju počinitelja te njihovo kažnjavanje. Obveza provođenja djelotvornog istraživanja jest „obveza načina/sredstava, a ne rezultata. Svako istraživanje ne mora nužno biti uspješno ili dovesti do zaključka koji se podudara s opisom događaja podnositelja kaznene prijave, ali treba u načelu biti prikladno da dovede do utvrđivanja činjenica predmeta i, ako se dokaže da su navodi istiniti, do identifikacije i kažnjavanja odgovornih“ (Odluka USRH točka 121.). Učinkovita istraga je detaljna i brižna, te mora obuhvatiti sve relevantne okolnosti i uključiti sve razumne aktivnosti potrebne za osiguranje dokaza. Istražitelji moraju biti neovisni i nepristrani. Žurnost istrage označava promptnost u poduzimanju radnji, njihovu pravodobnost, iako se uvažava da mogu postojati prepreke i teškoće koje sprečavaju napredak u istraživanju u određenoj situaciji. Transparentnost označava javnu kontrolu rezultata istrage kako bi se osigurala odgovornost kako u teoriji tako i u praksi te zadržalo povjerenje javnosti. U istraživanje mora biti uključena i žrtva koja ima pravo dobiti informacije o napretku i istraživanju ali i podnositi određene upite i prigovore kako bi osigurala ta svoja prava (vidi Krapac, D., Đurđević, Z., i dr., 2013.).

Odredbe ZKP-a koje imaju za cilj oživotvorite standarde učinkovite istrage odnose se na propisivanje rokova za donošenje odluka od strane državnog odvjetnika, i to o kaznenoj

prijavi, trajanju istrage, optuženje, pravu žrtve na obavijest o radu na prijavi i pravu osumnjičenika na pravno sredstvo zbog nerješavanje prijave. U pravilu rokovi propisani za postupanje državnog odvjetnika instruktivne su naravi.

Rok u kojem je državni odvjetnik dužan donijeti odluku o kaznenoj prijavi je šest mjeseci od dana upisa prijave u upisnik kaznenih prijava. O tome obavještava i podnositelja prijave uz navođenje kratkih razloga te odluke. Po isteku rokova za donošenje odluke podnositelj prijave, oštećenik i žrtva mogu podnijeti pritužbu višem državnom odvjetniku zbog nepoduzimanja radnji državnog odvjetnika koje dovode do odugovlačenja postupka. Viši državni odvjetnik, ako ocijeni da je pritužba osnovana, mora odrediti primjereni rok u kojem se mora donijeti odluka o prijavi. O poduzetom se obavještava podnositelja pritužbe u roku od petnaest dana od dana primitka pritužbe. Podnositelj pritužbe može ponoviti pritužbu ako prijava nije riješena u navedenom roku (čl. 206.b ZKP). Daljnji rokovi normirani ZKP-om su oni koji se odnose na provedbu istrage i istraživanja.

Ako po proteku šest mjeseci od upisa kaznene prijave u upisnik kaznenih prijava ili od uhićenja državni odvjetnik nije donio odluku o prijavi, okrivljenik ima pravo podnijeti prigovor sucu istrage zbog odugovlačenja postupka. Sudac istrage ovlašten je rješenjem odrediti rok u kojem državni odvjetnik mora odlučiti o kaznenoj prijavi ako je utvrdio da je prigovor zbog odugovlačenja postupka osnovan. O svojoj odluci državni odvjetnik je dužan obavijestiti suca istrage. Ako sudac istrage utvrdi da je prigovor neosnovan obavijestiti će o tome okrivljenika. Ukoliko se netko od ovlaštenika pritužio višem državnom odvjetniku a ovaj je odredio rok za rješavanje prijave (članak 206.b stavak 4. ZKP), a rok je odredio i sudac istrage, državni odvjetnik je dužan riješiti prijavu u roku koji je odredio sudac istrage (čl. 213.b ZKP).

Redoviti rok u kojem državni odvjetnik mora završiti istragu je šest mjeseci. Ako se istraga ne završi u roku od šest mjeseci, državni odvjetnik je dužan izvijestiti višeg državnog odvjetnika o razlozima zbog kojih istraga nije završena. Viši državni odvjetnik dužan je poduzeti mjere da se istraga završi. U složenim predmetima viši državni odvjetnik može na obrazloženi prijedlog državnog odvjetnika produljiti rok za najviše šest mjeseci. U posebno složenim i teškim predmetima, glavni državni odvjetnik može na obrazloženi prijedlog državnog odvjetnika rok završetka istrage produljiti za najviše dvanaest mjeseci. Okrivljenik i oštećenik mogu se tijekom istrage obratiti pritužbom višem državnom odvjetniku zbog odugovlačenja postupka i drugih nepravilnosti u tijeku istrage. Okrivljenik se može obratiti pritužbom višem državnom odvjetniku i ako državni odvjetnik nije donio rješenje o provođenju istrage u roku od 48 sati od ispitivanja okrivljenika (čl. 216. st. 4. ZKP) niti podigao optužnicu bez provođenja istrage (čl. 341. stavka 3. ZKP). Viši državni odvjetnik ispituje navode iz pritužbe i obavještava podnositelja ako je to ovaj zahtijevao (č. 229. ZKP).

Nakon završene istrage ili istraživanja državni odvjetnik je dužan u roku od petnaest dana od dana upisa završetka istrage ili istraživanja u upisnik kaznenih prijava podignuti optužnicu ili obustaviti istragu odnosno odbaciti kaznenu prijavu. U složenim predmetima taj rok iznosi trideset dana. Viši državni odvjetnik može rok za podizanje optužnice produljiti na prijedlog

državnog odvjetnika za najviše petnaest dana, a u složenim predmetima za najviše trideset dana. Iznimno, ako su postojali nepredvidivi ili neotklonjivi razlozi, viši državni odvjetnik može na prijedlog državnog odvjetnika produljiti rokove za najviše petnaest dana. Državni odvjetnik obavještava oštećenika o podizanju optužnice ili o obustavi istrage odnosno odbacivanju kaznene prijave uz pouku o pravu na preuzimanje progona (iz čl. 55. stavka 5. ZKP). Ako državni odvjetnik ne postupi prema navedenim pravilima, dužan je o razlozima izvijestiti višeg državnog odvjetnika. Ukoliko državni odvjetnik u opisanim rokovima ne podigne optužnicu, smatrat će se da je odustao od kaznenog progona (čl. 230. ZKP).

Uz navedene odredbe i Zakon o državnom odvjetništvu propisuje rokove za postupanje državnog odvjetnika. Obveza državnog odvjetnika ili zamjenika državnog odvjetnika da postupa bez odugovlačenja u pogledu donošenja odluka povodom kaznenih prijava koje su mu dodijeljene u rad. Ako u predmetu bez opravdanog razloga u roku od petnaest dana od dana primitka nove prijave, ili predmeta u kojem su provedeni izvidi ili dokazne radnje, nije donio odluku ili poduzeo drugu radnju koju je trebalo poduzeti, dužan je o tome izvijestiti državnog odvjetnika ili višeg državnog odvjetnika koji će poduzeti potrebne mjere kako bi se u predmetu postupalo bez odgode. Kad je kaznena prijava podnesena protiv policijskog službenika, državni odvjetnik sam provodi istragu odnosno istraživanje. Tako će državni odvjetnik postupiti i u slučaju kad je prijava podnesena protiv druge službene osobe koja je ovlaštena i dužna otkrivati i prijavljivati kaznena djela za koja se progoni po službenoj dužnosti (čl. 67. ZDO).

Državni odvjetnik ili zamjenik državnog odvjetnika dužan je kaznenu prijavu riješiti u rokovima propisanim zakonom. Ako državni odvjetnik ne donese odluku o prijavi u tim rokovima, dužan je izvijestiti višeg državnog odvjetnika o razlozima zbog kojih nije donesena odluka o prijavi. Ako je počinitelj kaznenog djela ostao nepoznat i nakon isteka šest mjeseci od dana upisa kaznene prijave u upisnik kaznenih prijava, spis će se staviti u evidenciju. Ako je u evidenciju stavljena prijava za kazneno djelo za koje je propisana kazna zatvora veća od pet godina, državni odvjetnik je dužan po isteku godine dana od dana stavljanja prijave u evidenciju provjeriti jesu li i koje radnje poduzete kako bi se počinitelj otkrio (čl. 68. ZDO).

B) Neovisnost i nepristranost istražitelja

Neovisnost i nepristranost istražitelja jest zaseban kriterij koji zahtjeva dodatnu razradu. Prema Odluci Ustavnog suda i presudama ESLJP protiv RH nepristranost i neovisnost podrazumijeva da istražne vlasti ne smiju biti povezane s osobama uključenim u događaje koji se istražuju ni hijerarhijski, ni institucionalno, ni stvarno. Neovisnost i nepristranost obuhvaća sve osobe koje neposredno sudjeluju u postupku pribavljanja dokaza ili donošenja odluka. Sudionici postupka, sukladno postojećoj koncepciji su i državni odvjetnik i policijski službenici koji sudjeluju u poduzimanju radnji ali i istražitelji iz drugih državnih tijela.

U našoj teoriji i praksi velika pozornost se posvećivala uvjetima važnim za pravilnost sudskih odluka među kojima i objektivnosti odnosno nepristranosti suca koji rješava konkretni kazneni predmet. Navodili smo da objektivnost, odnosno nepristranost postoji ako bi donesena odluka bila ista i kad bi druge osobe bile stranke ili ako bi u istom predmetu drugi sudac donio istovjetnu odluku. Moguća pristranost, neobjektivnost, suca razlog je za njegovo

izuzeće u konkretnom postupku a ti razlozi primjenjuju se u suštini i na državnog odvjetnika. Izmjenama ZKP-a uvjetovanih primjenom nove koncepcije državnoodvjetničke istrage i Odluke Ustavnog suda razrađeni su uvjeti i za policijske službenike.
Naše pravo razlikuje isključenje od otklona. Isključenje predstavlja obvezno izuzeće s obzirom na razloge dok otklon ne predstavlja obvezno izuzeće.
ZKP normira obje situacije propisujući uvjete kad sudac ili sudac porotnik moraju biti isključeni od obavljanja sudačke dužnosti. Razlozi isključenja taksativno su navedeni i njihovim postajanjem smatra se da sudac nije nepristran, objektivan. Razlozi su: ako je oštećen kaznenim djelom; ako mu je okrivljenik, njegov branitelj, tužitelj, žrtva, oštećenik, njihov zakonski zastupnik ili opunomoćenik, bračni drug ili srodnik u ravnoj lozi do bilo kojeg stupnja, u pobočnoj lozi do četvrtog stupnja, a po tazbini do drugog stupnja; ako je s okrivljenikom, njegovim braniteljem, tužiteljem, žrtvom ili oštećenikom u odnosu skrbnika, štićenika, posvojitelja, posvojenika, hranitelja, hranjenika, smještene osobe ili udomitelja; ako je u tom kaznenom predmetu u prethodnom postupku provodio dokazno ročište ili dokazne radnje ili je odlučivao o prigovoru za zaštitu postupovnih prava obrane ili o žalbi protiv rješenja o provođenju istrage, ili je odlučivao o potvrđivanju optužnice, ili je sudjelovao u postupku kao tužitelj, branitelj, zakonski zastupnik, savjetnik žrtve ili opunomoćenik oštećenika, odnosno tužitelja, ili je ispitan ili treba biti ispitan kao svjedok ili vještak (osima kao izuzetno nije propisano drugačije); ako je u istom predmetu sudjelovao u donošenju odluke koja se pobija žalbom ili izvanrednim pravnim lijekom (čl. 32. st. 1. ZKP).

Razlozi otklona su svi oni koji izazivaju sumnju u njegovu objektivnost, nepristranost (moraju se dokazati), (čl. 32. st. 2. ZKP). Sudac ili sudac porotnik čim saznaju da postoji koji od razloga za isključenje (iz članka 32. stavka 1. ZKP), moraju prekinuti svaki rad na tom predmetu i o tome izvijestiti predsjednika suda, koji im određuje zamjenu. Ako je riječ o isključenju predsjednika suda, on će odrediti sebi zamjenika između sudaca tog suda, a ako to nije moguće, zatražit će od predsjednika neposredno višeg suda da odredi zamjenu. Kad sudac ili sudac porotnik smatra da postoje druge okolnosti koje opravdavaju njegov otklon (članak 32. stavak 2. ZKP), izvijestit će o tome predsjednika suda (čl. 33. ZKP). Izuzeće mogu tražiti i stranke (čl. 34. st. 1. ZKP).

ZKP u čl. 37. određuje da se pravila o izuzeću suca i sudaca porotnika primjenjuju i na državne odvjetnike i osobe koje su na temelju Zakona o državnom odvjetništvu ovlaštene zastupati državnog odvjetnika u postupku, istražitelje, zapisničare, tumače i stručne osobe, a i na vještake (osim ako za njih nije što drugo određeno prema članku 311. ZKP). O izuzeću istražitelja, zapisničara, tumača, stručne osobe i vještaka, koji sudjeluju u istrazi koju provodi sudac istrage (članak 225. stavak 5.) odlučuje taj sudac. Kad radnju provodi sud, o izuzeću istražitelja, zapisničara, tumača, stručne osobe i vještaka odlučuje vijeće, predsjednik vijeća ili sudac. O izuzeću osoba koje su na temelju Zakona o državnom odvjetništvu ovlaštene da ga zastupaju u kaznenom postupku, istražitelja, zapisničara, tumača, stručne osobe i vještaka prije podizanja optužnice, odlučuje državni odvjetnik. O izuzeću državnog odvjetnika odlučuje neposredno viši državni odvjetnik. O izuzeću glavnog državnog odvjetnika odlučuje kolegij svih zamjenika glavnog državnog odvjetnika. Istražitelj i druge osobe koje sudjeluju u istrazi koju provodi državni odvjetnik čim saznaju da postoji koji od razloga za izuzeće, dužni

su o tome izvijestiti državnog odvjetnika i predložiti mu svoju zamjenu. Kad osoba sazna da postoji razlog za njezino izuzeće, dužna je odmah obustaviti svaki rad na predmetu, a ukoliko je riječ o otklonu, može do donošenja odluke državnog odvjetnika poduzimati samo one radnje za koje postoji opasnost od odgode.

Zakon o policijskim poslovima i ovlastim u čl. 11. normira hijerarhijsku i institucionalnu neovisnost u provedbu kriminalističkih istraživanja s ciljem udovoljavanja standardima neovisne i učinkovite istrage. ZOPPO propisuje da kad postoji osnova sumnje da je kazneno djelo počinio **policijski** službenik ili drugi zaposlenik određene ustrojstvene jedinice Ministarstva ili njima bliska osoba ili je kazneno djelo počinjeno u prostorijama ustrojstvene jedinice Ministarstva, kriminalističko istraživanje ne može provoditi ta ustrojstvena jedinica, osim kada su navedene osobe zatečene u počinjenju kaznenog djela ili kada je potrebno provesti hitne dokazne radnje ili druge radnje koje ne trpe odgodu. Kad postoji osnova sumnje da je **policijski** službenik ili drugi zaposlenik određene ustrojstvene jedinice odnosno njima bliska osoba oštećena kaznenim djelom koje je u vezi s obavljanjem **policijskog posla,** kriminalističko istraživanje ne može provoditi ustrojstvena jedinica u kojoj je oštećeni zaposlen, osim kada je potrebno provesti hitne dokazne radnje ili druge radnje koje ne trpe odgodu. U navedenim slučajevima kriminalističko istraživanje će provesti ona ustrojstvena jedinica Ministarstva koju za to odredi glavni ravnatelj ili osoba koju on za to ovlasti. Kad postoji osnova sumnje da je kazneno djelo počinio rukovodeći **policijski** službenik Ravnateljstva policije, bez odgode će se izvijestiti Državno odvjetništvo Republike Hrvatske koje će odlučiti o preuzimanju izvida kaznenog djela.

Prema čl. 67. st. 3. Zakona o državnom odvjetništvu ako je kaznena prijava podnesena protiv policijskog službenika državni odvjetnik će sam provesti istragu, a ako se istraga ne provodi provest će sam potrebne dokazne radnje koje su svrhovite za odlučivanje o podizanju optužnice. Tako će državni odvjetnik postupiti i u slučaju kad je prijava podnesena protiv druge službene osobe koja je ovlaštena i dužna otkrivati i prijavljivati kaznena djela za koja se progoni po službenoj dužnosti.

Kod poduzimanje hitnih dokaznih radnji (čl. 212. st.3. ZKP) policija gubi pravo na njihovo samostalno poduzimanje ako je hitne dokazne radnje potrebno poduzeti prema osobi koja je ovlaštena i dužna otkrivati i prijavljivati kaznena djela za koja se progoni po službenoj dužnosti. U takvim situacijama policija mora odmah obavijestiti državnog odvjetnika koji donosi odluku o tome da li će sam provesti tu radnju ili će za njezinu provedbu ovlastiti istražitelja.

4. ZAKLJUČAK

Zakon o kaznenom postupku iz 2008. godine značajno je promijenjen temeljem Odluke Ustavnog suda. Odluka Ustavnog suda, iako je od nje prošlo nekoliko godina, zasigurno će još određeno vrijeme predstavljati reformski okvir za naš kazneni postupak. Kako je i uvodno navedeno, Odluka je značajna po svojim posljedicama i stajalištu da Zakon o kaznenom postupku ne smije odstupati od Ustava u pogledu odredbi kojima se normiraju prava njegovih sudionika (okrivljenika ali i žrtve). Standardi koji se odnose na učinkovitu i neovisno istragu kao i neovisnost samog istražitelja prisutni su u našem postupku i praksi a normativnim uređenjem utemeljenim na Odluci Ustavnog suda doživjeli su aktualizaciju sukladno novo prihvaćenim i novo protumačenim standardima proizašlim iz tumačenja odredbi samog Ustava i odluka ESLJP. U svojoj suštini odnose se na poznate zahtjeve za uravnoteženjem postupanja i zaštitom prava žrtve i prava osumnjičenika u postupku.

LITERATURA

Batistić Kos, V. (2008). *Mjerila Europskog suda za ljudska prava za učinkovitu istragu zlostavljanja motiviranog rasnom diskriminacijom* (slučaj Šečić protiv Republike Hrvatske). HLJKPP, br. 1/08., str. 55–85.

Đurđević, Z. (2012). *Odluka Ustavnog suda RH o suglasnosti Zakona o kaznenom postupku s Ustavom*. HLJKPP br. 2/12., str. 409–438.

Đurđević, Z. (2013). *Rekonstrukcija, judicijalizacija, konstitucionalizacija, europeizacija hrvatskog kaznenog postupka V. novelom ZKP/08., prvi dio.* HLJKPP br. 2/13., str. 315–362.

Gluščić, S., Veić, P. (2015). *Komentar Zakona o policijskim poslovima i ovlastima*. Zagreb: MUP RH.

Krapac D. (2008). *Zakon o kaznenom postuku i drugi izvori hrvatskog kaznenog postupovnog prava*. Zagreb: Narodne novine.

Krapac, D., Đurđević, Z. i dr. (2013). *Presude Europskog suda za ljudska prava protiv Republike Hrvatske u kaznenim predmetima.* Zagreb: Sveučilište u Zagrebu - Pravni fakultet.

Milivojević, L., Gluščić, S. (2015). *O kaznenim djelima koja prijete organiziranom životu u zajednici.* U: Zbornik radova s konferencije Istraživački dani Visoke policijske škole 2015. Zagreb: MUP RH.

Tomašević, G., Krapac, D., Gluščić, S. (2012). *Kazneno procesno pravo*. Zagreb: Narodne novine.

Zakon o državnom odvjetništvu (NN 76/09., 153/09., 116/10., 145/10., 57/11., 130/11., 72/13., 148/13., 33/15., 82/15.).

Zakon o kaznenom postupku (NN 152/08., 76/09., 80/11., 91/12. Odluka i Rješenje USRH, 143/12., 56/13., 145/13. i 152/14.**).**

Stjepan Gluščić
Lana Milivojević

REGULATION OF THE INSTITUTE OF INDEPENDENCE AND EFFECTIVENESS OF INVESTIGATION AND INDEPENDENCE OF INVESTIGATORS IN THE CROATIAN CRIMINAL PROCEEDINGS

Summary

The paper analyses the impact of the decisions of the Croatian Constitutional Court and those of the European Court of Human Rights on the normative system and on the interpretation of the fulfilment of the requirements necessary for the implementation of effective and independent investigations and for the independence of investigators in criminal proceedings. In recent years, the ECTHR and the Republic of Croatia Constitutional Court have delivered several significant judgments establishing that in some cases an effective and independent investigation of the existence of a reasonable doubt about the commission of a criminal offence was not carried out. In the latest amendments to the Criminal Procedure Act, the Public Attorney's Office Act as well as to the Police Duties and Powers Act, the procedures and rules for the fulfilment of the standards required for an independent and effective investigation have been regulated.

Key words: *Constitutional Court, Criminal Procedure, Investigation, Investigators.*

PREGLEDNI ČLANAK

Petar Veić[300]
Igor Martinović[301]

IZAZOVI POLICIJSKOG POSTUPANJA U OTKRIVANJU I DOKAZIVANJU RAČUNALNOG KRIMINALA

Sažetak
Kaznenim zakonom iz 2011. reformirana su računalna kaznena djela. Ona su prvi put izdvojena u zasebnu glavu XXV. (kaznena djela protiv računalnih sustava, programa i podataka) čime je zakonodavac simbolički istaknuo opasnost ovog oblika kriminala. U nastojanju usklađivanja hrvatskog zakonodavstva s Konvencijom o kibernetičkom kriminalu i Okvirnom odlukom (sada Direktivom) o napadima na informacijske sustave, uvedena su nova kaznena djela i izmijenjena dotadašnja. Danas su računalna kaznena djela sadržana ponajprije u glavi XXV., ali u širem smislu računalnom kriminalu pripadaju i sva druga kaznena djela koja se mogu počiniti korištenjem informatičkih tehnologija (npr. iskorištavanje djece za pornografiju, prostitucija, javno poticanje na nasilje i mržnju itd.). Dinamične zakonske promjene i stalni napredak informatičke tehnologije, koji omogućava sve kompleksnije oblike računalnog kriminala, suočavaju policiju s dva temeljna izazova. Prvi izazov sastoji se u ranom i pravilnom prepoznavanju zabranjenih ponašanja te u razlikovanju potencijalnog računalnog kriminala od nepoželjnih ponašanja kojima se ne ostvaruju obilježja kaznenih djela. Daljnji izazov sastoji se u korištenju policijskih ovlasti na način koji je usklađen sa Zakonom o policijskim poslovima i ovlastima i Zakonom o kaznenom postupku, a sve u svrhu da se prikupe informacije koje će se moći koristiti u eventualnom kaznenom postupku protiv počinitelja računalnih kaznenih djela.

Ključne riječi: *računalni kriminal, policijske ovlasti, Kazneni zakon, Zakon o policijskim poslovima i ovlastima, Zakon o kaznenom postupku.*

1. UVOD

Statistički podaci za 2014. godinu[302] pokazuju da se računalnoj sigurnosti i računalnom kriminalu u hrvatskom pravnom sustavu još uvijek ne pristupa dovoljno ozbiljno. Naime, prijavljenih punoljetnih osoba za počinjenje svih kaznenih djela protiv računalnih sustava, programa i podataka (glava XXV. Kaznenog zakona; u daljnjem tekstu: KZ) bilo je te godine ukupno 290, od čega se njih 207 ubraja u računalnu prijevaru. Optuženih je u istom razdoblju

[300] Prof. dr. sc., redoviti profesor, predstojnik Katedre za kazneno postupovno pravo Pravnog fakulteta Sveučilišta u Rijeci
[301] Doc. dr. sc., docent na Katedri za kazneno postupovno pravo Pravnog fakulteta Sveučilišta u Rijeci
[302] Punoljetni počinitelji kaznenih djela, prijave, optužbe i osude u 2014., Statistička izvješća 1551, Zagreb, 2015.

bilo 90, od čega 81 za računalnu prijevaru, dok je osuđenih bilo ukupno 83, od čega 78 za računalnu prijevaru. Prema tome, izuzmemo li računalnu prijevaru, koju je u praksi katkad vrlo jednostavno prepoznati i sankcionirati (npr. kada je počinjena kupovanjem robe preko interneta tuđom debitnom karticom), osuđenih punoljetnih počinitelja za počinjenje svih kaznenih djela iz glave XXV. KZ-a bilo je 2014. godine ukupno pet.

Činjenica da je za šest računalnih kaznenih djela u godinu dana ukupno osuđeno svega pet osoba, ukazuje na izuzetno visoku „tamnu brojku" računalnog kriminala. Više je uzroka takvog stanja. Jedan je zasigurno i okolnost da je novi KZ, koji je stupio na snagu 2013. godine, uveo nemale promjene u području računalnih kaznenih djela: prvi put su ti delikti objedinjeni u zajedničku zakonsku glavu, a jedno kazneno djelo iz starog zakona (povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava iz članka 223. Kaznenog zakona iz 1997.) „razbijeno" je na čak pet kaznenih djela.

Međutim, ne treba se zavaravati da su zakonske promjene jedini uzrok velike tamne brojke. Očito je da tijela koja sudjeluju u kaznenom progonu – od policije, preko državnog odvjetništva pa sve do sudova – imaju određenih poteškoća s pravilnim prepoznavanjem računalnog kriminala i njegovim podvođenjem pod odgovarajuću zakonsku normu. Za takvo što potrebno je znanje o načinu funkcioniranja računala i zlouporabama koje u tom području postoje. Složenija specijalistička znanja o računalnim tehnologijama ne mogu se, dakako, zahtijevati od svakog policijskog službenika, državnog odvjetnika i suca, no nije dovoljno ni oslanjati se na vještačenja kao oblik „outsourcinga" jer se vještačko znanje najčešće može koristiti tek nakon što računalno kazneno djelo – barem u osnovnim konturama – u konkretnom slučaju već bude prepoznato. Ključnu ulogu u tom procesu ima policija jer upravo ona provodi to prepoznavanje tj. postavlja preliminarnu kriminalističku diferencijalnu „dijagnozu",[303] bez koje je učinkovit kazneni progon računalnog kriminala nemoguć.

Daljnji izazov s kojim se policija suočava u ovoj domeni jest kako na zakonit i učinkovit način primjenjivati policijske ovlasti predviđene Zakonom o policijskim poslovima i ovlastima (u daljnjem tekstu: ZPPO) i Zakonom o kaznenom postupku (u daljnjem tekstu: ZKP) te time osigurati mogućnost da se prikupljene informacije koriste kao dokazi u kaznenom postupku protiv počinitelja računalnih kaznenih djela. U tom kontekstu, od izuzetne su važnosti radnja provjere uspostavljanja elektroničke komunikacije (čl. 68. ZPPO-a) i provjere uspostavljanja telekomunikacijskog kontakta (čl. 339.a ZKP-a), radnja presretanja, prikupljanja i snimanja računalnih podataka (čl. 332. st. 1. toč. 2.), pretraga računala (čl. 257. ZKP-a) te privremeno oduzimanje računalnih podataka (čl. 263. ZKP-a i čl. 59. ZPPO-a).

[303] O sadržaju pojma v. Pavišić/Modly/Veić, Kriminalistika, Knjiga 1, Zagreb, 2006., str. 152.

2. RAČUNALNA KAZNENA DJELA

2.1. Računalna kaznena djela u užem i širem smislu

Kaznena djela protiv računalnih sustava, programa i podataka uređena su glavom XXV. KZ-a po uzoru na Konvenciju Vijeća Europe o kibernetičkom kriminalu i Okvirnu odluku (sada Direktivu) o napadima na informacijske sustave. Djelima iz te glave štite se različite društvene vrijednosti odnosno pravna dobra, kao što su privatnost, sigurnost i imovina. Zakonodavcu kao kriterij za grupiranje računalnih delikata u zajedničku glavu nije poslužilo zajedničko zaštićeno pravno dobro, nego činjenica da se sva ta djela čine na računalnom sustavu, programu ili podatku kao objektu radnje.[304] Takav kriterij kategorizacije delikata otežava utvrđivanje smisla konkretnog kaznenog djela, ali on ima i svojih prednosti. Jedna od njih je da su najvažnija računalna kaznena djela „okupljena" na jednome mjestu, što policiji može olakšati prepoznavanje računalnog kriminala i međusobno razlikovanje pojedinih njegovih oblika.[305]

Kada se govori o računalnom kriminalu odnosno računalnim kaznenim djelima, treba imati u vidu da kaznena djela propisana u glavi XXV. (računalna kaznena djela „u užem smislu") nisu jedina koja se mogu počiniti uporabom računalnih sustava, programa i podataka: u širem smislu, računalnim kaznenim djelima pripadaju i druga kaznena djela (npr. prijetnja, iskorištavanje djece za pornografiju, javno poticanje na nasilje i mržnju itd.) ako je pri njihovu počinjenju uporabljeno računalo. Takva računalna kaznena djela („u širem smislu") raspršena su u različitim zakonskim glavama, npr. u glavi XIII. (kaznena djela protiv osobne slobode), glavi XVII. (kaznena djela spolnog zlostavljanja i iskorištavanja djeteta) i glavi XXX. (kaznena djela protiv javnog reda). U nastavku ćemo se ograničiti samo na računalna kaznena djela „u užem smislu", kao ona koja su u ovom kontekstu najrelevantnija i čije je prepoznavanje i učinkovito suzbijanje u praksi najproblematičnije.

2.2. Pojmovi računalnog sustava, računalnog podatka, računalnog programa i elektroničkog dokaza

Temeljni zakonski pojmovi čije je razumijevanje nužno za shvaćanje problematike računalnih kaznenih djela jesu računalni sustav, računalni program i računalni podatak. Ta tri pojma KZ definira u članku 87. S procesnog je aspekta važan i pojam elektroničkog (digitalnog) dokaza, definiran u članku 202. stavku 33. ZKP-a.

(1) Računalni sustav je svaka naprava ili skupina međusobno spojenih ili povezanih naprava, od kojih jedna ili više njih na osnovi programa automatski obrađuju podatke, kao i računalni podaci koji su u njega spremljeni, obrađeni, učitani ili preneseni za svrhe njegova

---

[304] Za pojašnjenje razlike između pravnog dobra i objekta radnje v. Novoselec/Bojanić, Opći dio kaznenog prava, Zagreb, 2013., str. 127.-128.; Grozdanić/Škorić/Martinović, Opći dio kaznenog prava, Rijeka, 2013. str. 98.

[305] Vuletić i Nedić odobravaju izdvajanje računalnih delikata u zasebnu zakonsku glavu, smatrajući da se time postiže „bolja preglednost". V. Vuletić/Nedić, Računalna prijevara u hrvatskom kaznenom pravu, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, 2/2014, str. 684.

rada, korištenja, zaštite i održavanja (čl. 87. st. 18. KZ-a). Navedena definicija obuhvaća kako fizičke dijelove računalnog sustava (hardver), tako i računalne podatke (softver). Pojam računalnog sustava obuhvaća naprave koje na osnovi programa automatski[306] obrađuju podatke, npr. stolna, prijenosna i tablet računala, „pametne“ telefone i satove i sl.[307] Te naprave omogućuju obradu (elektronskih, magnetnih ili drugih) podataka koje čovjek ne može izravno opažati.[308] One se mogu više puta programirati tijekom korištenja kako bi obavljale širok spektar funkcija. U pojam računalnog sustava ulaze i naprave koje su spojene ili povezane (bilo kabelom, bilo bežično) s napravom koja automatski obrađuje podatke (tzv. periferni uređaji). Postoje ulazni (npr. tipkovnica, miš, skener), izlazni (npr. pisač, monitor) i ulazno-izlazni periferni uređaji (npr. modem).

Definiciji računalnih sustava pridodani su i računalni podaci koji su u taj sustav spremljeni, obrađeni, učitani ili preneseni za svrhe njegova rada, korištenja, zaštite i održavanja. U tu skupinu ne ulaze računalni podaci koji su spremljeni na vanjskoj memoriji (CD-u, prijenosnom hard disku itd.) ako ta memorija nije učitana putem računalnog sustava.

(2) Računalni podatak je svako iskazivanje činjenica, informacija ili zamisli u obliku prikladnom za obradu u računalnom sustavu (čl. 87. st. 19. KZ-a). Posebnost računalnih podataka je u tome što su pohranjeni u obliku koji nije neposredno dostupan čovjeku,[309] obično u binarnom znakovnom sustavu. Njihov sadržaj korisniku postaje dostupan tek korištenjem softvera (npr. programa za obradu teksta).

Računalni podaci mogu biti pohranjeni na različitim vrstama medija, a najčešće magnetnim (hard disk, disketa, magnetna vrpca, magnetna kartica), optičkim (CD, DVD i sl.) i poluvodičkim medijima (RAM, USB memorija, memorijska kartica). Oni mogu biti pohranjeni i u oblaku *(cloud)*.

(3) Računalni program je skup računalnih podataka koji su u stanju prouzročiti da računalni sustav izvrši određenu funkciju (čl. 87. st. 20. KZ-a).

(4) Elektronički (digitalni) dokaz je podatak koji je kao dokaz pribavljen u elektroničkom obliku prema odredbama ZKP-a (čl. 202. st. 32. ZKP-a). U kaznenom postupku može se kao dokaz pojaviti i elektronička isprava (definirana u čl. 4. alineji 1. Zakona o elektroničkoj ispravi). Svako korištenje SMS ili MMS poruka, elektronička pošta, plaćanje s bankovnih računa i pomoću platnih kartica, korištenje navigacijskog sustava i sl. smatra se elektroničkim dokazom.

2.3. Neovlašteni pristup (čl. 266. KZ-a)

Djelo čini tko neovlašteno pristupi računalnom sustavu ili računalnim podacima (čl. 266. st. 1. KZ-a). Pristupanje računalnim sustavima moguće je na različite načine; tehničke inovacije neprekidno omogućavaju nove oblike pristupa. U svakom slučaju, počinitelj se ne

---

[306] „Automatski“ znači „bez izravne ljudske intervencije“. V. Obrazloženje *(Explanatory report)* Konvencije o kibernetičkom kriminalu, § 23.
[307] Slično Kokot, Kaznenopravna zaštita računalnih sustava, programa i podataka, Zagrebačka pravna revija, 3/2014, str. 305.
[308] Schönke/Schröder-*Stree/Hecker*, § 303b, r. br. 8.
[309] Münchener Kommentar - *Erb*, § 269, r. br. 13.

mora nalaziti u fizičkoj blizini računalnog sustava kojem pristupa, već mu može pristupiti i posredstvom drugog računala (putem interneta, LAN-a itd.).[310] U pojam pristupanja ulaze i napadi pomoću malicioznih računalnih programa (npr. trojanaca i drugih špijunskih programa) namijenjenih praćenju procesa na drugom računalu, prikupljanju tuđih podataka i sl. Slanjem virusa najčešće se ne ostvaruje pristup tuđem računalnom sustavu, a time ni obilježja kaznenog djela neovlaštenog pristupa, ali je moguća odgovornost počinitelja za druga kaznena djela, npr. za (dovršeno ili pokušano) oštećenje računalnih podataka (čl. 268. KZ-a).

Računalnim podacima moguće je pristupiti i bez pristupa tuđem računalnom sustavu, npr. upadom na tuđi profil na društvenoj mreži putem interneta, učitavanjem datoteka s tuđeg CD-a ili pristupanjem podacima o stanju tuđeg bankovnog računa korištenjem krivotvorene kartice na bankomatu. I počinitelj koji neovlašteno otvori tuđu elektroničku poštu, poruku poslanu putem društvenih mreža i sl., neovlašteno pristupa računalnim podacima.[311] Pristupiti računalnim podacima može se i kada su ti podaci pohranjeni u oblaku *(cloud)*. Samim pristupom mediju za pohranu računalnih podataka (npr. spajanjem žrtvina USB štapića s počiniteljevim računalom) ne ostvaruju se obilježja djela; potrebno je da počinitelj pristupi i podacima koji su pohranjeni na tom mediju.

Pravo pristupa računalnom sustavu obično će imati vlasnik računalnog sustava, ali to pravo istodobno s vlasnikom mogu imati i treće osobe (npr. na temelju ugovora o radu). Računalni podaci nisu stvari pa je pitanje tko im je ovlašten pristupiti složenije. Tu ovlast ima osoba kojoj su podaci namijenjeni, a to je u pravilu osoba koja ih je stvorila i pohranila ili osoba kojoj su podaci preneseni (npr. zaprimljeni elektroničkom poštom). Činjenica da se računalni podaci u sadržajnom smislu odnose na počinitelja ili da je on vlasnik medija na kojem su pohranjeni ne daje mu unaprijed ovlast pristupiti tim podacima. Za razliku od poslovno relevantnih podataka, privatnim podacima zaposlenika poslodavac nije ovlašten pristupiti ni onda kada je računalni sustav u vlasništvu poslodavca. Mrežni administrator ovlašten je pristupiti jedino podacima koji se odnose na tehničko funkcioniranje računala.[312] Treća osoba računalnom sustavu ili podacima smije pristupiti samo uz pristanak ovlaštenika.

Djelo može biti počinjeno jedino s namjerom (izravnom ili neizravnom). Poseban motiv nije potreban pa ovo djelo čini i npr. haker koji neovlašteno pristupi tuđem računalnom sustavu samo kako bi pokazao svoju informatičku vještinu.[313]

Kažnjiv je i pokušaj (st. 3.). Tipičan primjer pokušaja su slučajevi u kojima se pristup izjalovi zbog učinkovite računalne zaštite (npr. kada pristup računalu onemogući *firewall*), a mogući su i drugi uzroci (npr. nesposobnost hakera, neispravnost CD-a).[314]

2.4. Ometanje rada računalnog sustava (čl. 267. KZ-a)

---

[310] Slično i Turković i dr., Komentar Kaznenog zakona, Zagreb, 2013., str. 342.
[311] U tom slučaju postojat će prividni stjecaj s kaznenim djelom povrede tajnosti pisama i drugih pošiljaka (čl. 142. KZ-a), no to pitanje nije relevantno za otkrivačku djelatnost pa se njime ovdje nećemo baviti.
[312] Schönke/Schröder - *Lenckner/Eisele*, § 202a, r. br. 9-10; Münchener Kommentar -*Graf*, § 202a, r. br. 20-23. i 63.
[313] Münchener Kommentar - *Graf*, § 202a, r. br. 71.
[314] Za kriminalističke aspekte neovlaštenog pristupa v. Pavišić/Modly/Veić, Kriminalistika, Knjiga 2, Rijeka, 2012., str. 616.-618.

Djelo čini tko onemogući ili otežа rad ili korištenje računalnog sustava, računalnih podataka ili programa ili računalnu komunikaciju (čl. 267. st. 1.).

Onemogućiti ili otežati rad ili korištenje *računalnog sustava* može se napadom na hardver (npr. fizičkim uništenjem procesora ili instaliranjem *trojan hardwarea*), ali i softver, osobito na tzv. sustavne programe (sistemski softver).[315] Da bi odgovarao za ovo djelo, počinitelj ne mora pristupiti podacima pohranjenim u okviru napadnutog sustava niti narušiti njihovu cjelovitost.[316]

Rad ili korištenje *računalnih podataka ili programa* moguće je onemogućiti ili otežati radnjama opisanima u članku 268. stavku 1.,[317] ali i na druge načine, npr. instaliranjem malicioznog programa koji usporava rad drugih programa.

Onemogućiti ili otežati *računalnu komunikaciju* moguće je npr. DoS *(Denial of Service)* napadom na internetski poslužitelj *(web server)* pri kojem se poslužitelj „zagušuje" velikim brojem zahtjeva, što dovodi do nemogućnosti otvaranja napadnute internetske stranice. Obilježja ovog djela ne ostvaruju se slanjem neželjene elektroničke pošte *(spamming)*, osim ako je priljev neželjene pošte tolik da se njime usporava rad računalnog sustava ili računalna komunikacija.[318]

Djelo je moguće počiniti jedino s namjerom (izravnom ili neizravnom). Kažnjiv je i pokušaj (st. 2.).

2.5. Oštećenje računalnih podataka (čl. 268. KZ-a)

Djelo čini tko neovlašteno u cijelosti ili djelomično ošteti, izmijeni, izbriše, uništi, učini neuporabljivim ili nedostupnim ili prikaže nedostupnim tuđe računalne podatke ili programe (čl. 268. st. 1. KZ-a).

Radnjama oštećenja, izmjene, brisanja, uništenja i činjenja neuporabljivim obuhvaćeni su svi zahvati kojima se narušava cjelovitost računalnih podataka odnosno programa. Cjelovitost podataka ili programa moguće je narušiti softverskim putem (npr. brisanjem datoteke ili instaliranjem virusa koji izmjenjuje podatke), ali i fizičkim uništenjem ili oštećenjem medija (npr. USB štapića, CD-a, platne kartice) na kojem su pohranjeni. Samim kopiranjem (presnimavanjem) podataka, kao niti izmjenom presnimljenih podataka ne ostvaruju se obilježja djela.[319] Djela nema ni kada počinitelj podatke stavi u „kantu za smeće" (*recycle bin*) jer ti podaci nisu nepovratno izbrisani s računala.[320]

Obilježja djela iz članka 268. stavka 1. mogu se ostvariti i tako da se podaci učine nedostupnim (npr. oduzimanjem CD-a s pohranjenim podacima; blokiranjem pristupa datotekama pomoću uvođenja pristupnih šifri – Županijski sud u Osijeku, Kž-48/15) ili prikažu nedostupnim (npr. sakrivanjem datoteka unutar napadnutog računala uz pomoć

---

[315] U slučaju napada na softver (npr. slanjem virusa) postojat će prividni stjecaj s djelom iz čl. 268. KZ-a.
[316] Turković i dr., op. cit., str. 342.
[317] U tom slučaju postojat će prividni stjecaj s djelom iz čl. 268. KZ-a.
[318] Obrazloženje *(Explanatory report)* Konvencije o kibernetičkom kriminalu, § 69.
[319] Münchener Kommentar - *Wieck/Noodt*, § 303a, r. br. 15.
[320] Kokot, op. cit., str. 318.

virusa). Tim se radnjama žrtvi onemogućuje pristup podacima odnosno programima iako se pritom ne narušava njihova cjelovitost. Činjenica da žrtva kasnije može rekonstruirati podatke ne utječe na postojanje djela.[321]

Djelo je moguće počiniti jedino s namjerom (izravnom ili neizravnom). Kažnjiv je i pokušaj (st. 2.). Primjer pokušaja je instalacija programa (npr. virusa) koji je privremeno neaktivan, ali je sposoban u budućnosti izazvati brisanje podataka.[322]

2.6. Neovlašteno presretanje računalnih podataka (čl. 269. KZ-a)

Djelo čini tko neovlašteno presretne ili snimi nejavni prijenos računalnih podataka, uključujući i elektromagnetsku emisiju računalnog sustava, ili drugome učini dostupnim tako pribavljene podatke (čl. 269. st. 1. KZ-a).

Pod prijenosom računalnih podataka najčešće se misli na prijenos podataka između dvaju računalnih sustava, npr. elektroničkom poštom, internetskom telefonijom (*VoIP*), *online chatom, instant messaging* aplikacijama (npr. *WhatsApp, Viber, Skype*). Nebitno je odvija li se prijenos podataka kabelima ili bežično (putem WLAN-a). Djelo se odnosi samo na podatke koji se u trenutku djela nalaze u postupku prijenosa, a ne i podatke koji su već preneseni i pohranjeni. Prijenos traje i dok se podaci nalaze na poslužitelju *(serveru)* spremni da ih preuzme primatelj. Neovlaštenim uključivanjem na tuđu nezaštićenu bežičnu mrežu (WLAN) ne ostvaruju se obilježja ovog djela jer se time ne presreće prijenos podataka, nego se stvara vlastita komunikacija počinitelja s mrežom.

Prijenos računalnih podataka mora biti nejavan. Pojam „nejavan“ ne odnosi se na sadržaj podataka, nego na način njihova prijenosa pa djelo može postojati i kada su u pitanju javno dostupni podaci. Pri ocjeni je li prijenos nejavan, odlučujuće je je li on namijenjen ograničenom krugu korisnika (npr. pismo poslano elektroničkom poštom) ili širem, nedefiniranom broju korisnika tj. općoj javnosti (npr. vijest na otvorenom novinskom portalu). Prijenos može biti nejavan i kada se obavlja putem interneta.[323]

Uz pomoć suvremene tehnologije računalni podaci mogu se neovlašteno pribaviti i neizravnim putem, na način da ih se rekonstruira iz elektromagnetske emisije računalnog sustava. Tom se radnjom obilježja djela ostvaruju unatoč tome što se ne presreće niti snima prijenos računalnih podataka u užem smislu riječi.

Počinitelj prijenos računalnih podataka ne mora snimiti odnosno pohraniti; dovoljno je i njegovo presretanje (npr. prisluškivanje razgovora, čitanje elektroničke pošte, „špijuniranje“ internetskog prometa pomoću tzv. *sniffer* alata). Obilježja djela ostvaruje i osoba koja nije sama presrela ili snimila prijenos podataka, nego je tako pribavljene podatke učinila dostupnim trećim osobama.

Djelo može biti počinjeno jedino s namjerom (izravnom ili neizravnom). Kažnjiv je i pokušaj (st. 2.). Tipičan primjer pokušaja su slučajevi u kojima se presretanje odnosno snimanje izjalovi zbog učinkovite računalne zaštite.

---

[321] Münchener Kommentar - *Wieck/Noodt*, § 303a, r. br. 13.
[322] Schönke/Schröder - *Stree/Hecker*, § 303a, r. br. 11.
[323] Münchener Kommentar - *Graf*, § 202b, r. br. 10; Nomos Kommentar-*Kargl*, § 202b, r. br. 5.

Podaci nastali ovim kaznenim djelom obvezno se oduzimaju i uništavaju (st. 3.).

2.7. Računalno krivotvorenje (čl. 270. KZ-a)

Djelo čini tko neovlašteno izradi, unese, izmijeni, izbriše ili učini neuporabljivim ili nedostupnim računalne podatke koji imaju vrijednost za pravne odnose, u namjeri da se oni uporabe kao vjerodostojni, ili tko takve podatke uporabi ili nabavi radi uporabe (čl. 270. st. 1. KZ-a).

Razlog uvođenja ovog djela u KZ je u tome što pojam isprave (čl. 87. st. 15.) obuhvaća samo predmete, pa zaštitu vjerodostojnosti tzv. *računalnih isprava* – koje nisu predmeti – nije moguće ostvariti u okviru delikata kojima se inkriminira krivotvorenje „klasičnih" isprava. Pojam računalne isprave ovdje se inače koristi kao sinonim za „računalne podatke koji imaju vrijednost za pravne odnose. Taj pojam ima šire značenje od pojma elektroničke isprave koji je definiran u Zakonu o elektroničkim ispravama. Prema članku 3. alineji 5. i članku 7. tog Zakona, obvezan dio elektroničke isprave je elektronički potpis, no on nije nužno i sastavni dio računalne isprave u smislu KZ-a.

Predmet ovog djela mogu biti računalni podaci koji sadrže ljudsku izjavu (npr. dokument pisan u programu za obradu teksta), ali i oni koji ne sadrže ljudsku izjavu (npr. digitalna snimka koju je načinila nadzorna kamera).

Za razliku od znakova koji sačinjavaju ispravu (npr. slova na komadu papira), računalni podaci obično nisu vezani za određeni predmet. Oni se mogu premještati (kopirati) s jednog medija na drugi (npr. s računala na USB štapić) pa i unutar istog medija. Pukim umnožavanjem računalnih podataka u pravilu se ne ostvaruju obilježja računalnog krivotvorenja. Iznimno, računalni podaci mogu biti strogo vezani za određeni predmet. To je slučaj ponajprije kod čipiranih kartica (npr. platna kartica, zdravstvena iskaznica). Kopiranjem takvih podataka na drugi medij (npr. na računalo) moguće je počiniti računalno krivotvorenje pod uvjetom da imaju vrijednost za pravne odnose.[324]

Da bi bili objekt računalnog krivotvorenja, računalni podaci moraju imati *vrijednost za pravne odnose*. Tu vrijednost imaju oni računalni podaci koji su određeni ili barem podobni služiti kao dokaz tih činjenica, tj. samo oni koji imaju dokaznu funkciju. Računalni podaci koji nisu relevantni za pravni život jer ih je korisnik izradio isključivo za svoje privatne potrebe nemaju vrijednost za pravne odnose pa ne mogu biti objekt računalnog krivotvorenja.[325]

Da bi mogla služiti kao dokaz u pravnom prometu, računalna isprava mora biti vjerodostojna (prava, autentična). Računalna isprava je vjerodostojna kada osoba koja je na njoj navedena kao izdavatelj to doista i jest. Izdavatelj ne mora biti izričito naveden u računalnoj ispravi; dovoljno je da se iz cjelokupne računalne isprave može zaključiti tko je on. Računalna isprava koja ne potječe od onoga tko je na njoj (izričito ili barem konkludentno) naveden kao izdavatelj predstavlja lažnu računalnu ispravu, tj. računalnu ispravu čijom se izradom ostvaruju obilježja računalnog krivotvorenja. Za opstojnost djela nije važno je li

[324] Münchener Kommentar - *Erb*, § 269, r. br. 26-28.
[325] Münchener Kommentar - *Erb*, § 269, r. br. 12.

sadržaj lažne računalne isprave istinit ili neistinit. Nisu ostvarena obilježja računalnog krivotvorenja kada počinitelj unese u računalnu ispravu neistinit sadržaj ali takvu ispravu elektronički potpiše svojim pravim imenom.

Lažnu računalnu ispravu predstavlja i elektronička pošta (pod uvjetom da sadržava podatke koji imaju vrijednost za pravne odnose) ako je potpisana tuđim imenom ili ako se na drugi način može zaključiti tko je njezin izdavatelj, neovisno o tome sadržava li i elektronički potpis.[326] Navedeno vrijedi i za prilog (*attachment*) elektroničkoj pošti. Internetska stranica također može predstavljati lažnu računalnu ispravu, pod uvjetom da se iz nje dade iščitati tko je njezin izdavatelj i da sadrži pravno relevantne podatke[327] (npr. internetska stranica na kojoj banka navodi opće uvjete poslovanja).

U pojam računalne isprave (tj. računalnih podataka koji imaju vrijednost za pravne odnose) ulaze i različiti *tehnički zapisi* (npr. elektrokardiogram, tahografski listić) pod uvjetom da ih stroj ne bilježi izravno na papir ili koji drugi predmet, nego ga pohranjuje u obliku računalnih podataka. Takva automatski generirana računalna isprava može se sastojati od slova, brojki, dijagrama, slika, zvukova ili drugih zapisa. Iz nje mora biti jasno na koji se događaj zapis odnosi.[328]

Kao i računalna isprava koja sadrži izjavu čovjeka, automatski generirana računalna isprava mora biti vjerodostojna (prava, autentična) da bi mogla služiti kao dokaz u pravnom prometu. Vjerodostojnost se u ovom slučaju nešto drugačije tumači. Automatski generirana računalna isprava vjerodostojna je kada podaci u njoj odgovaraju podacima koje je računalni sustav automatski zabilježio. Takva isprava stoga može biti vjerodostojna i kada podaci u njoj nisu istiniti (npr. zato što stroj ne radi ispravno).

Računalno krivotvorenje moguće je počiniti radnjama izrade, unošenja, izmjene, brisanja, činjenja neuporabljivim i činjenja nedostupnim računalnih podataka. Svrha svih tih radnji je zavarati žrtvu o osobi izdavatelja računalne isprave. Sve one mogu se podvesti pod dvije temeljne radnje: izradu lažne računalne isprave i preinačenje prave (vjerodostojne) računalne isprave.

Izrada lažne računalne isprave u zakonu je opisana radnjama izrade ili unošenja računalnih podataka. U pojam izrade ulazi svako izdavanje računalne isprave pomoću kojeg izdavatelj želi prikazati kao da je takvu ispravu izdala druga osoba. Čest primjer takve radnje je slanje elektroničkom poštom obavijesti o tobožnjem dobitku na lutriji, potpisane tuđim imenom, u kojoj se od žrtve traži da pošalje privatne podatke kao što su broj platne kartice ili različite šifre (tzv. *phishing email*).[329] Primjer je i izrada internetske stranice koju počinitelj pripisuje drugoj osobi (npr. poznatom proizvođaču) ili neovlašteno popunjavanje elektroničkog blanketa (npr. popunjavanje pristupnice u političku stranku u ime druge osobe).

Preinačenje prave (vjerodostojne) računalne isprave u zakonu je opisano radnjama

---

[326] Elektronički potpis znači skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i vjerodostojnosti potpisanoga elektroničkog dokumenta (čl. 2. toč. 1. Zakona o elektroničkom potpisu).
[327] Schönke/Schröder - *Heine/Schuster*, § 269, r. br. 14.
[328] Münchener Kommentar - *Erb*, § 268, r. br. 27.
[329] Opširnije o *phishingu* („nigerijskoj prijevari") v. Vuletić/Nedić, op. cit., str. 682; Bača/Ćosić, Prevencija računalnog kriminaliteta, Policija i sigurnost, 1/2013, str. 155-156.

izmjene, brisanja, činjenja neuporabljivim i činjenja nedostupnim računalnih podataka. U pojam preinačenja ulazi svaka izmjena izjave sadržane u pravoj (vjerodostojnoj) računalnoj ispravi radi dobivanja izjave koju izdavatelj nije dao (npr. kada počinitelj izmijeni podatke o kamati na internetskoj stranici banke). Preinačiti pravu računalnu ispravu moguće je i brisanjem računalnih podataka (npr. brisanjem pojedinih odredaba sadržanih u općim uvjetima poslovanja koji su objavljeni na internetskoj stranici trgovačkog društva). Računalnu ispravu preinačuje i tko računalne podatke, radi dobivanja izjave koju izdavatelj nije dao, učini neuporabljivim ili nedostupnim (npr. napadne ih malicioznim programom kako bi trajno uklonio ili „sakrio“ važan dio internetske stranice).

Posebni načini počinjenja javljaju se kod automatski generiranih računalnih isprava. Primjerice, počinitelj može na računalu sam izraditi tobožnji tehnički zapis tvrdeći da se radi o zapisu koji potječe od određenog uređaja (npr. izradi lažni računalni zapis masenog spektrometra o prisutnosti steroida u urinu), preinačiti originalni zapis (npr. izmijeniti brojke na zapisu), izbrisati dio zapisa koji ne odgovara njegovim interesima itd. Lažni zapis može se izraditi i uz pomoć prethodne manipulacije na računalnom programu koji bilježi podatke (npr. preprogramiranjem električne vage na način da bilježi veću masu od stvarne).

Djelo čini i tko *uporabi* lažnu računalnu ispravu ili je *nabavi* radi uporabe. Uporaba je svaka radnja kojom se lažna računalna isprava čini dostupnom žrtvi kako bi se ova upoznala s njezinim sadržajem.

Djelo mora biti počinjeno s namjerom (izravnom ili neizravnom). Moguće je i da počiniteljeva namjera bude da netko treći, a ne on sam, uporabi računalnu ispravu. Namjera se ne može pripisati počinitelju koji pod lažnim imenom sudjeluje u komunikaciji putem interneta (npr. lažno se predstavljajući kao poznata osoba) ako pritom ne očekuje da bi njegove izjave mogle izazvati pravno relevantne učinke, tj. da bi netko tim izjavama doista mogao pripisati vrijednost za pravne odnose.[330] Pokušaj je kažnjiv (st. 2.).

Podaci nastali računalnim krivotvorenjem obvezno se oduzimaju i uništavaju (st. 3.).[331]

2.8. Računalna prijevara (čl. 271. KZ-a)

Računalnu prijevaru čini tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, izmijeni, izbriše, ošteti, učini neuporabljivim ili nedostupnim računalne podatke ili ometa rad računalnog sustava i na taj način prouzroči štetu drugome (čl. 271. st. 1. KZ-a).

Smisao uvođenja ovog djela bio je u popunjavanju zakonskih praznina nastalih razvojem tehnologije, zbog kojih je pojedine računalne zlouporabe bilo nemoguće podvesti pod prijevaru ili druge „klasične“ imovinske delikte. Primjerice, upisivanjem tuđih podataka u aplikaciju za internetsko bankarstvo s ciljem da se novac prebaci na račun počinitelja ne ostvaruju se obilježja „klasične“ prijevare (čl. 236. KZ-a) jer se kod prijevare traži dovođenje

[330] Münchener Kommentar - *Erb*, § 269, r. br. 42.
[331] Za kriminalističke aspekte računalnog krivotvorenja v. Pavišić/Modly/Veić, Kriminalistika, Knjiga 2, str. 619.-620.

drugog (čovjeka) u zabludu, dok se ovdje u „zabludu“ dovodi računalni program. Pri razmatranju je li u pojedinom slučaju počinjena računalna prijevara, korisna je usporedba u kojoj se „prevareno“ računalo u mislima zamjenjuje čovjekom. Tako se, primjerice, do zaključka da podizanje novca ukradenom karticom i PIN-om predstavlja računalnu prijevaru dolazi usporedbom sa slučajem u kojem bi počinitelj novac podignuo na šalteru banke dovevši bankovnog službenika u zabludu predočenjem ukradenih isprava, a koji bi predstavljao „klasičnu“ prijevaru.

Zakon predviđa sedam različitih radnji počinjenja (unos, izmjenu, brisanje, oštećenje, činjenje neuporabljivim i činjenje nedostupnim računalnih podataka te ometanje rada računalnog sustava). Najvažnija od tih radnji je unos računalnih podataka.

Pojam unosa računalnih podataka izuzetno je širokog opsega. Tipičan slučaj računalne prijevare unosom računalnih podataka jest podizanje novca s bankomata neovlaštenim korištenjem tuđe platne kartice i PIN-a (npr. kada je počinitelj karticu pribavio krađom ili ju je krivotvorio ili mu je ona predana na čuvanje pa je kriomice doznao njezin PIN). Računalnu prijevaru čini i tko ukradenom ili krivotvorenom karticom ili karticom čiji je PIN protupravno nabavio bezgotovinski plaća robu ili usluge provlačenjem kartice kroz POS uređaj. Računalna prijevara u takvim slučajevima postoji neovisno o tome traži li se pri plaćanju PIN (najčešće kod debitnih kartica), potpis (npr. kod nekih kreditnih kartica) ili se transakcija provodi bez ikakve daljnje autorizacije (npr. pri plaćanju manjih iznosa). S bezgotovinskim plaćanjem u ovom je kontekstu izjednačeno i plaćanje putem interneta (npr. naručivanje robe preko *eBay*-a korištenjem podataka s tuđe kartice; kupnja bonova za mobitel putem interneta pomoću neovlašteno pribavljenih podataka s tuđih kartica – Vrhovni sud Republike Hrvatske, I Kž-201/07).

Raširena metoda počinjenja računalne prijevare je tzv. *skimming*. Tim pojmom označava se pribavljanje podataka s magnetne vrpce na platnoj kartici pomoću posebnog uređaja priključenog na bankomat uz istodobno pribavljanje PIN-a pomoću kamere kojom se promatra tipkovnica bankomata. Tako pribavljeni podaci s kartice koriste se kako bi se izradila krivotvorena kartica kojom se zatim podiže novac uz pomoć PIN-a. Računalne prijevare tipične su za plaćanja putem interneta, npr. kada počinitelj plati robu koristeći podatke koje je pribavio *phishingom* ili kada plaća karticom koju mu je prijatelj ostavio na čuvanje, jer se u „internet trgovinama“ za kupnju često ne traže nikakvi podaci osim onih zapisanih na samoj kartici.

Računalna prijevara postoji i u slučaju pristupa naplatnim internetskim uslugama (npr. internetskoj televiziji i sl.) posredstvom tuđih pristupnih podataka bez pristanka osobe kojoj su podaci namijenjeni ili uz upotrebu krivotvorenih podataka (npr. piratskih kartica za gledanje *Pay TV-a*). Preda li počinitelju pristupne podatke sama osoba kojoj su oni namijenjeni (npr. pretplatnik internetske televizije), obilježja djela neće biti ostvarena. Računalnom prijevarom ne smatra se ni korištenje tuđeg nezaštićenog WLAN-a ili WLAN-a čije je pristupne podatke počinitelju vlasnik mreže dao na slobodno korištenje.[332]

Računalnu prijevaru predstavlja i izrada prijevarnog programa (npr. kada programer prema narudžbi banke izradi program za obračun kamate, ali to učini tako da program

[332] Münchener Kommentar - *Wohlers/Mühlbauer*, § 263a, r. br. 57.

automatski prebacuje neprimjetan djelić kamate svakog klijenta na bankovni račun programera)[333] ili instalacija prijevarnog programa (npr. instaliranje tzv. *dialera*, tj. softvera koji prekida vezu s internetom i putem modema bira telefonski broj s visokom cijenom poziva).

Nužan element računalne prijevare je prouzročenje štete drugoj osobi. Šteta može biti prouzročena na imovini osobe kojoj su namijenjeni računalni podaci (tj. osobe koja je ovlaštena koristiti se računalnim sustavom), ali i na imovini treće osobe (bilo fizičke, bilo pravne).[334]

Djelo može biti počinjeno jedino s namjerom (izravnom ili neizravnom). Počinitelj mora imati cilj da sebi ili drugome pribavi protupravnu imovinsku korist. Pokušaj je kažnjiv. Pri računalnim prijevarama na bankomatu pokušaj postoji u trenutku stavljanja kartice u bankomat. Podaci nastali računalnim krivotvorenjem obvezno se oduzimaju i uništavaju (st. 3.).[335]

2.9. Zlouporaba naprava (čl. 272. KZ-a)

Djelo iz članka 272. stavka 1. čini tko izradi, nabavi, uveze, proda, posjeduje ili čini drugome dostupne uređaje ili računalne programe ili računalne podatke stvorene ili prilagođene za počinjenje kaznenih djela iz članka 266., članka 267., članka 268., članka 269., članka 270. i članka 271. ovoga Zakona s ciljem da ih se uporabi za počinjenje nekog od tih djela.

Predmet radnje mogu biti uređaji koji su *stvoreni* upravo za počinjenje kaznenog djela, npr. USB tipkovnica s ugrađenim hardverskim trojancem kojim se „špijuniraju“ podaci s računala. Međutim, to mogu biti i uređaji koji su *prilagođeni* za počinjenje djela, tj. koji se mogu koristiti i u dopuštene i u kriminalne svrhe (*dual-use devices*),[336] npr. minijaturna kamera koja može služiti u zakonite svrhe, ali i za počinjenje *skimminga*. Predmet radnje mogu biti *računalni podaci* odnosno *programi* koji su *stvoreni* za počinjenje kaznenog djela (tzv. *hacker tools* – npr. računalni crvi, virusi, trojanci), ali i podaci odnosno programi koji su *prilagođeni* za počinjenje djela, tj. koji se mogu koristiti i u dopuštene i u kriminalne svrhe. Primjer takvog programa je tzv. *packet analyzer* (*sniffer*), koji može koristiti mrežnom administratoru za analizu mrežnog prometa, ali i hakeru za presretanje tuđeg prometa podataka.

Djelo iz članka 272. stavka 2. čini tko izradi, nabavi, uveze, proda, posjeduje ili čini drugome dostupne računalne lozinke, pristupne šifre ili druge podatke kojima se može pristupiti računalnom sustavu s ciljem da ih se uporabi za počinjenje kaznenih djela iz članka 266., članka 267., članka 268., članka 269., članka 270. i članka 271. ovoga Zakona. Djelom nisu obuhvaćene šifre za pristup sobama, garažama, sefovima i sličnim objektima koji ne ulaze u kategoriju računalnog sustava.

---

[333] Primjer preuzet prema Münchener Kommentar - *Wohlers/Mühlbauer*, § 263a, r. br. 24.
[334] Tako i Vuletić/Nedić, op. cit., str. 685.
[335] Za kriminalističke aspekte računalne prijevare v. Pavišić/Modly/Veić, Kriminalistika, Knjiga 2, str. 621.-622.
[336] Obrazloženje *(Explanatory report)* Konvencije o kibernetičkom kriminalu, § 73.

Djelo iz stavka 1. ili 2. može biti počinjeno jedino s namjerom, pri čemu je dovoljna neizravna namjera. Počinitelj mora imati i cilj da se objekt radnje uporabi za počinjenje nekog od djela iz članaka 266.-271. On postoji i kada počinitelj nije isplanirao tijek djela u potpunosti, nego samo u glavnim crtama, npr. kada kupi *sniffer* alate kako bi hakirao tuđu bežičnu mrežu (WLAN), a da pritom još nije odlučio na koji će se točno način time okoristiti.[337] Pokušaj nije kažnjiv.

Posebne naprave (tj. uređaji) iz stavka 1. obvezno će se oduzeti, neovisno o tome postoji li opasnost da će se ponovno uporabiti za počinjenje kaznenog djela. Podaci iz stavka 1. i 2. će se uništiti (st. 4.).

3. POLICIJSKE OVLASTI U OTKRIVANJU I DOKAZIVANJU RAČUNALNOG KRIMINALA

3.1. Postupovne odredbe Konvencije o kibernetičkom kriminalu

Kada je riječ o postupovnim mogućnostima u odnosu na računalna kaznena djela, valja govoriti o normativnom okviru koji je propisan Konvencijom o kibernetičkom kriminalu i nacionalnim propisima koji se na njoj temelje, te o stvarnim mogućnostima postupanja po tim propisima.

Konvencija o kibernetičkom kriminalu u članku 14. obvezuje države stranke da usvoje zakonske i druge mjere potrebne kako bi se uspostavila ovlaštenja i postupci u svrhu provedbe specifičnih kriminalističkih istraga i postupaka. Naglasak je, dakle, na kriminalističkim istragama odnosno na policijskom postupanju. Osim ako je to izričito utvrđeno članka 21. Konvencije, svaka stranka će ovlaštenja i postupke primjenjivati na: a) kaznena djela utvrđena Konvencijom, b) druga kaznena djela počinjena pomoću računalnog sustava i c) prikupljanje dokaza o kaznenom djelu u elektroničkom obliku.

Konvencija u članku 16.-21. propisuje mjere koje država može poduzimati u tom smislu. To su: a) hitna zaštita pohranjenih računalnih podataka; b) hitna zaštita i djelomično otkrivanje podataka o prometu; c) nalog za proizvodnju; d) pretraga i oduzimanje pohranjenih računalnih podataka; e) prikupljanje računalnih podataka u realnom vremenu; f) presretanje podataka o sadržaju.[338]

3.2. Kriminalistički aspekti policijskog postupanja u slučajevima računalnog kriminala

Kao što je istaknuto još u uvodu, postavlja se pitanje stručnog profila osoba i karakteristika sredstava koja se mogu koristiti u otkrivanju i dokazivanju računalnih kaznenih djela. Postoje li u tom smislu neki zahtjevi koji se razlikuju od otkrivanja i dokazivanja drugih kaznenih djela? U otkrivanju i dokazivanju svih kaznenih djela postoji određena zajednička metodologija, ali i ono što je *differentia specifica* za pojedino djelo. Tako je i u slučaju

[337] Primjer preuzet prema Münchener Kommentar *Graf*, § 202c, r. br. 25.
[338] Pavišić, Kazneno pravo Vijeća Europe, Zagreb, 2006., str. 261-265.

otkrivanja i dokazivanja računalnog kriminala. Ono što je *differentia specifica* otkrivanja računalnog kriminaliteta jest stručni profil osobe i računalni programi kojima se taj kriminal istražuje. U vezi s razmatranim, posebno se ističe pojam kriminalističkog ispitivanja ili, kako stoji u nazivu središnje ustanove u Republici Hrvatskoj koja bi se time trebala baviti, „forenzičnog“ ispitivanja.[339]

Kada se provodi ispitivanje tragova? Je li to procedura na mjestu počinjenja kaznenog djela ili je to neka početna, neformalna, preliminarna aktivnost stručne osobe (ne vještaka jer još nema odluke ovlaštenika za vještačenje)? Na to pitanje normativni ustroj ne daje odgovor. Odgovor slijedi iz procedure kriminalističkog istraživanja: uvijek kad je potrebno stručno pribaviti ili analizirati neki trag, kriminalisti traže stručno mišljenje osobe odgovarajuće struke, koja može biti funkcionalno i organizacijski na različitim mjestima (ili takve aktivnosti u cijelosti poduzimaju osobe sa specifičnim kriminalističkim znanjem). Pitanja na koja se traži odgovor povezana su s relevantnošću pronađenih predmeta ili podataka kao tragova, ali često predstavljaju i traženje definitivnih odgovora na sva ona pitanja koja se mogu postaviti vještaku. S obzirom na to da nema formalne odluke ovlaštenika na traženje vještačenja, rezultat takve aktivnosti nije vještački nalaz. Kakav je postupak ako stručna osoba otkrije podatke koji su bitni za kazneni postupak, osobito kada se radi o primjeni destruktivnih metoda ispitivanja kojima se predmet ispitivanja uništava, zbog čega isto ispitivanje nije moguće ponoviti u kasnijoj fazi postupka? Praksa je da se u takvim slučajevima dostavlja nalog za vještačenje i da se takvo ispitivanje “prerušava” u vještačenje, a da stručna osoba tada postaje vještak. Kriminalističko ispitivanje može biti ključno za usmjeravanje kriminalističkog istraživanja i zato je logično da je Centar o kojem je riječ smješten pri Ministarstvu unutarnjih poslova.

Kriminalističko ispitivanje više je od pukog davanja mišljenja o nekom stručnom pitanju. Ono podrazumijeva i određene stručne preglede i analize korištenjem tehničkih sredstava. Davanje mišljenja stručne osobe je djelatnost koja je prigodna, najčešće temeljena na slici određenog stanja koje je očito i bez posebnog istraživanja.

3.3. Provjera uspostavljanja telekomunikacijskog kontakta (čl. 339.a ZKP-a) i provjera uspostavljanja elektroničke komunikacije (čl. 68. ZPPO-a)

Provjeru uspostavljanja telekomunikacijskog kontakta ZKP svrstava među dokazne radnje. Tu je radnju, zbog načina na koji je normativno uređena, moguće smatrati i posebnom dokaznom radnjom premda nije izrijekom propisana u katalogu tih radnji (čl. 332. ZKP-a); na takvo tumačenje neizravno upućuje i sam zakon kad pri propisivanju za koja se kaznena djela ova radnja može provesti upućuje na članak 334. ZKP-a (u kojem su popisana djela za koja se mogu odrediti posebne dokazne radnje).[340]

---

[339] Centar za forenzična ispitivanja, istraživanja i vještačenja 'Ivan Vučetić' središnja je ustanova u Republici Hrvatskoj za kriminalistička ispitivanja i vještačenja. Organizacijski je smještena u Ministarstvu unutarnjih poslova.

[340] Za normativno i faktično stanje prema ZKP-u iz 1997. v. Kralj, Provjera istovjetnosti telekomunikacijskih adresa u kriminalističkoj praksi, Policija i sigurnost, 2/2009, str. 166.-179.

Radnja se sastoji od provjere istovjetnosti, trajanja i učestalosti komunikacije s određenim elektroničkim komunikacijskim adresama, utvrđivanja položaja komunikacijskog uređaja, kao i utvrđivanja mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju, te identifikacijske oznake uređaja. Provjeru može zatražiti policija putem Operativno-tehničkog centra za nadzor telekomunikacija, na temelju naloga suca istrage, od operatora javnih komunikacijskih usluga ako postoji sumnja da je registrirani vlasnik ili korisnik telekomunikacijskog sredstva počinio kazneno djelo iz članka 334. ovog Zakona ili neko drugo kazneno djelo za koje je propisana kazna zatvora teža od pet godina (čl. 339.a st. 1. ZKP-a). Pod istim uvjetima, provjera se može zatražiti i za osobu koja je povezana s osobom za koju postoji sumnja da je počinitelj nekog od navedenih kaznenih djela (čl. 339.a st. 2.). Za provjeru uspostavljanja telekomunikacijskog kontakta policiji nije potreban nalog ako je registrirani vlasnik ili korisnik komunikacijskog sredstva dao pisani pristanak (čl. 339.a st. 8. ZKP-a). U slučaju da ne postoji pisani pristanak, ishođenje naloga od ključne je važnosti jer se u suprotnom podaci koje policija prikupi ne mogu upotrijebiti kao dokaz u kaznenom postupku (čl. 339.a st. 9. ZKP-a).

Sličnu ovlast policija ima na temelju članka 68. ZPPO-a („provjera uspostavljanja elektroničke komunikacije“). Naime, policija može od davatelja komunikacijskih usluga zatražiti provjeru istovjetnosti, trajanja i učestalosti komunikacije s određenim elektroničkim komunikacijskim adresama radi sprečavanja i otkrivanja kaznenih djela za koja se progoni po službenoj dužnosti i njihovih počinitelja, sprečavanja opasnosti i nasilja te traganja za osobama i predmetima (čl. 68. st. 1. ZPPO-a). Taj zahtjev može obuhvaćati i utvrđivanje položaja komunikacijskog uređaja, kao i utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju te identifikacijske oznake uređaja (čl. 68. st. 2. ZPPO-a).

S obzirom na to da se radi o mjerama kojima se značajno zahvaća u prava i slobode čovjeka, važno je lapidarno se osvrnuti na normativnu osnovu EU i praksu Europskog suda. Zadržavanje podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža bilo je uređeno Direktivom 2006/24/EZ. Direktiva je predviđala da pružatelji komunikacijskih usluga moraju zadržati podatke o prometu i lokaciji i s tim povezane podatke koji su nužni za identificiranje pretplatnika ili korisnika. Time bi se osigurala dostupnost tih podataka u svrhu sprečavanja, istrage, otkrivanja i progona teških kaznenih djela, osobito kaznenih djela povezanih s organiziranim kriminalom i terorizmom. Presudom u spojenim predmetima C-293/12 i C-594/12, Europski sud je Direktivu proglasio nevaljanom, smatrajući da se propisivanjem obveze zadržavanja tih podataka i dopuštanjem da im pristupe ovlaštena nacionalna tijela Direktiva osobito teško miješa u temeljna prava poštovanja privatnog života i zaštite osobnih podataka te da širina i težina miješanja te Direktive u temeljna prava nisu dovoljno ograničene. Sud je pri odlučivanju uzeo u obzir različite faktore, poput neprimjereno definiranog razdoblja zadržavanja podataka i nepropisivanja obveze da se podaci zadržavaju na području EU. Pritom treba naglasiti da Europski sud ne zabranjuje postupke koje propisuje Direktiva, već ustraje na mnogobrojnim zaštitnim elementima, kao što su težina djela, način čuvanja podataka, razmjernost, vrijeme čuvanja i dr.

S gledišta spomenute presude, našem normativnom uređenju ne nalazi se prigovor. Kolokvijalni prigovor da se mjera provjere uspostavljanja elektroničke komunikacije ne bi trebala nalaziti u ZPPO-u jer slična mjera postoji u ZKP-u, ne stoji, jer se radi o mjerama različite naravi i svrhe. Dok je u jednom slučaju svrha heuristička (otkrivačka), u drugom je to silogistička (dokazna).[341]

3.4. Presretanje, prikupljanje i snimanje računalnih podataka (čl. 332. ZKP-a)

Presretanje, prikupljanje i snimanje računalnih podataka predstavlja posebnu dokaznu radnju iz članka 332. stavka 1. točke 2. ZKP-a. Pojam računalnog podatka definiran je u članku 87. stavku 19. KZ-a (opširnije v. gore, 2. 2.). ZKP ne definira pobliže sadržaj ove radnje. Ona se provodi ako se izvidi kaznenih djela ne bi mogli provesti na drugi način ili bi to bilo moguće samo uz nerazmjerne teškoće; drugim riječima, „u situaciji dokazne nužde“[342]. Određuje ju sudac istrage na zahtjev državnog odvjetnika protiv osobe za koju postoje osnove sumnje da je počinila ili sudjelovala u kaznenom djelu iz kataloga navedenog u članku 334. ZKP-a (čl. 332. st. 1.). Nalog iznimno može izdati državni odvjetnik, pod uvjetima i u postupku propisanom u članku 332. stavku 2.-5. ZKP-a. Radnja se može provesti i prema osobi čijim se priključcima na telefon ili drugim telekomunikacijskim uređajem počinitelj služi (čl. 332. st. 7. ZKP-a). Prikupljeni podaci mogu se upotrijebiti kao dokaz u postupku (čl. 333. st. 1. ZKP-a).

Radnju presretanja, prikupljanja i snimanja računalnih podataka uvijek provodi policija (čl. 337. st. 1. ZKP-a). Operativno-tehnički centar za nadzor telekomunikacija koji obavlja tehničku koordinaciju s davateljem telekomunikacijskih usluga u Republici Hrvatskoj, kao i davatelji telekomunikacijskih usluga, dužni su policiji osigurati potrebnu tehničku pomoć (čl. 335. st. 2. ZKP-a). Važno je da policija slijedi postupovna pravila propisana u članku 332. jer se u suprotnom prikupljeni podaci ne mogu upotrijebiti kao dokaz u postupku (čl. 335. st. 8. ZKP-a).

3.5. Pretraga računala (čl. 257. ZKP-a)

U otkrivanju i dokazivanju računalnog kriminala važnu ulogu ima dokazna radnja pretrage računala, uređena u članku 257. ZKP-a. Svrha takve pretrage nije pretražiti računalo kao tjelesnu stvar,[343] nego doći do računalnih podataka pohranjenih u njemu. ZKP u članku 257. stavku 1. s računalom kao objektom pretrage izjednačava i uređaj povezan s računalom, drugi uređaj koji služi prikupljanju, pohranjivanju i prijenosu podataka, uređaj koji služi telefonskim, računalnim i drugim komunikacijama (npr. mobilni telefon) te nositelj podataka (tj. medij za pohranu podataka, npr. USB štapić ili CD).[344]

---

[341] Opširnije Gluščić/Veić, Zakon o policijskim poslovima i ovlastima, Zagreb, 2015., str. 118.-119.
[342] Pavišić i sur., Kazneno postupovno pravo, Rijeka, 2014., str. 265.
[343] Tako i Krapac, Kazneno procesno pravo, Prva knjiga: institucije, VII. izdanje, Zagreb, 2015., str. 330.
[344] Pavišić/Modly/Veić, Kriminalistika, Knjiga 1, str. 351.-353.

Osobe koje koriste ili imaju pristup računalu ili nekom drugom navedenom uređaju ili nositelju podataka, te davatelji telekomunikacijskih usluga, dužni su na zahtjev tijela koje poduzima pretragu omogućiti pristup računalu ili drugom uređaju ili nositelju podataka te dati potrebne obavijesti (npr. zaporke za pristup datotekama) za nesmetanu uporabu i ostvarenje ciljeva pretrage (čl. 257. st. 1. ZKP-a). U pojam tijela koje poduzima pretragu ulazi i policija (čl. 242. st. 4.), pa je i ona ovlaštena postaviti navedeni zahtjev pod uvjetom da postoji prethodni nalog o pretrazi ili uvjeti za provođenje pretrage bez naloga.

Po nalogu tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu i drugim uređajima iz stavka 1. ovog članka, te davatelj telekomunikacijskih usluga, dužni su odmah poduzeti mjere kojima se sprečava uništenje ili mijenjanje podataka. Tijelo koje poduzima pretragu, može provedbu tih mjera naložiti stručnom pomoćniku (čl. 257. st. 2. ZKP-a).

Ogluše li se navedene osobe ili davatelji telekomunikacijskih usluga bez opravdanog razloga na zahtjev nadležnog tijela, sudac istrage može na prijedlog državnog odvjetnika primijeniti kaznu iz članka 259. stavka 1. ZKP-a zbog povrede procesne discipline (novčana kazna do pedeset tisuća kuna, a u slučaju daljnjeg odbijanja i kazna zatvora do mjesec dana). Od mogućnosti disciplinskog kažnjavanja izuzet je okrivljenik (čl. 257. st. 3. ZKP-a) zbog tzv. privilegija od samooptuživanja.

3.6. Privremeno oduzimanje računalnih podataka (čl. 59. ZPPO-a i čl. 263. ZKP-a)

Prema članku 263. stavku 1. ZKP-a, privremeno se oduzimaju dvije kategorije predmeta: (1) oni koji se imaju oduzeti prema kaznenom zakonu i (2) oni koji mogu poslužiti pri utvrđivanju činjenica u postupku. Premda računalni podaci po svojoj prirodi nisu predmeti, zakonodavac ih u članku 263. stavku 1. ZKP-a izjednačava s predmetima, čime omogućava da se i na njih primjenjuju odredbe o privremenom oduzimanju predmeta. Primijenimo li članak 263. stavak 1. na kontekst računalnih podataka, dolazimo do zaključka da je privremeno oduzimanje računalnih podataka moguće ponajprije kada je oduzimanje propisano kod računalnih kaznenih djela iz članka 269.-272. KZ-a, ali i kod drugih kaznenih djela kod kojih se računalni podaci oduzimaju u okviru mjere oduzimanja predmeta (čl. 79. KZ-a). Nadalje, privremeno oduzimanje računalnih podataka moguće je i kada se oni mogu poslužiti pri utvrđivanju činjenica u postupku, što uključuje i slučajeve računalnog kriminala u širem smislu (npr. oduzimanje dječje pornografije, računovodstvenih podataka, tekstualnih dokumenata). Pojedini računalni podaci izuzeti su od privremenog oduzimanja (čl. 262. ZKP-a).

Na pisani zahtjev državnog odvjetnika, računalni podaci moraju mu se predati u cjelovitom, izvornom, čitljivom i razumljivom obliku (čl. 263. st. 2. ZKP-a). Te podatke snimit će u realnom vremenu tijelo koje provodi radnju. Pri pribavljanju, snimanju, zaštiti i čuvanju podataka posebno će se voditi brigu o propisima koji se odnose na čuvanje tajnosti određenih podataka (čl. 186.-188. ZKP-a). Prema okolnostima, podaci koji se ne odnose na kazneno djelo zbog kojega se postupa, a potrebni su osobi prema kojoj se provodi mjera,

mogu se snimiti na odgovarajuće sredstvo i vratiti toj osobi i prije okončanja postupka (čl. 263. st. 3. ZKP-a).

U slučaju odbijanja predaje u roku koji odredi državni odvjetnik, osobu koja odbija predati računalne podatke može se disciplinski kazniti prema članku 259. stavku 1. ZKP-a (novčana kazna do pedeset tisuća kuna, a u slučaju daljnjeg odbijanja i kazna zatvora do mjesec dana). Od mogućnosti disciplinskog kažnjavanja izuzet je okrivljenik i osobe koje su oslobođene dužnosti svjedočenja (čl. 263. st. 4. ZKP-a).

Iako ZKP u članku 263. stavku 2. ne spominje policiju kao tijelo koje je ovlašteno postaviti zahtjev za predaju računalnih podataka, već jedino državnog odvjetnika, takva ovlast policije postoji pri poduzimanju hitnih dokaznih radnji sukladno sa člankom 212. ZKP-a. Ona postoji i u slučaju kada policija na temelju zakonske ovlasti provodi pretragu pa pronađe računalne podatke koji su u vezi sa svrhom pretrage ili podatke koji upućuju na drugo kazneno djelo za koje se progoni po službenoj dužnosti (čl. 248.-249. ZKP-a). Što je u praktičnom smislu još važnije, policijski službenik računalne podatke može privremeno oduzeti i u okviru mjere privremenog oduzimanja, čuvanja, uništenja i prodaje predmeta propisane u članku 59. ZPPO-a. Policijski službenik to će učiniti kada je (1) vjerojatno da je računalni podatak namijenjen počinjenju kaznenog djela za koje se progoni po službenoj dužnosti ili prekršaja ili pak kada je (2) oduzimanje računalnog podatka potrebno radi zaštite opće sigurnosti (npr. kada je riječ o vrlo opasnom računalnom virusu).

4. ZAKLJUČAK

Računalni kriminal prisutan je posljednjih tridesetak godina i u procesu je stalne evolucije. S razvojem računalne tehnologije, bilo je potrebno stvoriti normativni okvir koji će odrediti zabranjenu zonu u tom području i sredstva kojima će se djelovati u otkrivanju i dokazivanju takvih djela. Konvencija o kibernetičkom kriminalu daje solidne smjernice za definiranje zabranjene zone tj. za izgradnju materijalnog kaznenog zakonodavstva, koje je RH prihvatila i implementirala uvođenjem glave XXV. KZ-a (kaznena djela protiv računalnih sustava, programa i podataka). Ta Konvencija sadrži i postupovne odredbe, koje su također na odgovarajući način prenesene u hrvatsko zakonodavstvo. Međutim, preuzimanje odredaba Konvencije i drugih međunarodnih standarda u KZ, ZKP i ZPPO ne jamči samo po sebi učinkovit progon računalnih kaznenih djela. S obzirom na niske brojke osuđenih počinitelja, upitno je prepoznaju li tijela kaznenog progona u praksi računalna kaznena djela te koriste li se predviđenim mehanizmima za njihovo otkrivanje i dokazivanje.

S time u vezi, u ovom su radu identificirana dva temeljna izazova. Prvi se odnosi na prepoznavanje računalnog kriminala i njegovo razlikovanje od dopuštenih računalnih praksi. Za rješavanje tog problema potrebno je odgovarajuće poznavanje kaznenog materijalnog prava sadržanog u glavi XXV. KZ-a. Drugi je izazov vezan za posjedovanje odgovarajućih kriminalističkih znanja te poznavanja postupovnih propisa (ZPPO-a i ZKP-a) s ciljem zakonite i učinkovite primjene policijskih ovlasti u praksi. Rješavanje tih problema podrazumijeva odgovarajuću kvalificiranost policijskih službenika – kriminalističkih istražitelja. Radi uspješnog kriminalističkog istraživanja trebala bi se formirati posebna tijela s

ovlastima za kriminalističko ispitivanje ili, kako je danas modernije reći, „forenzično“ ispitivanje računalnog kriminala. Radnje poput privremenog oduzimanja računala kao predmeta i pretrage računala treba povjeriti posebno akreditiranim službenicima koji će ponuditi polaznu osnovu za daljnja istraživanja, koja mogu poduzimati i „obični“ policijski službenici. To treba postati standard koji će biti razrađen odgovarajućim podzakonskim aktom. U prilog potrebi za razvitkom specifičnih znanja policijskih službenika u domeni računalnog kriminala govore i propisi na razini EU te praksa Europskog suda, u kojoj se inzistira na razmjernosti zahvata represivnih tijela u slobode i prava građana računalnom tehnologijom.

LITERATURA

Bača, M., Ćosić, J. (2013). Prevencija računalnog kriminaliteta. *Policija i sigurnost,* 22(1), str. 146.-158.

Gluščić, S., Veić, P. (2015). Zakon o policijskim poslovima i ovlastima. Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske, Policijska akademija.

Grozdanić, V., Škorić, M., Martinović, I. (2013). *Opći dio kaznenog prava*. Rijeka: Pravni fakultet Sveučilišta u Rijeci.

Kindhäuser, U., Neumann, U. Paeffgen, H.U. (2013). *Nomos Kommentar zum Strafgesetzbuch*. Gesamtredaktion: 2. Auflage, Baden-Baden 2005; 3. Auflage, BadenBaden 2010; 4. Auflage, Baden-Baden 2013 (4. Auflage zusammen mit Karsten Gaede) (Kommentierung der § 13, Vor § 102, §§ 102-109k, Vor § 284, §§ 284-290; §§ 292-297, § 323c).

Kokot, I. (2014). Kaznenopravna zaštita računalnih sustava, programa i podataka. *Zagrebačka pravna revija*, 3, 303-330.

Kralj, T. (2009). Provjera istovjetnosti telekomunikacijskih adresa u kriminalističkoj praksi. *Policija i sigurnost*, 2, 166-179.

Krapac, D. (2015). *Kazneno procesno pravo. Prva knjiga: institucije*. Zagreb: Narodne Novine.

Von Joecks, W., Miebach, K. (2012). *Münchener Kommentar zum Strafgesetzbuch*. München: C.H.BECK.

Novoselec, P., Bojanić, I. (2013). *Opći dio kaznenog prava*. Zagreb: Pravni fakultet.

Pavišić, B. (2006). *Kazneno pravo Vijeća Europe*. Zagreb: Golden marketing-Tehnička knjiga.

Pavišić, B. (2011). *Kazneno postupovno pravo.* Rijeka: Dušević & Kršovnik.

Pavišić, B., Modly, D., Veić, P. (2006). *Kriminalistika - Knjiga 1.* Zagreb: Golden marketing-Tehnička knjiga.

Pavišić, B., Modly, D., Veić, P. (2012). *Kriminalistika - Knjiga 2.* Rijeka: Dušević & Kršovnik.

Schönke/Schröder (2014). *Strafgesetzbuch, Kommentar*, XXIX. izdanje.

Turković, P. i dr. (2013). *Komentar Kaznenog zakona*, Zagreb: Narodne novine.

Vuletić, I., Nedić, T. (2014). Računalna prijevara u hrvatskom kaznenom pravu. *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 2, 679-692.

Petar Veić

Igor Martinović

CHALLENGES FOR POLICE PROCEDURES IN DETECTION AND INVESTIGATION OF CYBERCRIME

Summary

In 2011, the Croatian parliament enacted a new Criminal Code which contains some new computer-related offences. These offences are regulated under the title XXV (Offences against computer systems, programs and data). However, there are some computer-related offences which are not included in the title XXV, namely exploitation of children for pornography, prostitution, public incitement to violence and hatred, etc. Dynamic legislative changes and continuous improvement of information technology, allowing for more complex forms of computer crime, confront the police with two main challenges. The first challenge consists in early recognition of criminal conduct and its difference from undesirable but non-prohibited behaviors. The further challenge consists in the use of police powers in a manner that is compliant with the Police Powers and Duties Act and the Criminal Procedure Act, with the aim to collect information to be used in future criminal proceedings against the perpetrators of computer crimes.

Key words: *cybercrime, police powers, Criminal Code, Police Powers and Duties Act, Criminal Procedure Act*

REVIEW PAPER

Snežana Nikodinovska-Stefanovska[345]

THE EU DATA PROTECTION REFORM - DATA PROTECTION CHALLENGES IN THE FIELD OF POLICE AND LAW ENFORCEMENT

Summary

In the last few decades, the European Union has adopted several pieces of legislation to protect personal data, the main one being the 1995 Data Protection Directive. Since then, rapid technological and business developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased dramatically. In January 2012, the European Commission proposed a reform of the EU data protection rules to make them fit for the 21st century. The reform consists of a draft Regulation setting out a general EU framework for data protection and a draft Directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities. The proposed Directive is intended to replace the 2008 Data Protection Framework Decision and aims to ensure a consistent and high level of data protection in this field, enhancing mutual trust between police and judicial authorities of different Member States and facilitating the free flow of data and co-operation between police and judicial authorities by covering both domestic and cross-border processing. This paper briefly discusses the EU regulatory framework on data protection before and under the Lisbon Treaty. Also, the draft General Data Protection Regulation and Police and Criminal Justice Data Protection Directive are commented and analyzed, followed by some concluding remarks.

Key words*: general data protection regulation, Lisbon Treaty, personal data, Police and Criminal Justice Data Protection Directive, protection of personal data*

1. INTRODUCTION

The processing of personal data has become an inherent part of the daily life of Europeans, for example when booking a flight ticket, transferring money, applying for a job, or just using the Internet for private purposes. Nobody wants to miss the advantages of modern technologies. Sometimes individuals provide their personal data simply because they choose to do so. However, sometimes data is collected without consent and often without the knowledge of the individuals concerned. The protection of personal data is becoming more and more relevant as technology develops and the possibilities increase to use and misuse information more efficiently. Processing personal data also plays an increasing role in police and judicial cooperation: the lawful storage, exchange, and evaluation of information about a person can be an important instrument in ensuring public security.

[345] Prof. Snežana Nikodinovska-Stefanovska, Ph.D., Faculty of Security – Skopje, e-mail: snikodinovska@gmail.com

The protection of personal data is one of the basic values in Europe, for the Member States of the EU and for the EU institutions. The protection of persons in relation to the processing of their personal data is a fundamental right laid down in the Charter of Fundamental Rights of the EU[346] (Article 8) and in the Treaty on the Functioning of the European Union[347] (Article 16). Additionally it is a specified in the general Data Protection Directive 95/46/EC[348] as well as complemented by e-Privacy Directive 2002/58/EC[349].The processing by EU institutions and bodies is covered by Data Protection Regulation (EC) No 45/2001.[350] Since 2008, the EU general framework for the protection of personal data in police and judicial cooperation in criminal matters (ex-third pillar), is Framework Decision 2008/977/JHA.[351]

Rapid technological developments and globalization have brought new challenges for the protection of personal data. The scale of data collection and sharing has increased spectacularly. Technology allows competent authorities to make use of personal data on an unprecedented scale in order to pursue their activities.

The entry into force of the Lisbon Treaty[352] provides a much-needed opportunity to reflect on the main challenges for the protection of personal data and on how the European Commission intends to address these challenges in the future. In its Communication on "A comprehensive approach on personal data protection in the European Union"[353], the Commission concluded that the EU needs a more comprehensive and coherent policy on the fundamental right to personal data protection. In addition, the 27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement.

---

[346] Charter of Fundamental Rights of the European Union, OJ 2000/ C 364/01.

[347] The most striking change for data protection under the Lisbon Treaty is a new, prominent provision on the subject - Article 16 TFEU (Treaty on European Union and of the Treaty on the Functioning of the European Union) - which replaces and expands on the old Article 286 of the Treaty of the establishing European Community. Article 16 states as follows:

1.Everyone has the right to the protection of personal data concerning them.

2.The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union. Consolidated versions of the Treaty on European Union and of the Treaty on the Functioning of the European Union, together with the annexes and protocols thereto, as they result from the amendments introduced by the Treaty of Lisbon, see OJ 2010 C 83/1.

[348] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ 1995 L 281/31.

[349] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/07/2002 pp. 37–47.

[350] REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1, 12.

[351] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60.

[352] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, C 306, 17 December 2007.

[353] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, A comprehensive approach on personal data protection in the European Union COM (2010) 609 final, 4.11.2010.

Uniform and up-to-date legislation on data protection is essential to guarantee the fundamental right of individuals to have their personal data protected, to allow for the development of the digital economy and to strengthen the fight against crime and terrorism. In January 2012, European Commission proposed a comprehensive reform of the EU data protection rules. The data protection reform is a legislative package to update and modernize the rules of the 1995 data protection directive and the 2008 framework decision on data protection in judicial cooperation in criminal matters and police cooperation. It concerns two legislative instruments: the general data protection regulation (intended to replace 1995 Directive on Data Protection) and the data protection directive in the area of law enforcement (intended to replace the 2008 Data Protection Framework Decision). The Commission introduced again two sector-specific instruments rather than one of general application, broadly following the older Pillar distinction.[354]

2. THE EU DATA PROTECTION LEGAL FRAMEWORK

The right to data protection in the EU is based upon a set of legal acts belonging to both international and EU law. The Directive on Data Protection (1995 Directive) is the key piece of EU legislation on personal data protection. It was adopted in 1995 with two objectives in mind: to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States. The Directive applies to both the public and private sectors. It develops and specifies data protection principles in order to achieve harmonization throughout the EU. The Directive stipulates general rules on the lawfulness of personal data processing and the rights of the people whose data are processed ("data subjects"). The directive applies to the collection, storage, disclosure and dissemination of personal data, both by automatic (electronic databases) and non-automatic means (traditional filing systems), in relation to which it grants the 'data subject' a set of rights, including the right to be informed if data relating to him/her are being processed; the right to obtain the rectification, erasure or blocking of data that have not been lawfully processed; and the right to judicial recourse in the event of any breach of rights conferred during the processing of personal data. The Directive also sets out that at least one independent supervisory authority in each Member State shall be responsible for monitoring its implementation. In particular, the Directive regulates transfers of personal data to third countries: in general, personal data cannot be exchanged with a third country unless the latter provides guarantees for an adequate level of protection.

In order to address the threats posed by developments in technology to an individual's right to data protection, the directive has been supplemented by two further instruments (dealing with privacy in the telecommunications[355] and electronic communications[356] sectors). The main purpose of these is to guarantee the confidentiality of communications by prohibiting any unauthorized listening, taping, storage or other kinds of interception or surveillance.

---

[354] Pre-Lisbon, the EU comprised three legal pillars with separate legal bases for legislative action: (i) "Community" matters; (ii) Common Foreign and Security Policy; and (iii) Police and Judicial Cooperation in Criminal Matters.

[355] Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ 1998 L 24/1).

[356] e-PrivacyDirective.

As regard of data protection in the field of police and justice is a specific subject, which requires specific attention, taking into account the complex relation between the activities of the State to ensure security and the protection of the personal data of the individual. Personal data processing for security purposes gained in importance after 9/11. The terrorist attacks in several EU capitals strengthen the request by security agencies, both in and out of the EU, to be provided with more extensive and efficient means to process the personal information of individuals in order to facilitate their work.

In the area of police and judicial cooperation in criminal matters, the current data protection framework in the EU could be only described as a patchwork, as several instruments exist with specific data protection regimes or with data protection clauses. The legal provisions on Europol, Eurojust, the Schengen Information System, and those contained in the "Prüm" Council decision are just examples of such sector-specific regimes, the creation of different rights and obligations for Member States and individuals, and the setting up of several data protection supervisory authorities. The specificity of this area is not only the result of the former pillar structure of the previous EU-Treaties, but is more widely recognized (see for instance the exceptions of Article 13 of 1995 Directive and Declaration 21[357] attached to the Lisbon Treaty).

With the entry into force of the Lisbon Treaty, new perspectives were created for law making in the field of data protection. The pillar structure was abolished and with Article 16 TFEU-Treaty on the Functioning of the European Union, a single legal basis is created for data protection in almost all areas of EU law.[358] Article 16 paragraph 2 TFEU applies to all forms of data processing in the private and in the public sector and particularly includes the area of police and judicial cooperation in criminal matters, which was previously not the case. This does not necessarily mean that the implementation of data protection principles for police and justice should be the same as the rules in other parts of society. However, Declaration 21 attached to the Lisbon Treaty states that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation "may prove necessary because of the specific nature of these fields".

After several years of discussions and debates with the EU bodies, the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters was adopted by the Council and published in the Official Journal on 30 December 2008. The decision is the first horizontal data protection instrument in the field of personal data used by police and judicial authorities and its main purpose is to establish a common level of privacy protection and a high level of security when exchanging personal data. It can be seen as a first step towards a general framework in the former third pillar but is far from complete.

---

[357] Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation (annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, 13.12.2007).
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=EN (20.12.2015)

[358] See more: Nikodinovska-Stefanovska, S. (2012). Lisbon Treaty and the protection of personal data in the European Union. In Dimitrijevic, D. Miljus, B. (eds.) *Harmonizacija zakonodavstva Republike Srbije sa pravom Evropske Unije* , Beograd, Institut za medunarodnu politiku i privredu, Institut za uporedno parvo, Hans Zajdel Fondacija. 717-728.

The Framework Decision was necessary, as at that time there was no general instrument at European level covering data processing in the areas of police and judicial cooperation in criminal matters. Article 3 of 1995 Directive on the protection of personal data and on the free movement of such data states that it does not apply "to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Title VI of the Treaty on European Union, nor, in any case, to processing operations concerning public security, defense, state security or the activities of the State in areas of criminal law".

The purpose of the Framework Decision is to provide at EU level a high level of protection of the fundamental rights and freedoms of natural persons when processing personal data in the framework of police and judicial cooperation in criminal matters. At the same time, a high level of public safety should be guaranteed (Article 1). It does not preclude Member States from providing higher safeguards to protect personal data collected or processed at national level Article 1(5). The scope of the Framework Decision (Article 1(2)) is limited to the processing of personal data for the purpose of preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties of data which are or have been transmitted or made available:

- between Member States,
- by Member States to authorities or information systems established on the basis of Title VI of the Treaty on European Union ('Police and judicial cooperation in criminal matters'); or
- to the competent authorities of the Member States by authorities or information systems established based on the Treaty on European Union or the Treaty establishing the European Community.

Personal data, which have been transferred from one Member State to another one, may also be transferred to third States or international bodies, if certain requirements are met (Article 13).

In direct comparison with Directive 95/46/EC, this particular Framework Decision provides *inter alia* only for minimum standards and has a scope limited to the processing of personal data transmitted or made available between Member States. In view of such shortcomings, the European Parliament explicitly called for a timely revision of Council Framework Decision 2008/977/JHA in its Resolution on the Stockholm program.[359]

3. THE DATA PROTECTION REFORM PACKAGE

In January 2012, the European Commission proposed a full reform of the current EU data protection rules. On 15 December 2015, after a lengthy legislative process and many months of negotiations, the European Commission, the European Parliament and the European

[359] B7-0000/2009 European Parliament resolution on Communication from the Commission to the European Parliament and the Council - An area of freedom, security and justice serving the citizen - Stockholm programme , http://www.europarl.europa.eu/meetdocs/2009_2014/documents/juri/dv/stockholmprogramme_resolution_/stockholmprogramme_resolution_en.pdf (20.12.2015)

Council finally found an agreement on the data protection reform package, during the so-called "trilogue" meetings.

The Commission, while preparing the amended EU data protection framework, had two realistic options at hand: (1) to release a single, comprehensive, standard setting text that would set the general rules for all personal data processing within the EU, or (2) to continue distinguishing between commercial and security-related processing through the continued existence of the 1995 Directive and the 2008 Framework Decision, appropriately amended, respectively. Apparently, the Commission chose to replace both documents simultaneously, broadly following the model already in effect.

The proposed new legal framework consists of ***two legislative proposals***:

- a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), and
- a proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.[360]

This proposal is based on Article 16 TFEU, which is the new legal basis for the adoption of data protection rules introduced by the Lisbon Treaty. This provision allows the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Member States when carrying out activities, which fall within the scope of Union law. It also allows the adoption of rules relating to the free movement of personal data, including personal data processed by Member States or private parties.

The key ***purposes of the data protection reform*** are: (I) the creation of a single set of rules, (II) the affirmation and strengthening of the data subjects' rights, (III) increased responsibility and accountability of data controllers and data processors, (IV) the removal of unnecessary administrative burdens and (V) a strengthened enforcement framework.

3.1. Main provisions of the new Data Regulation

During the JHA Council of 15-16 June 2015, a general approach was reached on the data protection regulation that is part of the reform of the EU's data protection legal framework. The Council reached a general approach on the general data protection regulation that establishes rules adapted to the digital era.

The EU General Data Protection Regulation (GDPR) aims at enhancing the level of data protection for individuals whose personal data is processed and increasing business

[360]Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Communication COM (2012) 10 final. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf p.2. (20.12.2015)

opportunities in the digital single market including through reduced administrative burden. ***Topics*** covered in the draft regulations include:

- Rights of Data Subjects - Transparency, Access to Data, Rectification, Erasure, Right to Object to Profiling,
- Obligations of Companies - Data Security, Data Protection Assessment,
- Increased Powers for Data Protection Agencies and New Efforts for Coordination and Collaboration,
- New Remedies and Sanctions.

Strengthened ***data protection rights*** give data subjects more control over their personal data:

- easier access to their data,
- more detailed information about what happens to their personal data once they decide to share it: data controllers must be more transparent about how personal data is handled, for example by informing individuals about their privacy policy in clear and plain language,
- a right to erasure of personal data and "right to be forgotten", enabling anyone for example to demand deletion of data no longer needed for the purpose for which it was collected,
- a right of “data portability” enabling easier transmission of personal data from one service provider, for instance a social network, to another. This will also increase competition among service providers,
- limits to the use of 'profiling', i.e. automated processing of personal data to assess personal aspects, such as performance at work, economic situation, health, personal preferences etc. Although a generally accepted definition is yet to be seen, profiling is broadly understood as the creation of individual profiles through processing - intensive methods and the undertaking of actions based on such findings.

To ensure improved legal redress, data subjects will be able to have any decision of their data protection authority reviewed by their national court, irrespective of the member state in which the data controller is established. A Regulation is considered the most appropriate legal instrument to define the framework for the protection of personal data in the Union. The direct applicability of a Regulation in accordance with Article 288 TFEU will reduce legal fragmentation and provide greater legal certainty by introducing a harmonized set of core rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market.

The final draft of the new European General Data Protection Regulation was agreed on 15 December 2015 and, once the European Parliament has approved it in early 2016, is expected to take effect by early 2018. This reform aims to update data protection law to address the challenges of the digital age while simultaneously protecting the rights of individuals and enabling businesses to utilize personal data in a more consistent manner across the European Union.

3.2. Main provisions of the new Police and Criminal Justice Directive

The Commission stressed in its Action Plan implementing the Stockholm Program[361] the need to ensure that the fundamental right to personal data protection is consistently applied in the context of all EU policies. The Action Plan underlined that "in a global society characterized by rapid technological change where information exchange knows no borders, it is particularly important that privacy must be preserved. The Union must ensure that the fundamental right to data protection is consistently applied. We need to strengthen the EU's stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention as well as in our international relations."[362]

Framework Decision 2008/977/JHA has a limited scope of application, since it only applies to cross-border data processing and not to processing activities by the police and judiciary authorities at purely national level. This is liable to create difficulties for police and other competent authorities in the areas of judicial co-operation in criminal matters and police cooperation. They are not always able to distinguish easily between purely domestic and cross-border processing or to foresee whether certain personal data may become the object of a cross-border exchange at a later stage. Moreover, because of its nature and content, the Framework Decision leaves a large room for maneuver to Member States' national laws in implementing its provisions.

As it was mentioned, the Lisbon Treaty introduces a specific legal basis for the adoption of rules on the protection of personal data that also applies to judicial co-operation in criminal matters and police co-operation. Article 8 of the Charter of Fundamental Rights of the EU enshrines protection of personal data as a fundamental right. Article 16 TFEU requires the legislator to lay down rules relating to the protection of individuals with regard to the processing of personal data also in the areas of judicial co-operation in criminal matters and police cooperation, covering both cross-border and domestic processing of personal data. This will allow protecting the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data, ensuring at the same time the exchange of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This will contribute to facilitating the cooperation in the fight against crime in Europe.

Due to the specific nature of the field of police and judicial co-operation in criminal matters it was acknowledged in Declaration 21 that specific rules on the protection of personal data and the free movement of such data in the fields of judicial co-operation in criminal matters and police co-operation based on Article 16 TFEU may prove necessary.

Data protection directive in the field of law enforcement directive is aimed at protecting personal data processed for prevention, investigation, detection or prosecution of criminal

---

[361] Stockholm Action Plan, COM(2010)171final, 20.4.2010. .http://eur-lex.europa.eu/legal- ontent/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=EN. (25.12.2015)

[362]Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25.1.2012 http://ec.europa.eu/home-affairs/doc_centre/police/docs/com_2012_10_en.pdf (25.12.2015)

offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. It is crucial to ensure a consistent and high level of protection of personal data of individuals, while at the same time facilitating the exchange of personal data between law enforcement authorities in the different member states. The proposal aims to ensure a consistent and high level of data protection in this field, thereby enhancing mutual trust between police and judicial authorities of different Member States and facilitating the free flow of data and cooperation between police and judicial authorities.

The proposal is based on Article 16(2) TFEU, which is a new, specific legal basis introduced by the Lisbon Treaty for the adoption of rules relating to the protection of individuals with regard to the processing of personal data. These data are provided by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities, which fall within the scope of Union law, and the rules relating to the free movement of such data.

The Police and Criminal Justice Data Protection Directive is divided into 11 chapters, each regulating a specific data protection aspect. Chapter I contains its scope of application, that now extends to domestic processing too, as well as the definitions of terms used in the Directive – important additions refer to the terms of 'personal data breach', 'genetic' and 'biometric' data.

Chapter II of the Directive lays down the principles of the processing, expressly following those of the 1995 Directive and the Regulation intended to replace it. Explicit reference is made to the transparency and to the data minimization principles. It is mostly in this Chapter that flexibility options for the processing of personal data are afforded in the AFSJ context, enabling data controllers to process personal information (including sensitive data) of varied quality, for purposes other than those they were collected, using profiling techniques, if needed.

The rights of individuals/data subject are set in Chapter III of the Directive: the rights to information adding new elements for the information of the data subjects (on the storage period, their rights to rectification, erasure, or restriction and to lodge a complaint), access to data and objection to the processing are to be found among these provisions, properly adapted in the AFSJ context.

Chapters IV, VI and VII refer to the enforcement mechanism: this is to be composed of supervisory authorities at Member State level and a European Data Protection Advisory Board. Provisions on 'remedies, liability and sanctions' set in Chapter VIII complement these. Finally, international data transfers are regulated in Chapter V.

As expressly set in many instances in its 'detailed explanation', the Directive follows, whenever possible, the provisions of the General Data Protection Regulation and the 1995 Directive and at times, older suggestions by the Commission that were abandoned while introducing the 2008 Framework Decision.

The Directive appears to be making a positive contribution to the individual right to data protection; finally affording data subjects the means to protect their rights effectively.

The new Directive should be adopted in spring 2016, after which member states will have two years to transpose the provisions of the new directive into their national laws.

4. CONCLUSION

The Commission as a unique legal basis for the adoption of common rules for the processing and protection of personal data in both private and public sectors, including police and justice matters, envisaged the Treaty of Lisbon. In January 2012, the Commission proposed a comprehensive reform of the EU's data protection rules. Although the Commission has issued two different initiatives on this matter - the General Data Protection Regulation and the Data Protection Directive, the later focused on criminal matters, there is a consistent and common approach on this matter.

In January 2012, the Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online data protection rights and boost Europe's digital economy. The Commission's proposal - the General Data Protection Regulation -will replace and modernize the principles enshrined in the 1995 Data Protection Directive implemented in Member States since 1998. The new proposal will substantially enhance data protection compliance throughout Europe and firms will face tough new fines for data breaches. The Regulation will address one of the fundamental criticisms of the current data protection framework in that rules within Member States have been interpreted and implemented in a divergent manner, by the very nature of the law emanating from a Directive. The rules in the form of a Regulation, will be directly applicable in Member States thereby harmonizing the data protection rules, one of the key objectives of the European Commission. As regard of the draft Directive on the protection of individuals with regard to the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences it will be the first instrument to comprehensively harmonize 28 different law enforcement systems with respect to data processing for law enforcement purposes as well as set minimum standards for data processing for policing purposes within each member state. Namely, EU countries may set higher standards than those enshrined in the directive if they so wish.

The Data Protection Directive takes account of the specific needs of law enforcement, respects the different legal traditions in Member States and is fully in line with the Charter of Fundamental Rights. With the new Data Protection Directive, law enforcement authorities in EU Member States will be able to exchange information necessary for investigations more efficiently and effectively, improving cooperation in the fight against terrorism and other serious crime in Europe. The rules clarify police cooperation arrangements at all administrative levels and give citizens greater certainty as to the law. In addition, with the new Data Protection Directive better protection of citizens' data is provided. Individuals' personal data will be better protected, when processed for any law enforcement purpose including prevention of crime. It will protect everyone – regardless of whether they are a victim, criminal or witness. All law enforcement processing in the Union must comply with the principles of necessity, proportionality and legality, with appropriate safeguards for the individuals. Independent national data protection authorities ensure supervision, and effective judicial remedies are provided. The Data Protection Directive provides clear rules for the transfer of personal data by law enforcement authorities outside the EU, to ensure that the level of protection of individuals guaranteed in the EU is not undermined.

The new Data Protection Directive should replace the current 2008 Framework Decision laying down a harmonized legal framework in the 28 EU Members States. It takes account of the specificities of the law enforcement sector while ensuring the respect of the fundamental right to data protection. It is crucial to ensure a consistent and high level of protection of personal data of individuals while at the same time facilitating the exchange of personal data between law enforcement authorities in the different member states.

REFERENCES

B7-0000/2009 *European Parliament resolution on Communication from the Commission to the European Parliament and the Council - An area of freedom, security and justice serving the citizen - Stockholm programme*, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/juri/dv/stockholmprogramme_resolution_/stockholmprogramme_resolution_en.pdf (accessed 20/12/2015)

Charter of Fundamental Rights of the European Union, OJ 2000/ C 364/01. http://www.europarl.europa.eu/charter/pdf/text_en.pdf (accessed 20/12/2015)

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the regions (2010). *A comprehensive approach on personal data protection in the European Union.* COM 609 final, 4.11.2010.

Stockholm Action Plan, COM (2010). 171 final, 20/04/2010. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=EN (accessed 25/12/2015)

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (2008). OJ L 350, 30.12.2008, p. 60. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977 (accessed 20/12/2015)

Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation (annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, 13/12/2007), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=EN (accessed 20/12/2015)

Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector. (OJ 1998 L 24/1). http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32002L0058 (accessed 20/12/2015)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995). (OJ 1995 L 281/31). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 (accessed 26/12/2015)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). (2002). (OJ L 201, 31/07/2002) pp. 37–47. http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32002L0058 (accessed 26/12/2015)

Nikodinovska-Stefanovska, S. (2012). Lisbon Treaty and the protection of personal data in the European Union. In: Dimitrijevic, D. Miljus, B. (eds.) *Harmonizacija zakonodavstva Republike Srbije sa pravom Evropske Unije*. Beograd: Institut za medunarodnu politiku i privredu, Institut za uporedno parvo, Hans Zajdel Fondacija.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Communication COM. (2012). 10 final.

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf p.2 (accessed 26/12/2015)
Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. (2012). COM (2012) 10 final. 25/1/2012.
http://ec.europa.eu/homeaffairs/doc_centre/police/docs/com_2012_10_en.pdf (accessed 29/12/2015)
Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (2001). OJ L 8/1, 12. http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001R0045 (accessed 24/12/2015)
Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 (2007). C 306, 17 December 2007. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT (accessed 28/12/2015)

STRUČNI RAD

Damir Maračić[363]

WEB STRANICA EUROPEAN JUDICIAL NETWORK (EJN) KAO POMOĆ PRI USPOSTAVI MEĐUNARODNE PRAVOSUDNE SURADNJE

Sažetak

Europska pravosudna mreža (European Judicial Network) (u daljnjem tekstu EJN), utemeljena je 1998. godine na razini zemalja Europske unije. EJN je utemeljen prije svega zbog razmjene informacija o pravosudnim sustavima i pravnim izvorima zemalja Europske unije, dok se njegovim razvojem danas mogu dobiti i razmijeniti informacije i o pravosudnim sustavima trećih zemalja. Informacije se preko EJN mogu crpiti preko osoba iz pravosudnih i/ili policijskih tijela, registriranih kontaktnih točaka pojedinih zemalja ili preko web stranice EJN koja se nalazi na web adresi www.ejn-crimjust.europa.eu/ejn/EJN_Home.aspx . Sadržaj spomenute web stranice i poveznice na druge izvore opsežan su i kompetentan izvor podataka o pravosudnim sustavima zemalja EU, zemalja kandidata za EU, pridruženih zemalja i trećih zemalja te je riječ o vrijednom "alatu" koji može olakšati uspostavu međunarodne pravosudne suradnje. U radu su prikazane sve sastavnice web stranice EJN-a koje se odnose na bilo koji oblik međunarodne pravosudne suradnje u kaznenim stvarima te je namjera da se kroz rad predstavi puni potencijal i prednost takvog sadržaja informacija, koji je javno dostupan i može usmjeriti potencijalnu međunarodnu pravosudnu i policijsku suradnju u kaznenim stvarima kroz bilo koji vid djelovanja.

Ključne riječi: *European Judicial Network (EJN), Europska pravosudna mreža u kaznenim stvarima (EPMKS), međunarodna pravosudna suradnja, međunarodna policijska suradnja, web stranica EJN.*

1. UVOD

Pristupanjem Republike Hrvatske u Europsku uniju 1. srpnja 2013. godine, među mnoštvom propisa usklađenih s pravnom stečevinom Europske unije, na snagu je stupio i *Zakon o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije*[364]. Spomenutim Zakonom (u daljnjem tekstu ZPSKS-EU) uređuje se pravosudna suradnja u kaznenim stvarima između domaćih pravosudnih tijela s pravosudnim tijelima zemalja Europske unije. Vodeći se temeljnim načelom uzajamnog priznavanja između država članica Europske unije i načelom učinkovite suradnje, propisana je pravosudna suradnja na područjima koja se odnose: na europski uhidbeni nalog i postupak predaje, nalog za osiguranje imovine ili dokaza, europski nalog za pribavljanje dokaza, priznanje i izvršenje odluka o oduzimanju imovine ili predmeta, priznanje i izvršenje odluka o novčanoj kazni, priznanje i izvršenje presuda kojima je izrečena kazna zatvora ili mjera koja uključuje

[363] Damir Maračić, predavač, Visoka policijska škola, MUP RH, e-mail: dmaracic@fkz.hr

[364] Zakon o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije. Narodne novine 91/10., 81/13., 124/13., 26/15.

oduzimanje slobode, primanje i izvršenje presuda i odluka kojima su izrečene probacijske mjere i alternativne sankcije, priznanje i izvršenje odluka o mjerama opreza i europski nalog za zaštitu.

Kako bi međunarodna pravosudna suradnja bila kvalitetnija i uspješnija, još je 1998. godine na razini Europske unije utemeljena *Europska pravosudna mreža u kaznenim stvarima* (u daljnjem tekstu EPMKS), izvornoga engleskog naziva *European Judicial Network* (EJN).

U skladu sa člankom 2. ZPSKS-EU, kojim su definirani uporabljeni izrazi i pojmovi, EPMKS je mreža osoba za kontakt država članica osnovana Zajedničkom odlukom Vijeća o osnivanju Europske pravosudne mreže od 29. lipnja 1998., sa svrhom poboljšanja pravosudne suradnje u kaznenim stvarima. Bitno je napomenuti kako je pravni temelj EJN-a ojačan tijekom 2008. godine odlukom Vijeća Europske unije 2008/976 o Europskoj pravosudnoj mreži.

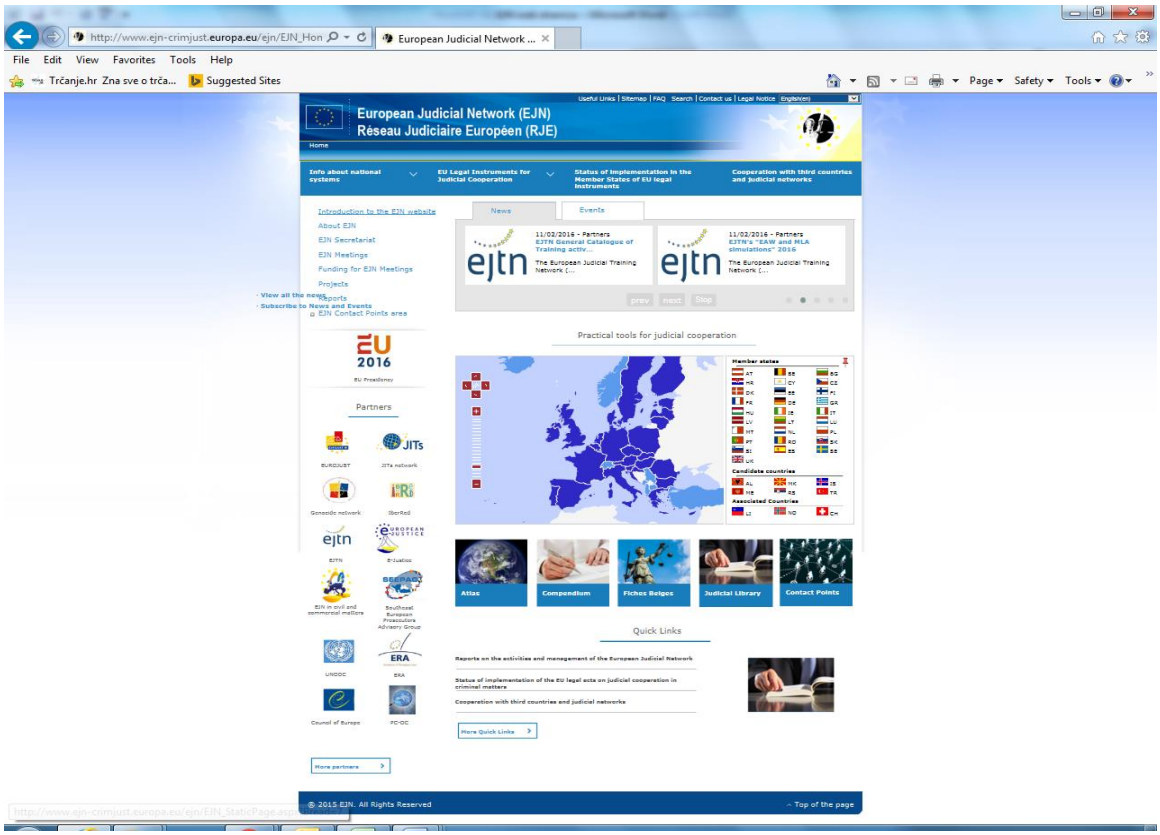
Jedan od alata Europske pravosudne mreže u kaznenim stvarima je *web stranica European Judicial Network* (EJN). Kreirana je i namijenjena svim zainteresiranim potencijalnim korisnicima. Iako je ponajprije stvorena da olakša komunikaciju i dostupnost informacijama za kontaktne točke pravosudnih tijela zemalja Europske unije, na spomenutoj web stranici su cjelokupnoj zainteresiranoj javnosti dostupni podaci o uvjetima međunarodne pravosudne suradnje, i to ne samo u okvirima zemalja Europske unije, već i za zemlje pridružene EU, za zemlje kandidate za EU i za pojedine ostale zemlje na globalnoj razini. Web stranica EJN-a osim podataka o pravosudnoj suradnji nudi i druge korisne i praktične sadržaje i poveznice, pomoću kojih je lakše doći do traženih podataka o nekoj zemlji ili organizaciji te o mogućnostima uspostave suradnje u smislu prikupljanja potrebnih podataka i dokaza te postizanja zajedničke akcije, odnosno cilja.

Republika Hrvatska kao punopravna članica Europske unije preko svojih predstavnika sudjeluje u uređivanju spomenute internetske stranice i na taj način čini vidljivim svoje mogućnosti pravosudne suradnje, stoga je spomenuta internetska stranica potencijalni izvor podataka i zainteresiranoj domaćoj javnosti o važećim domaćim propisima koji su značajni u kaznenim stvarima.

Unatoč dostupnosti i otvorenosti izvora web stranice te velikom broju mogućnosti pretraživanja i usporedbe, javnost iz hrvatskih pravosudnih i policijskih tijela ne koristi u svome radu spomenute potencijale web stranice EJN-a. Sadržaji internetske stranice EJN-a su i dalje nepoznati većini spomenute javnosti i rijetko se koriste. Pretraživanjem sadržaja objavljenih stručnih i znanstvenih članaka uočljivo je da se vrlo rijetko navodi internetska stranica EJN-a kao izvor, iako su podaci s nje od velike vrijednosti. Stoga se u nastavku prikazuje struktura i mogućnosti uporabe internetske stranice EJN-a kako bi se stručna i šira javnosti upoznala s njom.

2. WEB STRANICA EUROPEAN JUDICIAL NETWORK (EJN)

2.1. Naslovnica



Slika 1: Prikaz naslovnice web stranice EJN-a, internetski izvor web stranica EJN[365]

Promatrajući naslovnicu web stranice EJN-a na slici 1, prosječnom korisniku već je na prvi pogled vidljiva njena preglednost i jednostavnost korištenja. Otvaranjem glavne stranice, korijena web stranice EJN-a, ističe se naziv mreže *European Judicial Network* (EJN) na engleskom jeziku i njen naziv na francuskom jeziku *Réseau Judiciaire Européen* (RJE).

Osnovna, početna web stranica kreirana je na engleskom jeziku, a u gornjem dijelu su poveznice za korisničku podršku podijeljene na: korisne poveznice, mapu weba, često postavljana pitanja, mogućnostima pretrage, kontaktiranje i izjava o pravima.

[365] http://www.ejn-crimjust.europa.eu/ejn/EJN_Home.aspx (15.veljače 2016.).

2.2. Mapa weba

Slika 2: Prikaz mape weba stranice EJN-a, internetski izvor web stranica EJN[366]

Iz slike 2 koja prikazuje mapu weba, grananje naslova i podnaslova web stranice, vidljive su osnovne podjele opisane kroz podnaslove.

1.2.1. O Europskoj pravosudnoj mreži (About EJN)

Kroz nazive podnaslova, koji su ujedno i poveznice, prvi naslov *About EJN* nudi nam opće, temeljne informacije o EJN-u i sadržaju web stranice. Prevođenjem naslova navedenih poglavlja s engleskog na hrvatski jezik nazire se i njihov sadržaj, dakle riječ je o osnovnom upoznavanju sa sadržajem web stranice EJN-a, mreže EJN-a, tajništva, sastanaka i njihovih financiranja, projekata i izvješća. Područje za EJN kontaktne točke nije javno dostupno i do njega mogu pristupiti samo kontaktne točke, uz korisničke vjerodajnice. Valja napomenuti kako se u području *About EJN* nalaze brošure na jezicima EU, ali i drugim jezicima u kojima se opisuju osnovne zadaće i navode informacije o EJN-u. Pored u uvodu navedenih povijesnih činjenica u svezi s EJN-om, u brošurama je navedeno da je EJN prvi u praksi strukturirani mehanizam pravosudne suradnje sa stvarnim poslovanjem unutar Europske unije, osnovan za borbu protiv teškog kriminala na decentraliziran, fleksibilan i horizontalan način. Trenutno predstavlja preko 400 kontaktnih točaka širom EU, a također i u državama kandidatima i trećim zemljama.

U brošuri su navedeni podaci o tajništvu EJN-a koje je smješteno u Nizozemskoj te kao upravno tijelo osigurava funkcioniranje i kontinuitet EJN-a. Njegove glavne odgovornosti uključuju: omogućavanje kontaktnih točaka za ispunjenje svojih ciljeva; postavljanje, održavanje i poboljšavanje EJN web stranice i njezinih operativnih e-alata; širenje informacija na kontaktne točke i interesne skupine o EJN aktivnostima i pravnoj suradnji; osiguranje

[366] http://www.ejn-crimjust.europa.eu/ejn/sitemap.aspx (15. veljače 2016.).

zastupanja i uspostavljanja odnosa s drugim pravosudnim mrežama i strukturama u području pravosudne suradnje unutar i izvan Europske unije. Opisujući svrhu djelovanja EJN-a navedeno je kako je cilj stvoriti učinkovitiju pravosudnu suradnju posebice u borbi protiv teškog kriminala, putem aktivnog posredovanja, osiguravanjem pravnih i praktičnih informacija nadležnim lokalnim vlastima, uključujući i putem web stranice, osiguravanjem potpore zahtjeva za pravosudnu suradnju, stvaranjem pravne kulture Europske unije i suradnjom s drugim pravosudnim mrežama, trećim zemljama i pravnim partnerima.

1.2.2. Pravni alati (Legal Tools)

Kroz sadržaje podnaslova *Legal Tools* dolazimo do najvrjednijih informacija za bit ovog rada, do pravnih "alata", dakle praktičnih informacija o raznim oblicima međunarodne pravosudne suradnje i komunikacije koja prethodi ili se ostvaruje tijekom nje, što će u nastavku biti potanko opisano. Riječ je prije svega o podnaslovima *Atlas, Compendium, Fiches Belges i Judicial Library.*

1.2.3. Novosti (Announcements)

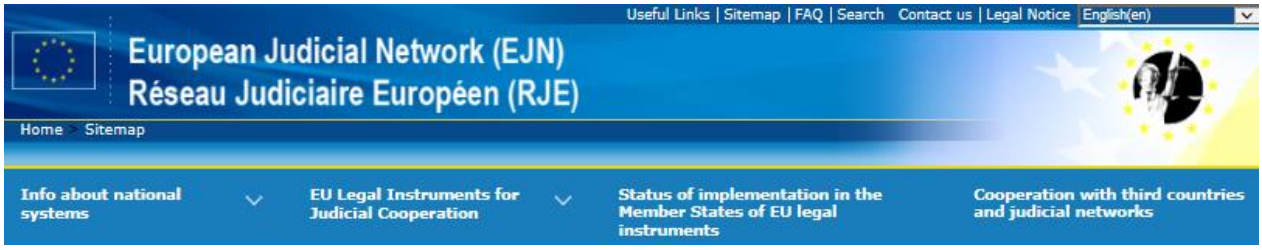
Kroz treću kolonu s mape weba pod naslovom *Announcements* može se pristupiti podacima o novostima, događajima, suradnji s trećim zemljama i o podacima o statusu implementacije pojedinih pravnih akata koji uređuju područje međunarodne pravosudne suradnje.

1.2.4. Partneri (Partners)

Posljednja kolona i poveznica naslova *Partners* vodi nas na sve partnere EJN-a, koji surađuju i doprinose kvaliteti i aktualnosti informacija web stranice. Riječ je o međunarodnim tijelima i organizacijama: Eurojust, Network of National Experts on Joint Investigation Teams, Network of contact point in respect of persons responsible for genocide and crimes against humanity, Ibero-American Network of International Legal Cooperation, European Judicial Training Network (EJTN), E-Justice, EJN in civil and commercial matters, SEEPAG – Southeast European Prosecutors Advisory Group, UNODC, Europol, OLAF, ERA, EPJUST II, Council of Europe, PC-OC (CoE), ECLAN, Euromed Justice III project, Network of Judicial international cooperation of the Portuguese speaking countries, Commonwealth Network of Contact persons, Moroccan Judicial network for international cooperation (MJNIC), Judicial Regional Platform of the Indian Ocean Commission, Sahel Judicial Platform (Judicial Regional Platform of Sahel countries).

1.2.5. Padajući izbornici – poveznice

Osim nabrojenih i opisanih kolona s mape weba, na njezinom vrhu su nabrojeni izbornici od kojih su neki ujedno i poveznice na pojedina temeljna poglavlja i podatke o međunarodnoj pravosudnoj suradnji i/ili mogućnostima za provođenje međunarodne pravne pomoći, što je vidljivo iz slike 3.



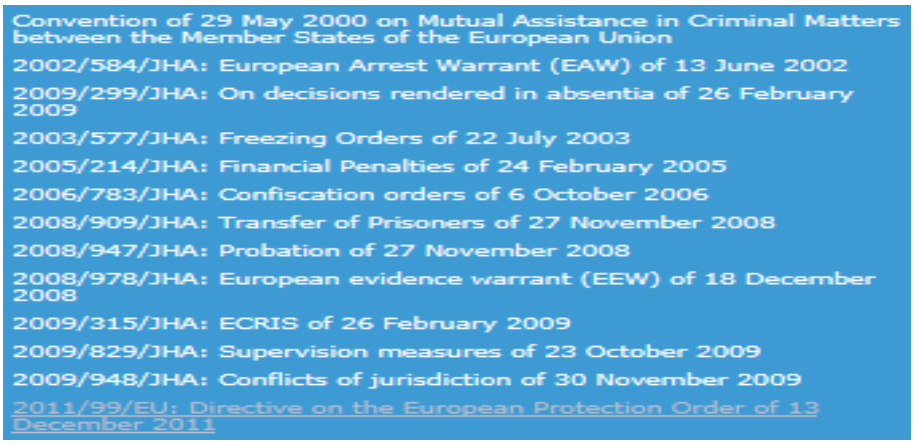
Slika 3: Prikaz padajućih izbornika – poveznica s web stranicom EJN-a, internetski izvor web stranica EJN[367]

Tako se pod naslovom *Info about national systems* dobiva prikaz s imenima zemalja Europske unije, zemljama kandidatima za EU i pridruženim zemljama, kao što je vidljivo iz slike 4, dok se odabirom pojedine zemlje očitavaju podaci o nacionalnom pravosudnom sustavu odabrane zemlje.

Slika 4: Prikaz sadržaja izbornika Info about national systems, internetski izvor web stranica EJN[368]

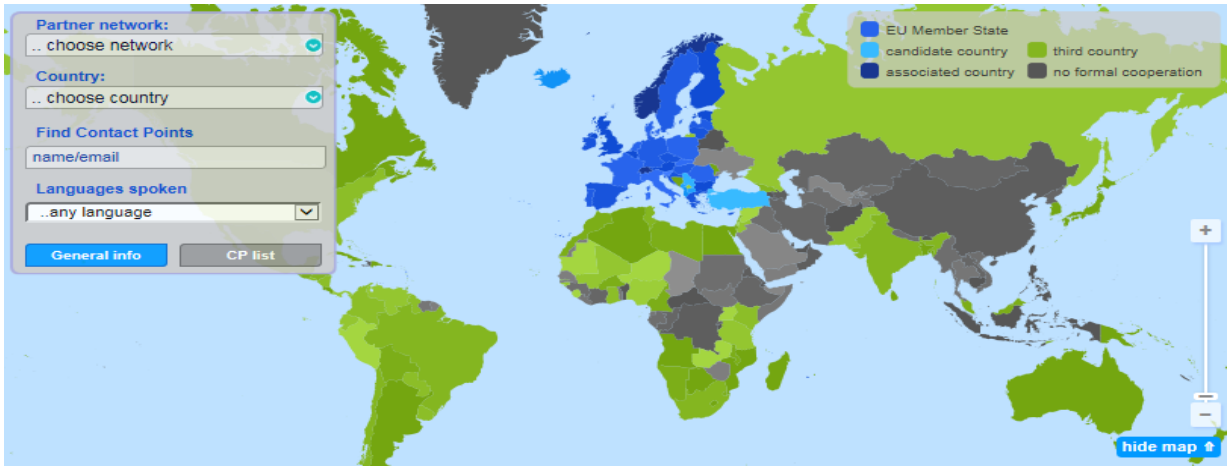
Odabirom sadržaja pod naslovom *EU Legal Instruments for Judicial Cooperation* kroz padajući izbornik dobivaju se mogućnosti povezivanja na temeljne pravne akte koja su donijela tijela Europske unije, a uređuju međunarodnu pravosudnu suradnju (slika 5).

[367] http://www.ejn-crimjust.europa.eu/ejn/sitemap.aspx# (15. veljače 2016.).
[368] http://www.ejn-crimjust.europa.eu/ejn/sitemap.aspx# (15. veljače 2016.).



Slika 5: Prikaz akata EU iz područja EU Legal Instruments for Judicial Cooperation, internetski izvor web stranica EJN[369]

Odabirom naslova *Status of implementation in the Member States of EU legal instruments* poveznica nas spaja na tablice s podacima o tijeku implementacije pojedinih pravnih akata od strane zemalja Europske unije, dok posljednji izbornik naslova *Cooperation with third countries and judicial networks* vodi na interaktivnu kartu s više padajućih izbornika, pomoću koje se filtriraju traženi podaci i moguće je pretraživati pravosudne sustave trećih zemalja (slika 6). Već jednostavni uvid u različitost boja označenih država svijeta na spomenutoj karti daje pregled mogućnosti/nemogućnosti suradnje s pojedinim zemljama.



Slika 6: Prikaz interaktivne karte s padajućim izbornicima poglavlja Cooperation with third countries and judicial networks, internetski izvor web stranica EJN[370]

[369] http://www.ejn-crimjust.europa.eu/ejn/sitemap.aspx# (15. veljače 2016.).
[370] http://www.ejnforum.eu/cp/network-atlas (15. veljače 2016.).

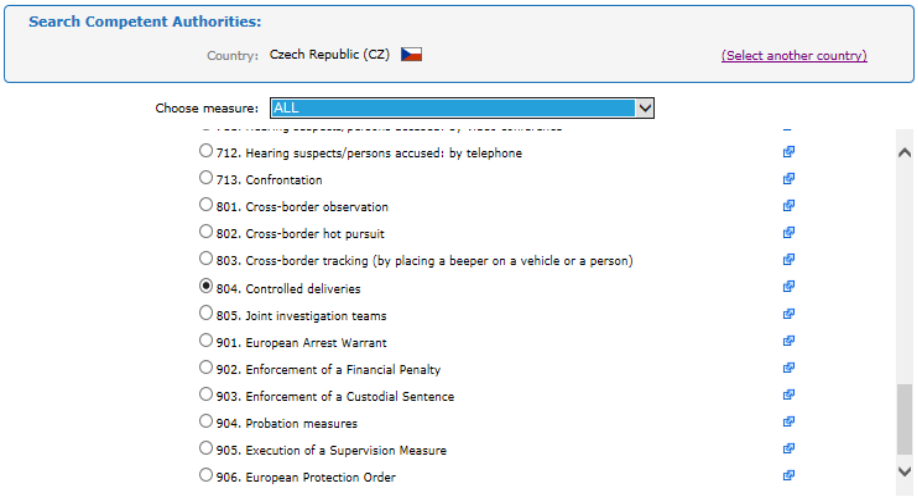
3. PRAVNI ALATI KAO POMOĆ PRI USPOSTAVI MEĐUNARODNE PRAVOSUDNE SURADNJE

U odjeljku *1.2.2. Legal tools* prikazuju se i opisuju najvrjedniji sadržaji s web stranice EJN-a, koji predstavljaju supstrate pojedinih pravosudnih uređenja u pogledu međunarodne pravosudne suradnje. Unatoč opstojnosti zajedničke pravne regulative, postoje i specifičnosti pojedinih zemalja, različiti statusi i stadiji implementacije i ratifikacije pojedinih propisa i akata i druge različitosti koje je uporabom naslovljenih alata moguće utvrditi i komparirati te pronaći najbolje rješenje za uspostavu kvalitetne i djelotvorne međunarodne pravosudne suradnje.

3.1. Atlas (Judicial Atlas)

Korištenje naslovljene poveznice omogućuje odabir zemlje prema kojoj namjeravamo uputiti zahtjev za međunarodnu pravosudnu suradnju, nakon čega se pomoću padajućeg izbornika prikazuje niz mjera i polja na kojima je takvu suradnju moguće ostvariti. Odabirom određene mjere prikazuje se pravni temelj korištenja i nadležnost pravosudnog tijela unutar te iste države. Pored toga, moguće je očitati podatke o ratifikaciji pravnog temelja za međunarodnu pravosudnu suradnju.

Iz slika 7 i 8 vidljiv je slijed i rezultat pretraživanja mogućnosti pravosudne suradnje s, primjerice Republikom Češkom na području nadziranog prijevoza i isporuke predmeta kaznenog djela, iz čega je vidljivo da je u prikazanom slučaju to moguće ostvariti temeljem Konvencije od 29. svibnja 2000. godine o zajedničkoj suradnji o kaznenim stvarima između zemalja članica Europske unije te da je nadležno tijelo s kojim valja kontaktirati Ured regionalnog javnog tužitelja u Pragu.



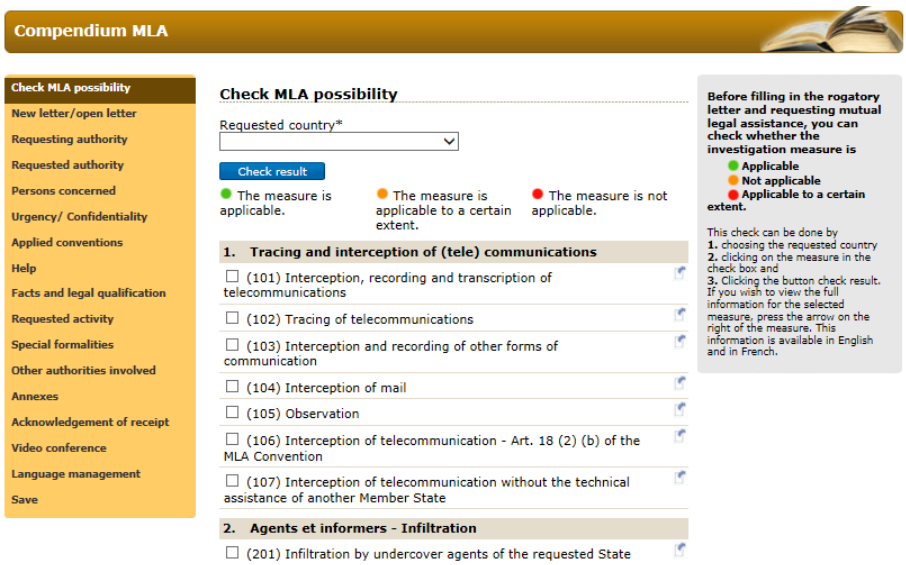
Slika 7: Prikaz pretrage za pravni temelj i nadležnost u pojedinim zemljama EU, internetski izvor web stranica EJN[371]

[371] http://www.ejn-crimjust.europa.eu/ejn/AtlasChooseMeasure.aspx?MP=0&Cou=259 (15. veljače 2016.).

Slika 8: Prikaz rezultata pretrage za pravni temelj i nadležnost u pojedinim zemljama EU, internetski izvor web stranica EJN[372]

3.2. Compendium

U odnosu na podnaslov naziva *Compendium*, doslovni prijevod naslova s engleskog jezika na hrvatski daje nam odgovor na sadržaj poveznice. Riječ je o sažetom prikazu mogućnosti međunarodne pravne suradnje na određenom polju.



Slika 9: Prikaz sažetaka mogućnosti međunarodne pravne pomoći, internetski izvor web stranica EJN[373]

Padajući izbornik (prikazano na slici 9) omogućuje odabir zemlje za koju se provjeravaju mogućnosti međunarodne pravne pomoći, a odabirom područja ili konkretnih mjera koje se namjeravaju provesti dobiva se osnovni odgovor s mogućnošću, uvjetovanom mogućnošću ili nemogućnošću provedbe željene mjere. Pored osnovnog odgovora, dodatno se mogu učitati detaljniji podaci u pisanom obliku, koji se odnose na mogućnosti primjene iste mjere ili istih mjera.

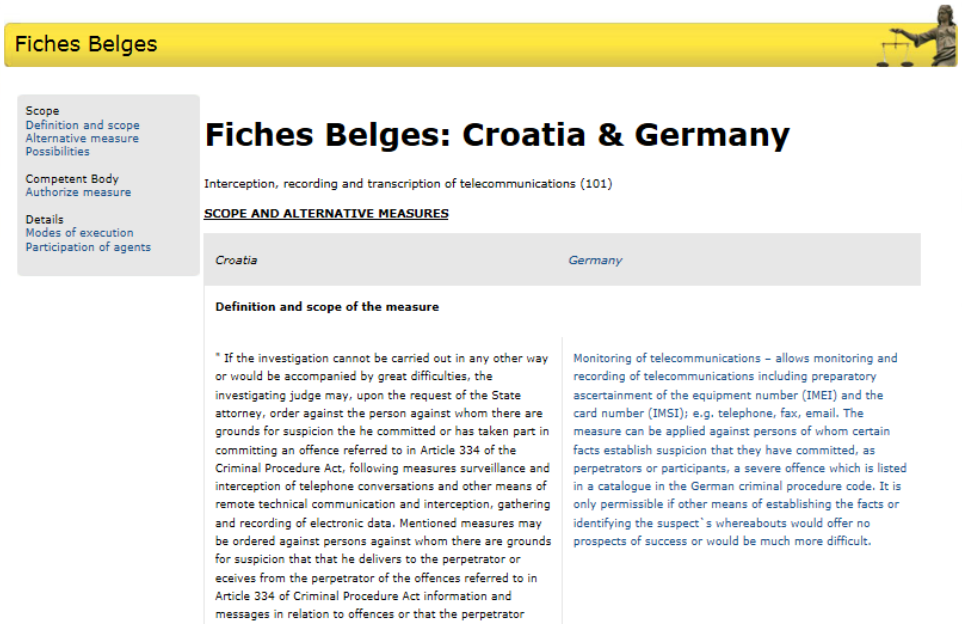
Osim navedene provjere mogućnosti uspostave pojedinih mjera, kroz ovo poglavlje je moguće kreirati i pojedine zahtjeve za međunarodnu pravnu pomoć i europski uhidbeni nalog. Pri tome je stranica koncipirana tako da se korisnika korak po korak vodi kroz formiranje

[372] http://www.ejn-crimjust.europa.eu/ejn/AtlasSelection.aspx (15. veljače 2016.).
[373] http://www.ejn-crimjust.europa.eu/ejn/EJN_Compendium.aspx (16. veljače 2016.).

zahtjeva i svih nužnih elemenata, uz pružanje potrebnih informacija o nadležnim tijelima i relevantnim pravnim aktima.

3.3. Usporedni prikaz provedbe mjera međunarodne suradnje (Fiches Belges)

Poveznica *Fiches Belges* omogućuje kreiranje usporednog prikaza mogućnosti provedbe pojedine mjere međunarodne pravne suradnje između dvije zemlje EU. Pritom su opisani opseg provedbe, alternativne mogućnosti, stvarna nadležnost i praktični savjeti u smislu primjene promatrane mjere. Na slici 10 prikazan je dio usporednog prikaza između Republike Hrvatske i Savezne Republike Njemačke, u pogledu mogućnosti primjene posebne dokazne radnje nadzora i tehničkog snimanja telefonskih razgovora i drugih komunikacija na daljinu.



Slika 10: Usporedni prikaz mogućnosti provdbe mjere nadzora komunikacija između RH i SR Njemačke, internetski izvor web stranica EJN[374]

3.4. Pravosudna knjižnica (Judicial Library)

Poveznica nas vodi do daljnjih mogućnosti odabira sadržaja iz pravosudne knjižnice, a moguće je izabrati sadržaje iz kategorija:

a) pravnih instrumenata (usvojili EU, Vijeće Europe ili UN)

b) statusa implementacije pojedinih pravnih instrumenata

c) stajališta o dobroj praksi u međunarodnoj pravnoj pomoći u kaznenim stvarima

d) obavijesti i deklaracije o međunarodnoj pravnoj pomoći

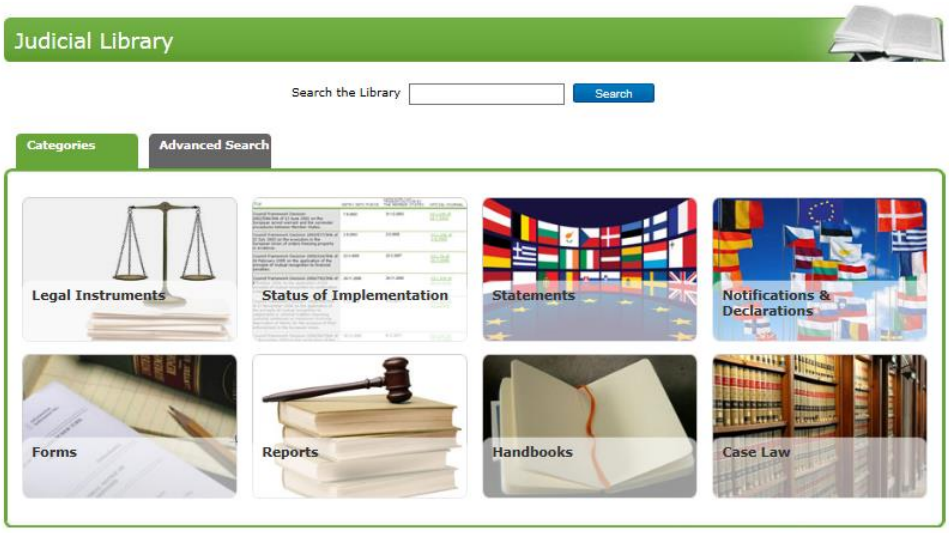
e) obrasci akata i zahtjeva po zemljama

f) izvješća zemalja o EJN i MLA aktivnostima

[374] http://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelgesResult.aspx?measure=101&country=432&other=277 (16.veljače 2016.).

g) priručnici

h) primjeri sudske prakse.



Slika 11: Prikaz sadržaja pravosudne knjižnice web stranice EJN-a, internetski izvor web stranica EJN[375]

4. ZAKLJUČAK

Europska unija i njena tijela omogućili su cijeli niz mehanizama i alata koji pojednostavljuju i olakšavaju komunikaciju između zemalja članica, ali i s drugim zemljama. Web stranica *European Judicial Network* (EJN) samo je jedan od alata koji pruža pomoć pri uspostavi međunarodne pravosudne suradnje, a predstavljen je u ovom radu kroz sažeti prikaz sadržaja i kroz prikaz potencijala koji se u svojoj punini očituju elektroničkom primjenom. Namjera je i ideja vodilja upoznavanje potencijalnih korisnika i zainteresirane javnosti i na neki način promocija internetske stranice do koje javnost, ponajprije stručna, nije dovoljno doprla, a vrijednost njezina sadržaja je značajna.

LITERATURA

Anić, V. i sur. (2003). *Hrvatski enciklopedijski rječnik*. Zagreb: Novi liber.
Gačić, M. (2001). *Pisanje i objavljivanje znanstvenih i stručnih radova.* Zagreb: MUP RH Policijska akademija.
Panian, Ž. (2005). *Informatički enciklopedijski rječnik*. Zagreb, Europapress holding.
Zakon o međunarodnoj pravnoj pomoći u kaznenim stvarima. Narodne novine 178/04.
Zakon o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije. Narodne novine 91/10., 81/13., 124/13., 26/15.
Web stranica European Judicial Network (EJN), www.ejncrimjust.europa.eu/ejn/EJN_Home.aspx .

[375] http://www.ejn-crimjust.europa.eu/ejn/libcategories.aspx (16.veljače 2016.).

Damir Maračić

WEB PAGE EUROPEAN JUDICIAL NETWORK (EJN) AS HELP FOR ESTABLISHING INTERNATIONAL JUDICIAL COOPERATION

Summary

The European Judicial Network (hereinafter referred to as EJN) is an international judicial network established in 1998 at the level of the European Union Member States, primarily with the aim of exchanging information on judicial systems and legal sources of the European Union Member States, while, due to its development, today it also allows for the provision and exchange of information on judicial systems of third countries. Information from EJN can be obtained through persons in judicial and/or police authorities, registered national contact points or through the EJN website at www.ejn-crimjust.europa.eu/ejn/EJN_Home.aspx.
The content of the mentioned website and links to other sources represent a comprehensive and competent source of information on judicial systems of the EU Member States, EU candidate countries, associated countries and third countries, and it is certainly a valuable "tool" that can facilitate the establishment of international judicial cooperation. This paper introduces all the elements of the EJN website referring to any form of international judicial cooperation in criminal matters and aims to present the full potential and all the advantages of such information which is publicly available and which can direct potential international judicial and police cooperation in criminal matters, through any kind of action.

Key words*: European Judicial Network (EJN), European Judicial Network in Criminal Matters (EPMKS), International Judicial Cooperation, International Police Cooperation, EJN Website.*

PRELIMINARY PAPER

Marjan Gjurovski[376]

Lazar Gjurov[377]

THE CONCEPT OF SECURITY OF CRITICAL INFRASTRUCTURE IN TERMS OF RISKS AND CRISES

Summary

In modern world, the concept of protection and security of critical infrastructure is very important. After the protection of individuals, the protection of socially important capacities is the next most important priority of the state. There are many reasons for risk and danger to critical infrastructure.

Critical infrastructure and its protection are the basis for the functioning of social and political life. Material objects as part of critical infrastructure and its protection are in the domain of state bureaucracy, which regards them as passive material objects. Nevertheless, material infrastructure is an object the material structure of which galvanizes and/or limits the influence on social everyday life so it cannot be treated as a passive object. Generally speaking, security subjects and objects are individuals and their collectives in form of community, society, nation, state that generate different cultural values, norms, ways of life, etc. The issue of security of critical infrastructure and material objects has had secondary importance. Given the fact that society represents a scope of human relations, within which the issues of identity, freedom, right, equality, etc. are realized and intertwined, and then these objects have a marginal role. They are just mere recipients that people use to imprint their ideal projections onto.

Rapid changes in international relations, crisis and compounded security threats have become part of our everyday life. This kind of environment is characterized by a phenomenon of increasing transnational security threats, which are becoming a threat to the man as well as to an individual and infrastructure facilities that he has created. Consequently, individual protection and protection of infrastructure facilities (or the system of these facilities) the security threat of which endangers the lives and health of people in a certain narrower or wider imperatives represent the today's security structures both at local and regional level. Following all the above, the aim of this paper is to get closer to the notion of critical infrastructure, what it means for the functioning of a society, and why its protection is becoming imperative in the times to come.

Keywords: *the state, the individual, security, protection, infrastructure, critical infrastructure, materiality*

[376] ass. prof. dr. sc. Marjan Gjurovski, Faculty of Security-Skopje, Republic of Macedonia e-mail: mgjurovski@fb.uklo.edu.mk

[377] ass. prof. dr. sc. Lazar Gjurov, Military academy „General Mihailo Apostolski“ Skopje, associate member of UGD – Stip, e-mail: lazar.gurov@ugd.edu.mk

1. INTRODUCTION

In the modern theory, there are several definitions of the term "critical infrastructure" (CI) and it is impossible to find one definition that is generally accepted and the reason of that is the everyday development of new technological achievements of the human civilization and in fact, the very same technological development allows those achievements of the human civilization. Actually, that technological development enables improvement of the methods of threat toward the human and toward everything that the civilization has created. The most definitions refer to the means and the property, which are essential for the functioning of the economy and the society. In USA the contemporary theoreticians define the critical infrastructure in the following way: „The critical infrastructure and the general resources (*Critical infrastructure and key resources – CIKR)* is a term that refer to wide range of different means and properties that are necessary for the everyday functioning of the social, economic, political and cultural system in the USA. Any interruption of the elements of the critical infrastructure is a serious threat for the proper functioning of these systems and can lead to damage of the property, human victims and a serious economic loss".

A similar definition of the term CI we can find among the Australian authors who define it as: "The critical infrastructure represents the physical objects, the supply network, the informatics technology and the communication network, which if get destroyed, or if get immobilized for a long period can significantly influence the social and the economic welfare of the nation, or they could influence the ability of Australia to keep the national defense and the national security." [378]

Unlike the USA and Australia in the European Union we can find two definitions of the CI that prevail on the European Continent and these are: the critical infrastructure is a property, system or its part which is located on the territory of the member country and which is necessary for keeping the key social functions, health, security, economic and social welfare and which damage or destruction may influence the member country. The second definition claims that „The European critical infrastructure means critical infrastructure located on the territory of the member country which damage or destruction may influence at least two member countries. A significant disruption of the functioning of the elements of the critical infrastructure can be estimated based on the criteria of interdependence. It includes the effects that are results of the inter-ministerial depending on other types of infrastructure." [379]

The concept of the CI origins from the 1960s and 1970s and it represents the all systems, organizations, goods and services without which the (modern) society and the state could not survive, maintain stability of functioning and development. The CI also includes the following sectors: energy production; water resources and water supply; health care system; communication / information technology; transport; chemical industry; biological substances; banking and financial systems; public administration; media; research institutes etc. Some of the definitions describe the critical infrastructure as „systems and products-

[378] Division of the Attorney-General's Department, 2003
[379] Council Directive 2008/114/EC, 2008

material and virtual, that are vital for the nation in a way that their incapacity or destruction can weaken or destroy the economic stability of a country and/or its public health and security“’ (US National Protection Plan – NIPP). The European Commission provides the following definition in the document „Protection of the critical infrastructure in the fight against the terrorism“ (2004): „The critical infrastructure consists of those material and informational and technological capacities, networks, services and products which if are under threat or destroyed may seriously influence the health, the security or the economic welfare of the citizens or the efficiency of the government of the countries members.“ The importance and role of these systems in modern society (which led to the emergence of industrial society the term), ie human, material, information resources available, financial and political power they generate, however, did not make the most stable elements of society in terms of security, on the contrary, organizational and territorial arrangements, technical and technological characteristics of the resources available to do subject to a number of different risks. From the perspective of a (responsible) country, the number of risks and their consequences for the citizens increases with the process in which "public monopolies are transformed into several decentralized organizations, competitive or privatized organizations”.

As could be seen, the understanding of the term CI is set quite wide, so it is difficult to found the sectors that are not critical. However, the modern theory and practice are increasingly focused on protecting the communications and information infrastructure, which may cause enormous financial damage or damage by stealing data.

2. DEFINING OF THE NATIONAL CRITICAL INFRASTRUCTURE

As it is very difficult for the term critical infrastructure to be defined it is even harder to be specified everything that the term critical infrastructure includes. However, by quoting *J. Moteff and P. Parfomak*, and their publications („*Critical Infrastructure and Key Assets: Definition and Identification“* and *„National Infrastructure Protection Plan“)*, it could be said that one national CI involves the following elements/systems:

1. Information and communications (telecommunications, networks, internet)
2. Electrical power
3. Transport
4. Oil and gas (supply, transport, refining and distribution)
5. Banking and financing
6. Water and Emergency services
7. Government (+military) (Moteff and Parfomak, 2009).

Within the framework of the directive 2008/114 EC, the elements/sectors for which it is necessary to define the CI are appointed, as it is listed in the Table 1.

Table 1: Sectors of the critical infrastructure in EU

Sector	Subsector	
I Power	1. Electrical power	Infrastructure and facilities necessary for the production and supply of electrical power
	2. Oil	Oil production and refining
	3. Gas	Gas production and refining
II Transport	4. Road transport Rail transport Air transport Inland waterway transport (rivers, lakes)	

The CI is interrelated on different ways and levels. A malfunction of a part of it can influence the other elements and vice versa. In general, the interdependence among the critical infrastructure is very expressive as illustrated on Figure 1.

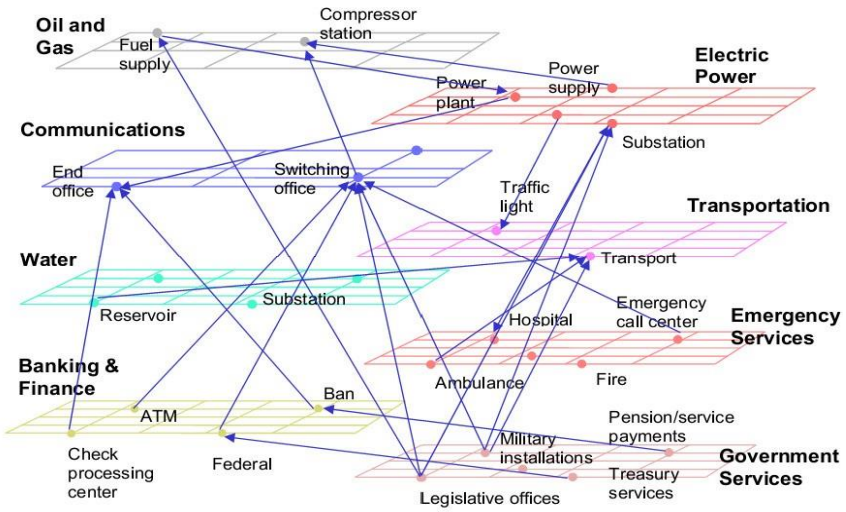


Figure 1: The interdependence among different infrastructures

In the Figure 1, it is evident that in the telecommunications sector and the large number of infrastructure elements there is a strong connection. Almost all the elements related to services for the production and distribution of electricity, water, gas, etc. require communication in some form. On the other hand, the communications sector largely depends on the other sectors. On this basis, we can conclude that the telecommunication sector is an infrastructure whose position is central and the understanding and modeling of the risks are associated with the interruption of communications should be given priority in consideration of critical infrastructure, to increase the level of public safety and resilience of the infrastructure side impacts.

3. STANDARDS IN PROVIDING A CRITICAL INFRASTRUCTURE IN THE EU AND THE US

The European Union aims to ensure an adequate level of safety and equipment for the selected critical infrastructure, which is feasible only if there is a common European framework as its protection. The interest for the critical infrastructure of the EU by its Member States comes from the danger of destruction or disruption of a particular critical infrastructure in one Member State, which can directly endanger the other member states. In such cases, the security measures are as strong as their weak link[380]. In accordance with European Union standards, critical infrastructure includes electricity; production and transmission, chemical industry and nuclear power plants, manufacturing, transportation and distribution of oil and natural gas, telecommunications systems, water resources, production of basic foodstuffs, heating system, public health institutions and services, public transport system, government bodies financial and security institutions. In this regard, and based on a directive of the European Commission, "EU COM (2006) 786 final, the EU adopted a European program to protect critical infrastructure, which includes a list of European Critical Infrastructure (ECI), created on the basis of proposals submitted by the Member States.

The concept of "critical infrastructure" in the United States, includes those products, systems and networks, and tangible and intangible, which are of such importance to the United States as their disabling or destruction would jeopardize national security system, the economic security of the state, public health and public security. In fact, any of these systems, individually or in combination (USA Patriot Act 2001, October 2001). In this regard, the critical infrastructure consists of public and private institutions in the sectors of agriculture, food, health care, emergency services, government, defense, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, mail and transportation. In order to protect and ensure the continued operation and national critical infrastructure and key resources (CIKR), Regulation of the President of the United States, introduced the marks 7 (I-ISPD-7), which provided guidelines for the establishment of a system the protection of these resources from potential attacks that jeopardize their functioning.

[380] Z.Kekovic, D.Caleta, Z.Kesetovic, Z.Jeftic, Nacional critical infrastructure protection –regional perspective, Faculty of security studies, Belgrade 2013

In the Committee on Homeland Security of the United States, a sub-committee deals with "security of computer networks and communications, information technology, production management systems, system power supply and databases, and government and private, from internal and external attacks, prevent depopulation and infrastructure"[381].

Because of that, the cyberspace is a nervous system: a system for managing the US economy and national security the country depends on, in February 2003, was brought up a National Strategy to secure cyberspace.

The consequences of a new understanding of the threats to the security of America and the United States embodied in strategies, directives and laws:

- Working on the development of the National Communications System (NCS),
- Reorganization of the intelligence community,
- Physical protection of an important facilities of the critical infrastructure,
- Insisting on the key role of the information technology in the growth of internal security,
- Support for the technological superiority of the United States,
- Support for the research in the field of protection of information infrastructure and training of citizens for acquiring habits of survival in case of techno gene and natural disasters and terrorist attacks.

4. EXPERIENCES AND CHALLENGES OF THE SOUTHEAST EUROPE

In the case of the countries of the former Yugoslavia, it is obvious that all of them strive to identify and define their critical infrastructures as accurately as possible.

Therefore, by the resolution of the Government of the Republic of Slovenia in 2010, it was established that the CI in this country is covering all goods and services that are essential for the country. Their disruption or destruction would have a major influence on the national security and the economy. Thus, CI is the vital in social functioning, health, safety, protection, and overall social welfare.

Macedonia has no specific law that is regulating the CI. However, some legal acts are placed on the protection of CI, which is in the direct jurisdiction of the Ministry of Interior, Ministry of Defense and the Ministry of Transport and Communications.

In the November 2008, the Republic of Croatia has adopted the Strategy for Prevention and Suppression of Terrorism. In this strategy, the critical national infrastructure is defined as the set of tools, services and systems that support the economic, political and social life. Partial or complete threat may result in loss of life, threats to national security and the functioning of the economy, and could seriously jeopardize part of the community or the union[382].

---

[381] [381] Z.Kekovic, D.Caleta, Z.Kesetovic, Z.Jeftic, Nacional critical infrastructure protection –regional perspective, Faculty of security studies, Belgrade 2013

[382] Z.Kekovic, D.Caleta, Z.Kesetovic, Z.Jeftic, Nacional critical infrastructure protection –regional perspective, Faculty of security studies, Belgrade 2013

In 2009, the Government of the Republic of Serbia adopted a Decision for determining the main technical systems important for defense. In accordance with this decision, the eight main technical systems in the areas of transport and telecommunications were involved in the CI resources in the Serbia. They are important for the defense of the state, as well as three public companies and four companies in the field of energy, public company and company in the field of coal production and 12 public enterprises and institutions in the field of water supply, transfer of thermal energy, forest management and broadcasting. This Decision shall regulate the notification procedure concerning the selection, construction and development of these systems, procurement of technical equipment and in providing technical equipment and setting requirements for their alignment with the needs of national defense.

The investor is obliged to inform the Ministry of Defense and the other ministries authorized for choosing, building of critical capital facilities, and the development of technical systems essential for the defense and for the purchase of technical equipment of importance for the functioning of these systems. The investor also submits the notification of the relevant investment, technical documentation system specifications for the purchase of technical equipment and program to explain the development of basic systems.

The most of the countries have defined their own critical infrastructure. However, in the region of Southeast Europe has been little or almost nothing done about the issue of national critical infrastructure. The biggest step forward in the process of determining the national critical infrastructure has the Republic of Croatia as a full member of the EU, which adopted a law on the protection of critical infrastructure.

The other countries from Southeast Europe have done quite a bit on the issue of defining the critical national infrastructure, although they have all the necessary conditions for the adoption of such legal acts.

5. CONCLUSION

The critical infrastructure has to be specially protected and that is very important in order to be provided a normal operation as one of the most difficult problems that can occur called chain reaction, which is transferred to the other system, and comes to a multiplication of effects. The aforementioned results of disturbances within the systems theory is described as an effect cascade or domino effect. For these reasons, the main task of managing critical infrastructure is preventing or reducing the probability of occurrence of natural or man-induced incentives that could lead to catastrophic distortions in the protected systems.

The process of European integration, among other things, also seeks to establish a connection and interoperability between the regional infrastructure and the infrastructure of the EU as a whole. In this regard, a special emphasis is placed on the critical infrastructure as holder of the stability of economic development and social relations. Therefore, the recommendations and legal framework for the protection of these resources are becoming a necessity in national development programs.

REFERENCES

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. (2008). *Official Journal of the European Union L*, pp. 345-375 (retrieved 23/12/2008).

A Division of the Attorney-General's Department (2003). *Critical Infrastructure Emergency Risk Management and Assurance*, Emergency Management Australia.

European Union Council Directive 2008/114/EC (2008). (retrieved 08/122008).

European Commission (2012). *Commission staff working document on the review of the European Programme for Critical Infrastructure Protection (EPCIP).*

Homeland Security (2009), *National Infrastructure Protection Plan*, Homeland Security.

Moteff, J., Parfomak, P. (2004). *Critical Infrastructure and Key Assets: Definition and Identification.* The Library of Congress, Congressional Research Service.

Murray, T.G.A.T. (2012). Critical infrastructure protection: The vulnerability conundrum. *Telematics and Informatics*, 29(1), 56-65.

Čaleta, D. (2010). Kritična inftastruktura i značaj osiguravanja njenog neprekidnog djelovanja. ADRIA - stručni magazine za kompletna sigurnosna rješenja, Sarajevo: DTP&Art Dizajn.

Kekovic, Z., Caleta, D., Kesetovic, Z., Jeftic, Z. (2013). *Nacional critical infrastructure protection – regional perspective*. Belgrade: Faculty of security studies.

Weinberg, L. (2004). *The Challenges of Conceptualizing Terrorism, Terrorism and Political Violence.* Reno, Nevada: University of Nevada.

PREVENCIJA KRIMINALA – DOPRINOS NOVIH TEHNOLOGIJA/ CRIME PREVENTION - CONTRIBUTION OF NEW TECHNOLOGIES

STRUČNI RAD

Dragan Arlov[383]
Milan Popović[384]

KVALITETA UTVRĐIVANJA OPRAVDANOSTI I PRAVILNOSTI UPOTREBE SREDSTAVA PRINUDE U FUNKCIJI JAČANJA ODNOSA POLICIJE I DRUGIH GRAĐANA

Sažetak

Upotreba sredstava prinude, od strane ovlašćenih službenih lica, predstavlja izuzetnu mogućnost za jačanje poverenja javnosti u rad policije, ali u isto vreme, i mogućnost njegovog narušavanja. Profesionalizam, u radu policije, je uslov za jačanje tog poverenja. U isto vreme, neprofesionalan odnos, u vidu neopravdane i/ili nepravilne upotrebe sredstava prinue, direktno i sa značajnim odjekom u javnosti, utiče na ukupno poverenje gradjana u rad policije. U izgradnji ili narušavanju medjusobnog poverenja, izuzetnu ulogu imaju mediji. Policija, mediji, ali i gradjani pojedinačno, angažovanjem postojećih tehnologija, mogu značajno uticati na kvalitet dokazivanja pojedinačnih problemskih situacija kao zakonskog osnova za upotrebu sredstava prinude, time i kvaliteta postupka utvrdjivanja opravdanosti i pravilnosti primene ovlašćenja. U radu se na tri upotrebe sredstava prinude, pripadnika policije, pokrivene video zapisima, različitih autora, na različitim prostorima (SAD, Hrvatska, Srbija) kao studije slučajeva, analizira doprinos video zapisa utvrdjivanju istine. Specifične kompetencije rukovodećih policijskih službenika, u vidu znanja u stvaranju uzročno posledične veze izmedju pojedinačne problemske situacije, korišćenja diskrecionog prava, poznavanja principa u rešavanju problemskih situacija, izbora i upotrebe pojedinačnih alata i kriterijuma u vrednovanju kvaliteta izvršenja službenog zadatka, su veoma važni za spoznaju istine o dogadjanju. Ništa manju važnost, u jačanju medjusobnog poverenja, ima i blagovremeno, adekvatno i kompetentno saopštenje javnosti, utvrdene istine.

Ključne riječi: *videozapis, prinuda, problemske situacije, zakonitost.*

1. UVOD

Obim poslova policije u svakom društvu je značajan i u funkciji je stvaranja povoljnog bezbednosnog ambijenta u zajednici. Cilj obavljanja poverenih joj poslova je da svakome obezbedi jednaku zaštitu bezbednosti, prava i sloboda, primenjujući zakon i ustavno načelo vladavine prava. Kako bi ostvarila svoju ulogu zaštite i unapredjenja bezbednosti gradjana i imovine, policija je u obavezi da razvija profesionalne kapacitete, kompetencije i etiku svojih pripadnika. U ostvarivanju društvene uloge policija i javnost su u stalnoj interakciji (ili bi

[383] Dragan Arlov, vanredni profesor, Univerzitet u Novom Pazaru, Pravni fakultet – pravo unutrašnjih poslova, nastavnik na predmetima: SFO I i SFO II – upotreba sredstava prinude, e-mail: dragan.arlov@uninp.edu.rs
[384] Milan Popović, Ministry of internal Affairs of Republic Serbia, Gandarmerie, Detachment in Novi Sad

morali biti) a kvalitet odnosa zavisi od niza faktora (očekivanje javnosti, uloga gradjanina kao pojedinca, očekivanje organizacije policije, kompetentnost postupajućeh policijskog službenika...) time i kvalitet njihovih ishoda. Kvalitet svakog neposredni odnos izmedju policijskog službenika i gradjanina kao pojedinca, direktno utiče na ukupni kvalitet odnosa policije i javnosti.

Pored uloge slučajnog prolaznika, svedoka, oštećenog, osumnjičenog... gradjanin može da ima izuzetno važnu ulogu i kao pojedinac koji pruža informacije policiji ili na drugi način pomaže, u cilju uticanja na kvalitet njenog rada, a time i na ukupan kvalitet ostvarenja društvene uloge. U cilju prethodnog, i gradjani mogu da koriste i blagodeti novih tehnologija, svakako uz poštovanje Ustavom zajamčenih ljudskih i manjinskih prava i sloboda i drugih zaštićenih vrednosti u demokratskom društvu. Navedeni odnos gradjanina kao pojedinca je opravdan i ne bi smeo biti uzrok nastajanja štetnih posledica prema njemu.[385]

Prinuda kao specifičnost policije je prostor u okviru ili povodom koga se ostvaruju neposredni kontakti izmedju gradjana sa ovlašćenjem na prinudu – policajaca, i drugih gradjana. U obavljanju poslova, pripadnicima policije je dozvoljeno da primenjuju samo mere i sredstva prinude koja su utvrdjena zakonom i kojima se rezultat postiže bez, ili sa što manje štetnih posledica po lice prema kome se mere preduzimaju.[386] Policija ima obavezu i potrebu utvrdjivanja istine o dogadjanju povodom koga je primenjeno ovlašćenje u vidu upotrebe sredstava prinude.

Dostupnost novih tehnologija, a naročito u vidu video zapisa, bez obzira na njihovo poreklo, značajno mogu pomoću u utvrdjivanju stvarnog dogadjanja a time i jedine istine o opravdanosti i pravilnosti primene ovlašćenja od strane policije. Tako utvrdjenu istinu veoma je važno blagovremeno i profesionalno saopštiti javnosti, svakako snagom argumenata i bez prostora za višesmisleno razumevanje.[387]

2. PROBLEMSKE SITUACIJE KAO OSNOVA ZA UPOTREBU SREDSTAVA PRINUDE

U okviru obavljanja poslova policije, ovlašćena službena lica (OSL) izvršavaju različite službene zadatke a u sklopu istih suočavaju se sa velikim brojem veoma različitih problemskih situacija. Analizom zakonskog teksta, mogu se prepoznati četiri globalne ili opšte problemske situacije i to: bekstvo, samopovredjivanje, otpor i napad.[388] Na osnovu

[385] Obaveza ministarstva je da neposredno saradjuje sa ovakvim gradjanima a na način da štiti njihova prava, pružanjem pravne i druge neophodne pomoći predvidjene članom 17. Zakona o policiji R Srbije (ZoP).

[386] Prethodno definisanje je sastavni deo teksta novousvojenog Zakona o policiji i isto je neznatno drugačije u odnosu na prethodno. Naime u prethodnom su mere i sredstva odvojena u tumačenju a na način da policijski službenici primenjuju mere i upotrebljavaju sredstva prinude koja su predvidjena u zakonu a na način da se profesionalni rezultat postigne bez nastajanja nepotrebnih štetnih posledica i gubljenja vremena.

[387] Značajno je i vreme i način kao i personalni izbor policijskog predstavnika za komunikaciju sa medijima time i sa javnošću. Preuzimanje ove uloge od strane najviših predstavnika ministarstva ostavlja prostora za različita shvatanja nemera.

[388] Ni u novousvojenom ZoP nema jasno navedenih problemskih situacija (svakako samo opštih) osim kod osnova za upotrebu sredstava za vezivanje. Tako se kod tumačenja fizičke snage u članu 110. ZoP, navodi pravo na njenu upotrebu radi odbijanja napada, savladjivanja otpora ili sprečavanja samopovredjivanja lica. Nema navoda o pravu na upotrebu sredstava prinude u vidu fizičke snage radi rešavanja problemske situacije bekstva, a

zajedničkih karakteristika, moguće je u okviru navedenih grupa, definisati značajan broj posebnih grupa problemskih situacija. U isto vreme, uz postojanje specifičnih kompetencija OSL, moguće je (neophodno) u okviru posebnih grupa problemskih situacije, definisati i značajno veliki broj pojedinačnih problemskih situacija, a po osnovu specifičnosti koje ih definišu i čine različitim od svake druge (Arlov, 2013). Upravo je mogućnost jasnog utvrdjivanja postojanja pojedinačne problemske situacije, osnov za zaključivanje o opravdanosti – zakonitosti, primene ovlašćenja u vidu upotrebe srdstava prinude. Osnovna uloga eventualnog video zapisa je mogućnost dokazivanja pojedinačne problemske situacije koja je OSL bila osnov za donošenje odluke o primeni ovlašćenja u vidu upotrebe sredstava prinude.

3. PROBLEMSKE SITUACIJE U OKVIRU ANALIZIRANIH DOGADJANJA

U analiziranim slučajevima, uz korišćenje dostupnih video zapisa[389] moguće je prepoznati više pojedinačnih problemskih situacija.

U slučaja postupanja OSL u SAD, jasno se vidi postojanje problemske situacija pružanja **pasivnog otpora** osobe muškog pola izrazito krupne gradje, crne puti, starosne dobi oko 40 godina, stajanjem naspram OSL na osnovnoj distanci bez predmeta pogodnih za povredjivanje sebe ili drugih lica. Vreme dogadjanja je dan, prostor gradska ulica uz prisustvo manjeg broja drugih gradjana ali i tri druga OSL koja su se nalazila na istoj distanci u odnosu na lice ali na više lokacija. Postojeći video zapis jasno pokriva problemsku situaciju u kojoj gradjanin verbalno negoduje i ne saradjuje na način zakonitog zahtevanja OSL.

U slučaju postupanja OSL u Osjeku, vidi se pojedinačna problemska situacija **aktivnog otpora otimanjem** osobe ženskog pola, starosne dobi oko 60 godina. Vreme dogadjanja je dan, prostor gradska ulica uz prisustvo manjeg broja drugih gradjana. Postojeći video zapis načinjen je kamerom koja se nalazila na delu uniforme OSL. Isti jasno pokazuje ostvaren hvat policijskog službenika za desni rukav kaputa i kretanje blago iza osobe, kao i verbalnu komunikaciju u kojoj OSL izdaje naredjenje osobi da stane, na šta se ista oglušuje i nastavlja kretanje, otimanje i verbalano izražava negodovanje prema postupanju policijskog službenika

U slučaju postupanja OSL u Beogradu, nakon veoma verovatnog značajnog prethodnog dogadjanja, vidi se **udaljavanje**[390] lica, muškog pola, visoko, starosne dobi oko

---

kod službene palice, raspršivača sa nadražujućim sredstvom i elektromagnetnih sredstava, ni problemske situacije samopovredjivanja.

[389] Sva tri video zapisa dostupni su na: youtube.com /prvi – (exclusive footage) Eric Garner Dies After Being Put in Shokehold bx Police; drugi – Croatia: 66-year-old woman brutally arrested for skipping red light; teći – N1 ekskluzivno: snimak intervencije Žandarmerije u kojoj je prebijen Andrej Vučić. 21.02.2016. godine.

[390] U zakonu se navodi pravo na upotrebu sredstava za vezivanje radi sprečavanja bežanja ali ne i fizičke snage, službene palice, elektromagnetnih sredstava... Ovo je jedan od primera nedoslednosti prilikom definisanja zakonskog teksta s obzirom da je za upotrebu sredstava za vezivanje, u uslovima kada lice ne prihvata da bude vezano, neminovono dovodjenje lica u poziciju za vezivanje pa tek nakon kontrole lica pre vezivanja i upotreba istih sredstava (Arlov, 2006a). Autorima nije namera da insistiraju na pravu na upotrebu službene palice ili drugih pomoćnih sredstava u rešavanju problemskih situacija bekstva, već na doslednosti u definisanju prava OSL s obzirom da ista, skoro po pravilu, izostane i kod donošenja odgovrajućih podzakonskih akata.

35 godina, odeveno u farmerke, patike, crni duks sa kapuljačom... kao i prisustvo većeg broja OSL policije, pripadnika žandarmerije u neposrednoj blizini lica prema kome su kasnije upotrebljena sredstva prinude u vidu službenih palica. Na istom video zapisu (vide se još dva lica koja se udaljavaju a za njima kreće nekoliko pripadnika žandarmerije. Jedno od lica ima plastičnu flašu i u jednom momentu istu baca unazad prema OSL[391] a nakon toga i upotreba sredstva prinude u vidu službene palice od strane drugog pripadnika žandarmerije u predelu slabinskog dela kičme, pri čemu lice pada na tlo bez daljeg postupanja OSL.

4. PRINCIPI ZA REŠAVANJE PROBLEMSKIH SITUACIJA

Na putu uspešnog rešavanja problemskih situacija neophodno je posedovanje specifičnih kompetancija OSL a u vidu prepoznavanja konkretne problemske situacije, poznavanja principa, posedovanje i izbor adekvatnih alata (Arlov, 2011). Odluka o započinjanju rešavanja ili ne, odredjene - konkretne problemske situacije je diskreciono pravo OSL ali u isto vreme i odgovornost za svoju procenu, time i za odluku koju donese na osnovu takve procene, ali i za nivo štetnosti eventualno nastalih posledica, primenom, ili ne, ovlašćenja u vidu upotrebe sredstava prinude (Arlov i Janković, 2013). U svemu prethodnom, postojanje kvalitetnog video zapisa može da ima veoma značajnu ulogu u razumevanju dogadjanja koja su prethodila pojedinačnoj problemskoj situaciji kao osnovu za primenu ovlašćenja u vidu upotrebe sredstava prinude (Arlov, 2011).

Principi za rešavanje problemske situacije pasivnog otpora su:

- *od momenta* kada odredjeno lice pruži pasivni otpor (definisanog oblika) a OSL odluči da isti bude osnov za primenu ovlašćenja u vidu upotrebe sredstava prinude, pa *do momenta* kada to lice trpi neophodan osećaj bola, takvog porekla da kod lica neće stvoriti nepotrebne štetne posledice[392], prodje što manje vremena i
- upotrebom istih ili drugih alata, iz prostora fizičke snage, obezbediti kontrolu nad licem i/ili stvoriti uslove za upotrebu sredstava za vezivanje, sa istim ciljem.
- Principi za rešavanje problemske situacije aktivnog otpora otimanjem[393] su:
- *od momenta* kada odredjeno lice pruži aktivni otpor otimanjem (definisanog oblika) a OSL odluči da isti bude osnov za primenu ovlašćenja u vidu upotrebe sredstava prinude, pa *do momenta* kada to lice trpi neophodan osećaj bola, takvog porekla da kod lica neće stvoriti nepotrebne štetne posledice, prodje što manje vremena i

[391] S obzirom na prostor, vreme, opremu... karakteristike predmeta (plastična flaša prazna ili puna!?) tešto je isti definisati kao predmet pogodan za napad i povredjivanje OSL. U naknadnim saznanjima (ne putem video zapisa) pominju se i problemske situacije napada rukom na glavu OSL, hvata za odeću i guranje OSL ali one, iz navedenog razloga, nisu predmet ovog rada.

[392] Opšte i specifične kompetencije OSL, kao ishod kvalitetne edukacije (svih oblika) bi morale biti garant ne nastajanja nepotrebnih štetnih posledica upotrebom sredstava prinude. U isto vreme neopravdano je očekivati mogućnost kvalitetne kontrole nad licem, koje je svojim stanjem ili činjenjem stvorilo uslove postojanja zakonskog osnova za primenu uvlašćenja u vidu upotebe sredstava prinude

[393] Sam oblik postupanja lica – otimanje, ukazuje na postojanje kontakta izmedju njega i OSL, i u isto vreme i na činjenicu da taj kontakt nije obezbedio kontrolu nad ponašanjem lica a iz razloga odsustva neophodno potrebnog osećaja bola kao potrebne štetne posledice i garanta za kontrolu nad licem prema kome se primenjuje ovlašćenje u vidu fizičke snage kao sredstva prinude. I pored prethodnog navodimo principe čije zadovoljenje vodi uspešnom rešenju konkretne – pojedinačne problemske situacije.

- upotrebom istih ili drugih alata, iz prostora fizičke snage, obezbediti kontrolu nad licem i/ili stvoriti uslove za upotrebu sredstava za vezivanje, s istim ciljem.
- Principi za rešavanje problemske situacije bekstva – udaljavanja, su:

- *od momenta* kada odredjeno lice započne bekstvo (definisanog oblika) a OSL odluči da isti bude osnov za primenu ovlašćenja u vidu upotrebe sredstava prinude, pa *do momenta* kada to lice trpi neophodan osećaj bola, takvog porekla da kod lica neće stvoriti nepotrebne štetne posledice, prodje što manje vremena, i
- upotrebom istih ili drugih alata, iz prostora fizičke snage, obezbediti kontrolu nad licem i/ili stvoriti uslove za upotrebu sredstava za vezivanje, sa istim ciljem.
- Kriterijumi za vrednovanje kvaliteta rešenja pojedinačne problemske situacije, a time i mogućnost zaključivanja o pravilnosti upotrebe sredstava prinude, su:

- kvalitet kontrole nad licem prema kome su upotrebljena sredstva prinude i
- nivo štetnosti nastalih posledica upotrebom sredstava prinude.

5. SREDSTVA PRINUDE NA RASPOLAGANJU OVLAŠĆENIM SLUŽBENIM LICIMA POLICIJE

Ovlašćenim službenim licima policije je Zakonom o Policiji R Srbije, stavljen na raspolaganje značajan broj sredstava prinude.[394] U analizi dogadjanja u ovom radu pojavljuju se fizička snaga i službena palica, tako će ona biti i teme tumačenja.

Fizička snaga, kao sredstvo prinude se često tumači kao najblaže, što je diskutabilno, a za utemeljenje valjanog tumačenje potrebna je dobra volja, kompetentnost i argumenti. Upotrebom fizičke snage, prema ZoP se smatra upotreba različitih zahvata borilačkih veština (Arlov, 2003) ili njima sličnih postupaka na telu drugog lica kojima se ono prisiljava na poslušnost a radi odbijanja napada, savladjivanja otpora ili sprečavanja samopovredjivanja.[395] Fizičku snagu, uz tumačenje sredstvima u vidu zahvata, bacanja, udaraca ili drugih veština, je potrebno bliže definisati po osnovu doprinosa stvaranja osećaja bola (kod lica prema kome se upotrebljava) ili osujećenja nastajanja osećaja bola (kod OSL koje ga upotrebljava) kao neophodno potrebne štetne posledice u funkciji kvaliteta kontrole nad licem prilikom rešavanja pojedinačne – konkretne problemske situacije.[396] Kriterijumi za vrednovanje kvaliteta alata iz prostora fizičke snage moraju biti:

- vreme za koje se obezbedi/osujeti nastajanje osećaja bola,

---

[394] Konačno su ZoP predvidjeni i raspršivač sa nadražujućim sredstvima i elektromagnetna sredstva kao sredstva prinude u okviru ukopno 13 predvidjenih. I dalje je redosled od fizičke snage do vatrenog oružja (uz „ubačena“ nova sredstva neposredno nakon fizičke snage) i dalje nedovoljno jasno, krajnjim korisnicima, da li je taj redosled i redosled „težine“ sredstava prinude, s obzirom da se od OSL traži da prilikom upotrebe, upotrebi najblaže sredstvo kojim se može postići zakoniti cilj.

[395] Bilo bi potrebno, za očekivati i logično, da svaki novo doneseni pravni akt bude kvalitetniji od prethodnog. U slučaju novo usvojenog ZoP nema značajnih novina u tumačenju fizičke snage kao sredstva prinude. Ostaje njeno definisanje korišćenjem pojmova *zahvati, borilačke veštine i pravila samoodbrane,* kao i ne predvidjanje prava na njenu upotrebu za rešavanje problemskih situacija bekstva.

[396] prvi koautor ovog rada je izdao naslova *Alati samoodbrane* sa kompakt diskom, sa namerom jasnog definisanja alata samoodbrane kao sredstava prinude (Arlov, 2007) time i mogućnosti korišćenja za potrebe različitih “strana”sa istim ciljem – podizanja kvaliteta primene ovlašćenja, time i kvaliteta odnosa policije i javnosti.

- kvalitet obezbedjenja/osujećenja nastajanja osećaja bola i
- nivo štetnosti nastalih posledica upotrebom alata iz prostora fizičke snage.
- Njihova adekvatnost jedino uz dovodjenje u neposrednu vezu sa pojedinačnom problemskom situacijom koju je ovlašćeno službeno lice policije, u okviru izvršenja službneog zadatka, rešavalo.

Službena palica je sredstvo prinude koje OSL mogu upotrebiti u cilju odbijanja napada ili savladjivanja otpora lica, ako je upotreba fizičke snage bezuspešna ili se ne može postići zakoniti cilj. Pod upotrebom službene palice, u ZoP je definisano zadavanje udaraca ili primena zahvata na telu lica, ali i odredjena ograničenja za zadavanje udaraca u odnosu na karakteristike (uzrasne, polne, zdravstvene...) lica kao i delove tela lica prema kome se zadaju.

Sredstva za vezivanje su pomoćna sredstva, ne i neophodna, u ostvarivanju kontrole nad licem u okviru rešavanja pojedinačne problemske situacije (Arlov, 2006) iz razloga onemogućavanja samopovredjivanja, sprečavanja bekstva, savladavanja otpora i odbijanja napada. Za kvalitetno ostvarivanje prethodnih ciljeva, sredstva za vezivanje samostalno su svakako nedovoljna.

6. SREDSTVA PRINUDE UPOTREBLJENA U ANALIZIRANIM DOGAĐAJIMA

U prvom analiziranom slučaju, OSL u cilju rešavanja definisane pojedinačne problemske situacije – pasivnog otpora, prvi navedeni princip je zadovoljilo upotrebom gušenja podlakticom sa ledja,[397] alata iz prostora fizičke snage, kao jednog od adekvatnih alata, čiji je osnovni cilj stvaranje osećaja bola kao neophodno protrebne štetne posledice, dovoljno brzo i dovoljno kvalitetno kako bi se stvorili uslovi za upotrebu drugih alata u cilju zadovoljenja drugog navedenog principa na putu kvalitetne kontrole. Vreme trajanja upotrebe fizičke snage u vidu alata – gušenja podlakticom sa ledja, i nivo štetnosti nastalih posledica načinom upotrebe sredstva prinude, direktno ukazuju na napravilnost u primeni ovlašćenja u vidu upotrebe sredstava prinude. Izbor alata i način upotrebe, u funkciji zadovoljenja definisanih principa, na putu iznalaženja individualnih – ličnih rešenja, u direktnoj su vezi sa nivoom štetnosti posledica koje nastaju pri rešavanju konkretne problemske situacije. U prostoru edukacije policijskih kadrova, prisutan je model rešavanja problemskih situacija oponašanjem rešenja odredjenog autoriteta (Arlov, 2013).

U drugom analiziranom slučaju, OSL u cilju rešavanja definisane pojedinačne problemske situacije – aktivnog otpora otimanjem, ukupno rešenje ukazuje na nepoznavanje principa neophodnih za uspešno rešavanje ove problemske situacije.[398] Primenjeni postupak u

[397] Navodima u štampi ističe se da je na prostorima države dogadjaja, gušenje od strane OSL zabranjeno još 1993. godine. Veoma je upitna opravdanost ovakvog stava s obzirom da su gušenja ravnopravni alati sa drugima iz grupe fizičke snage. Specifične kompetencije OSL garantuju da će i upotrebom ovih alata nastupiti samo potrebne štetne posledice u vidu neophodno potrebnog osećaja bola. Na našim prostorima je takodje skoro pa uobičajeno "ukidanje" odredjenih prava (gumeni metak, zabrana vezivanja za objekte...) od strane autoriteta (minister, držani sekretar...) bez argumentovanih razloga ali i bez značajnog učešća struke u eventualnoj argumentovanoj "odbrani" prava.

[398] Prethodno se ne bi moglo braniti da nije video zapisa o nastavku postupanja OSL. Doneta odluka da se ne rešava problemska situacija udaljavanja – bekstva, ili udaljavanja u pokušaju, ukazuje na odluku OSL o primeni diskrecionog prava a iz razloga očekivanog odustajanja lica od prethodnog ponašanja time i izostajanja

rešavanju definisane problemske situacije je posledica obuke na način oponašanja vidjenog, ponudjenog ili nametnutog. Upotrebljeni alat iz prostora fizičke snage kao sredstva prinude je neadekvatan s obzirom na lice prema kome je upotrebljen.[399] Način ostvarene kontrole nad licem je tekodje neadekvatan i u delu alata iz grupe fizičke snage i sredstava za vezivanje. Položaj ruke lica prema kome je upotrebljavana prinude, ukazuje na nepoznavanje alata iz grupe poluga na zglobu ramena prekomernim uvrtanjem, tako i posledica nemogućnosti obezbedjivanja druge ruke za namerenu upotrebu sredstava za vezivanje. Upotrebe sredstava za vezivanje, kao pomoćnog sredstva u kontroli lica, u konkretnom dogadjanju, je bila krajnje nepotrebna s obzirom da se značajnim brojem alata iz grupe poluga,[400] kao sredstava prinude, može obezbediti kvalitetna kontrola nad licem, bez nastajanja nepotrebnih štetnih posledica i negativnog uticanja na kvalitet izvršenja službenog zadatka.

U trećem analiziranom slučaju, OSL je, u cilju rešavanja definisane pojedinačne problemske situacije – udaljavanja, upotrebilo službenu palicu na način zadavanja udarca u predelu ledja. Na postojećem video zapisu, vidi se više upotreba istog sredstva prinude od strane više drugih OSL. Kvalitet video zapisa, u delu rešavanja problemske situacije udaljavanja, pokazuje nepravilnu upotrebu službene palice po osnovu lokacije zadavanja udarca ali i ukupne uloge ovog sredstva prinude na putu kvalitetne kontrole nad licem prema kome se upotrebljava. Službena palica je pomoćno sredstvo prinude na putu obezbedjenja kvalitetne kontrole nad licem, nikako osnovno.[401] U analiziranom slučaju, u cilju zadovoljenja navedenih principa za rešavanje problemske situacije bekstva – udaljavanja, nema upotreba sredstava prinude u vidu fizičke snage.

7. DOPRINOS VIDEO ZAPISA SPOZNAJI ISTINE O DOGAĐANJIMA

U sva tri analizirana dogadjanja, postojanje video zapisa, pruža mogućnost za kvalitetniji uvid i zajključivanje o opravdanosti (mogućnost prepoznavanja pojedinačne problemske situacije) i pravilnosti (poznavanje i zadovljenje principa za uspešno rešavanje pojedinačne problemske situacije, i izbor i način upotrebe izabranih alata).

U prvom analiziranom slučaju, vidio zapis pruža mogućnost ukupne kvalitetne spoznaje dogadjanja i ukazuje na problemsku situaciju nepostupanja lica po zakonitim naredjenjima OSL – pasivnog otpora stajanjem, uvid u započinjanje rešavanja iste problemske situacije, izbor alata iz prostora fizičke snage, način njegove upotrebe i način ostvarenja kontrole nad licem. Svakako, vidi se i nivo štetnosti nastalih posledica primenom ovlašćenja u vidu

eventualnih nepotrebnih štetnih posledica primene ovlašćenja u vidu upotrebe sredstava prinude. Medjutim, pokazalo se da je procena OSL bila pogrešna i prethodno propuštanje rešavanja konkretne problemske situacije, udaljavanja, stvorilo je mogućnosti nastajanja novih, sada težih (Arlov, 2010) problemskih situacija, aktivnog otpora, napada...

[399] Konkretan alat, hvat za ruku i pritisak drugom u predelu ramena i obaranje na tlo, je uobičajeno postupanje nametnuto obukom. Ovakav alat, po kriterijumu stvaranja osećaja bola, je obična zabluda. Istim nije moguće obezbediti osećaj bola kod lica prema kome se upotrebljava a time i primorati ga da legne na tlo, ukoliko lice nije toliko nemoćno ili "dobro" da samo legne (tada i pitanje, čemu onda obaranje na tlo!?).

[400] Svi alati iz grupe poluga na zglobovima šaka i prstiju, bez potrebe obaranja na tlo (a posebno osobe ženskog pola značajne starosne dobi), pružaju mogućnost kvalitetne kontrole lica Potrebno je "samo" poznavati takve alate a ono proističe iz adekvatne, realne obuke policijskih službenika.

[401] Iako je moguće kontrolu obezbediti prisustvom OSL i pretnjom na ponovnu upotrebu službene palice, ipak takva kontrola pruža mogućnost licu za započinjanje samopovredjivanja, bežanja, otpora ili napada.

upotrebe sredstava prinude. Iako je snimak, delo amatera, isti pruža dovoljne i kvalitetne informacije za zaključivanje o opravdanosti i pravilnosti a na način da je ovlašćenje primenjeno opravdano ali nepravilno.

I pored potpunog uvida u dogadjanje i primenu ovlašćenja u vidu upotrebe sredstava prinude, putem video zapisa, „država“ je, stavom 12 gradjana sa čistim dosijeom presudila da nema razloga za optužnicu protiv policajaca koji su po njima delovali u skladu sa zakonom, što će reći, opravdano i pravilno. Ishod presude izazvao je nemire velikih razmera na više lokacija SAD.[402]

Simptomatična je „sudbina“ autora video zapisa s obzirom da je istom naknadno podneta krivična prijava za posedovanje vatrenog oružja.

U drugom analiziranom slučaju, video zapis pruža značajno kvalitetne informacije o dogadjanju, iako se iz istog ne vidi osnov za donošenje odluke o započinjanju komunikacije OSL sa licem (prelazak puta u vreme dok je na semaforu crveno svetlo, pokušaj provere identiteta...). Policijski službenik, službenu kameru na svojoj opremi je, uz upozorenje i obaveštenje prema licu, uključio nakon što isto nije postupilo po zakonitom upozorenju o nedozvoljenoj radnji i pokušaju spoznaje identiteta. Video zapis dokumentuje kretanje OSL za licem i izdavanje naredjenja o zaustavljanju, a nakon toga i upotrebu sredstva prinude u vidu hvata za desni ruku/rukav lica/kaputa. Kretanje se nastavlja oblikom postupanja lica definisanog kao bekstvo-udaljavanje i aktivni otpor otimanjem. Prethodno stanje/dogadjanje traje neopravdano dugo[403] a okončava se upotrebom fizičke snage OSL u vidu hvata za ruku, pritiska u predelu ramena i obaranjem lica na betonsku podlogu prolaza u ulici. Kontrolu lica, OSL je delimično ostvarilo pritiskom na tela i namerom vezivanja. S obzirom da je vezao desnu ruku, bila mu je potrebna i leva koja se nalazila ispod tela lica i nije bila dostupna. Pokušaji izvlačenja ruke bili su značajno vreme neuspešni. Uz pomoć drugog OSL (s obzirom da je OSL tražilo pomoć putem radio veze) koje je pristiglo, lice je vezano i uz kontrolu dva OSL podignuto sa tla i ukrcano u službeno vozilo. Iz postojećeg video zapisa, moguće je ostvariti uvid u verbalnu komunikaciju s obzirom da ga prati i adekvatan tonski zapis.

Nakon analize opisanog dogadjaja, načelnik policijske uprave je upotrebu sredstava prinude ocenio opravdanom i zakonitom.[404]

U trećem analiziranom slučaju, video zapis pruža značajno kvalitetne informacije o konkretnoj upotrebi službene palice. Poreklo analiziranog video zapisa je privatna TV N1. Iz zapisa, načinjenog sa udaljenosti 7-8m, moguće je primetiti jedno lice muškog pola, visoko, u

---

[402] Na prostorima SAD, Los Angeles, tragičan je primer slučaja Rodni Kinga od 03. marta 1991. kada su četiri policajca oslobodjena od strane porote po svim tačkam osim jedn po kojoj se nisu mogli složiti, nakon što su upotrebili nesrazmernu silu a iz razloga kršenje ograničenja brzine vožnje i ne pokazane spremnost na saradnju. Dogadjaj je snimljen kućnom kamerom, a gradjani su smatrali da je vido zapis dovoljan dokaz i da je donešena presudu nepravedna. Eskaliralo nasilje, poginulo je više od 50 osoba, i nastala ogromna materijalna šteta. King je tužio grad Los Angeles i dobio odštetu od 3,6 miliona američkih dolara. Šteta po kvalitet odnosa, policije i javnosti!? Može se naslutiti.

[403] ili po odluci OSL dovoljno dugo u smislu pretpostavljanja promene ponašanja lica u vidu saradnje sa OSL. U isto vreme, trajanje se može tumačiti i kao posledica neadekvatne odluke OSL o odlaganju primene ovlašćenja u vidu upotrebe sredstava prinude sa ciljem rešenja konkretne problemske situacije.

[404] Iz informacija dostupnih autorima ovog rada nema stava službe o pravilnosti upotrebe sredstava prinude.

farmerkama, patikama i crnim duksom sa kapuljačom[405] koga 5-6 žandara potiskuje, a jedan udara palicom nakon čega je ovo lice selo na trotoar. Kontrola je ostvarivana prisustvom žandara ali ne i upotrebom sredstava prinude u vidu fizičke snage. U blizini su bila još dva lica a jedno od njih je imalo plastičnu flašu od vode, koju je jednog momenta bacilo unazad u pravcu OSL, žandara. Drugi žandar u uniformi, upotrebio je službenu palicu prema ovom licu a na način zadavanja udarca u predelu ledja.[406] Lice se uhvatilo svojom levom rukom za donji deo ledja, mesto udarca, i uz bolan izraz palo na zemlju. Isto lice je uz pomoć drugog lica u gradjanskoj odeći podignuto i povedeno. Kvalitet video zapisa ne daje potpun uvid u kretanje lica kao i u druga dešavanja s obzirom da se ponekad nepotrebno menja položaj kamere kao i povremeno gubi tonski zapis. Postojeći video zapis ukazuje i na druga dešavanja koja nisu predmet ovoga rada.[407]

Ukupan dogadjaj je dobio visok publicitet i povodom istog su se, putem medija, izjašnjavali mnogi.[408] Ishod po učesnike u dogadjanju definisan je krivičnom prijavom prema osam postupajućih žandara, Odreda iz Niša, a za zloupotrebu službenog položaja i napada na vojno lice u vršenju službe.[409]

Analiza slučajeva[410]

prostor	**SAD**	**R HRVATSKA**	**R SRBIJA**
lokacija	*Njujork*	*Osijek*	*Beograd*
Vreme	*17. 7. 2014.*	*16. 12. 2015.*	*28. 9. 2014.*
postojanje video zapisa	*DA*	*DA*	*DA*
poreklo video zapisa	*amaterski snimak*	*snimak OSL*	*privatna TV i službeni snimci*
kvalitet video zapisa	*potpun uvid u dogadjanje*	*nepotpun uvid u dogadjanje*	*nepotpun uvid u dogadjanje*
obavljani poslovi	*suzbijanje kriminaliteta*	*bezbednost saobraćaja*	*obezbedjenje javnog skupa*
službeni zadatak	*lišenje slobode lica sumnja u izvršeno KD*	*poštovanja saobraćajne signalizacije...*	*zaprečavanje prolaska lica u odredjeni prostor*
opšta problemska situacija	*otpor*	*otpor*	*napad, bekstvo,*

[405] Najverovatnije Predrag Mali, lice koje je bilo u društvu sa Andrejom Vučićem, licem prema kome je kasnije žandar upotrebio službenu palicu.
[406] Radi se o licu, Andreju Vučiću, rodjenom bratu premijera R Srbije.
[407] Svakako da je postojanje drugih video zapisa (prisutno ali i najavljeno), bez obzira na autora, veoma bitno u funkciji spoznaje jedine istine o dogadjanju a time i mogućnosti kvaliteta dokazivanja opravdanosti i pravilnosti primene ovlašćenja pa i u vidu upotrebe sredstava prinude.
[408] Od običnih gradjana do ministra unutrašnjih poslova i direktora policije koji su postupanje odmah ocenili kao brutalni napadi policije ali i predsednika Vlade na konferenciji za štampu. Simptomatično je postupanje predsednika Vlade koji je odmah po dogadjaju pozvao "aktere" dogadjanja kao i starešine policije na razgovor u svoj kabinet u Vladi R Srbije i sa njima obavio razgovor!?
[409] Sudski postupak, koji se vodi pred Višim sudom u Beogradu, još nije završen, a u medjuvremenu je više puta odlagan kao i 02. februara a za nastavak 04. marta za kada je predvidjeno svedočenje TV ekipe N1.
[410] Mogući i verovatan, nedostatak obima i kvaliteta informacija u vezi sva tri analizirana dogadjanja ne utiče na kvalitet njihove analize od strane autora ovog rada a po osnovu opravdanosti i pravilnosti primene ovlašćenja u vidu upotrebe sredstava prinude.

posebna problemska situacija	*pasivni otpor stajanjem ledjima ka OSL*	*aktivni otpor otimanjem*	*udaljavanje hodom*
pojedinčana problemska situacija	*osoba muškog pola, starosti oko 40god, izrazito krupne konstitucije...*	*osoba ženskog pola, starosne dobi ko 60god, bez predmeta pogodnih za povredjivanje...*	*osoba muškog pola, starosne dobi oko 35 godina, u gradjanskom odelu, farmerkama...*
diskreciono pravo[411]	*NE*	*NE*	*NE*
principi	*delimično*	*ne*	*ne*
alati adekvatni	*DA*	*NE*	*NE*
kontrola nad licem	*DA*	*DA*	*DA*
nivo štetnosti nastalih posledica	*smrtne posledice*	*bez telesnih povreda*	*lake telesne povrede...*
opravdanost primene ovlašćenja	***DA***	***DA***	***DA***
pravilnost upotrebe sredstava	***NE***	***NE***	***NE***
stav policije	*zakonito*	*opravdano i zakonito*	*direktor- brutalni napad*
doprinost odnosu policija - javnost	***negativno***	***negativno***	***negativno***
posledice po izvor video zapisa	*krivično gonjenje za posedovanje oružja*	–	*nema - nije završeno sudjenje*

8. ZAKLJUČAK

Upotreba sredstava prinude, od strane ovlašćenih službenih lica, predstavlja izuzetnu mogućnost za jačanje poverenja javnosti u rad policije, ali u isto vreme, i mogućnost njegovog narušavanja. Profesionalizam, u radu policije, je uslov za jačanje tog poverenja. U isto vreme, neprofesionalan odnos, u vidu neopravdane i/ili nepravilne upotrebe sredstava prinude, direktno i sa značajnim odjekom u javnosti, utiče na ukupno poverenje gradjana u rad policije. U izgradnji ili narušavanju medjusobnog poverenja, izuzetnu ulogu imaju mediji.

Policija, mediji, ali i gradjani pojedinačno, angažovanjem postojećih tehnologija, mogu značajno uticati na kvalitet dokazivanja pojedinačnih problemskih situacija kao zakonskog osnova za upotrebu sredstava prinude, time i na kvalitet postupka utvrdjivanja opravdanosti i pravilnosti primene ovlašćenja.

Video zapis odredjenog dogadjaja, a posebno povodom primene ovlašćenja u vidu upotrebe sredstava prinude OSL, bez obzira na njegovo poreklo, umnogome olakšava postupak utvrdjivanja opravdanosti i pravilnosti na putu spoznaje jedine istine.

Kvalitet video zapisa ogleda se u mogućnosti analize dogadjaja u svojoj ukupnosti od prilike za jasnu spoznaju problemskih situacija, kao osnova za donošenje odluke o primeni

[411] Prostor od suštinske važnosti i za primenu ovlašćenja u vidu upotrebe sredstava prinude, zavredjuje mnogo više od jednog pominjanja u analizi dogadjanja. No s obzirom da su OSL policije, zahvaljujući svojim procenama doneli odluku da iskoriste postojanje zakonskog osnova i upotrebe sredstva prinude, autori su u ovom radu "preskočili" analizu razloga za i protiv korišćenja diskrecionog prava u analiziranim dogadjanjima.

ovlašćenja, pa do načina ostvarivanja kontrole nad lice/licima prema kojima je primenjeno ovlašćenje.

Programi obrazovanja i obuke OSL, uz uvažavanje dobre prakse medjunarodnih snaga, moraju biti značajnije obogaćeni primerima iz stvarnih životnih dogadjanja, karakterističnih slučajeva primene ovlašćenja u vidu upotrebe sredstava prinude, koji su pokriveni kvalitetnom analizom postojećih video zapisa.

Policije bi morala biti aktivnija na polju edukacije javnosti a povodom razumevanja uloge policije (poslovi, ovlašćenja, kontrola...) i drugih subjekata društva, u ostvarivanja visokog nivoa ukupne bezbednosti.

Dosledno poštovanje, pravnim aktima definisanih obaveza, pripadnika policije svih nivoa, predstavnik vlasti, medija, kao i drugih gradjana, obezbedilo bi ostvarivanje prava svih navedenih, a tim i značajno umanjilo mogućnosti nastajanja nemilih dogadjanja kakva su bila predmet ovoga rada.

LITERATURA

Arlov, D. (2003). Fizička snaga kao sredstvo prinude u zaštiti bezbednosti pripadnika policije. Zbornik radova/Međunarodno naučno-stručno savetovanje: Ugrožavanje bezbednosti pripadnika policije – uzroci, oblici i mere zaštite. Beograd: Policijska akademija, str. 223.

Arlov, D. (2006). Upotreba sredstava prinude-sredstva za vezivanje. *Bezbednost*, god. 48, br. 4, str. 633-646.

Arlov, D. (2007). *Alati samoodbrane.* SIA: Novi Sad.

Arlov, D. (2008). *Upotreba sredstava prinude u funkciji lišenja slobode lica zatečenog u izvršenju krivičnog dela*. Zbornik radova „Primjena savremenih metoda i sredstava u suzbijanju kriminaliteta“, str. 461-469. Brčko: Internacionalna asocijacija kriminalista.

Arlov, D. (2009). Kvalitet upotrebe i izveštavanja o upotrebi sredstava prinude u funkciji unapredjenja policijskih poslova bezbednosti saobraćaja. *Bezbednost*, god. 51, br.1-2, str. 275-284.

Arlov, D. (2010). *Aktivni otpor učesnika u saobraćaju kao osnov za primenu policijskih ovlašćenja.* Zbornik radova – 9. stručni skup – Unapredjenje policijskih poslova bezbednosti saobraćaja, Vrnjačka Banja.

Arlov, D. (2011). *Competences of police officers as a positive outcome of quality education*, Thematic proceedings of international significance Archibald Reiss Days, Volume I, 77-88, Academy of criminalistic and police studies, Belgrade.

Arlov, D.; Janković, R. (2013). *Veštačenje primene ovlašćenja u vidu upotrebe sredstava prinude kao neophodnost u spoznaji istine*. Zbornik radova „Nove sigurnosne ugroze i kritična nacionalna infrastruktura“, 3. međunarodna znanstveno-stručna konferencija Istraživački dani Visoke policijske škole RH, str. 15-26., Zagreb.

Roberg, R., Crank, J., Kuykendall, J. (2004). *Policija i društvo*. Sarajevo: Office of Public Affairs of the United States of America.

Žaberl, M., Arlov, D. (2007). Nezakonita upotreba sredstava prinude i dužnost Države, da uspešno istraži eventualna nezakonita zadiranja u ljudska prava, Science-Security-Police. *Journal of Police Academy,* god 11, broj 3, str. 65-80.

Dragan Arlov

Milan Popović

QUALITY DETERMINING THE ELIGIBILITY AND REGULARITY OF THE USE OF FORCE TO STRENGTHEN RELATIONS BETWEEN THE POLICE AND OTHER CITIZENS

Summary

The use of coercive measures by the authorized officials, represents a tremendous opportunity to strengthen public confidence in the police, but at the same time, the possibility of its distortion. Professionalism in policing, is a condition for strengthening that trust. At the same time, unprofessional behavior, in the form of unjustified andor incorrect use of force directly and with significant echo in the public, affect the confidence of citizens in the work of the police. In building or distortion of mutual trust, the exceptional role, have the media. The police, the media, as well as individual citizens, engaging existing technology, can significantly affect the quality of proving individual problem situations as the legal basis for the use of force, thus the quality of the process of determining the justification and correctness of the application of powers. The work on the three use of force, police officers, covered with videos, by different authors, in different areas (USA, Croatia, Serbia) as a case study, analyzes the contribution of video records establishing the truth. Specific managerial competencies of police officers, in the form of knowledge in the creation of a causal link between the individual problem situations, use discretion, knowledge of principles in dealing with problem situations, select and use tools and individual criteria in the evaluation of the quality of execution of official duty, are very important for the knowledge of the truth of events. Nothing less importance in enhancing mutual trust, have also timely, adequate and competent communication to the public, establishing the truth.

Key words*: video recording, coercion, problem situations, legality, regularity.*

PRETHODNO PRIOPĆENJE

Željko Mršić[1]

ULOGA NOVIH TEHNOLOGIJA I METODA U PREVENCIJI KAZNENIH DJELA POLICIJSKIH SLUŽBENIKA

Sažetak

U radu su prezentirani rezultati istraživanja kaznenih djela počinjenih od strane policijskih službenika tijekom desetogodišnjeg razdoblja, te je napravljena usporedba s kaznenim djelima počinjenim od ostatka građanske populacije. Rultati istraživanja ukazuju da su policijski službenici ipak, višestruko manje kriminalno aktivni, tj. „pošteniji" su od ostatka građanske populacije. Razmotrena je nova tehnologija koja se uvodi u rad policijskih službenika, te su u tom smislu identificirane tri tehničke mjere koje imaju određeni antikorupcijski, tj. antidelinkvencijski potencijal. Te mjere su: geografsko pozicioniranje policijskih službenika na terenu, uvođenje prijenosnog računala umjesto „papirnate" opreme te pokretne kamere koje policijski službenici nose na sebi. Prve dvije mjere su ocijenjene značajnim iskorakom, dok se kod treće mjere (kamera), otvaraju brojna sporna pitanja.

Ključne riječi: *geografsko pozicioniranje, kamere, prijenosno računalo, policijska delinkvencija, prevencija*

1. UVOD

Zločini, tj. kaznena djela i drugi sadržaji „crne kronike" oduvijek zaokupljaju ljudsku pažnju, a ako se u ulozi počinitelja nađu oni koji bi trebali takve pojave sprečavati i sankcionirati, interes javnosti se umnogostruči. Nesumnjiva je činjenica da se kaznenim djelima počinjenim od strane policijskih službenika uvijek pridavao poseban značaj i gledalo ih se pod posebnim svjetlom, ali je pitanje jesu li se, i u kojoj mjeri sagledavali svi aspekti te, po mnogočemu specifične delinkvencije. Cilj ovog rada je da se baci novo svjetlo na tu pojavu, a moglo bi se reći da su se stekli povoljni uvjeti da se istraži u Republici Hrvatskoj, što znači da se za dovoljno dugo razdoblje ta problematika metodološki istovjetno pratila, a da istovremeno nije bilo ključnih promjena u Kaznenom zakonu, da bi rezultati istraživanja jamčili relevantnost. Razdoblje o kojem je riječ odnosi se na period od 2002. do 2011., a podloga su podaci dobiveni od Odjela (Službe) za unutarnju kontrolu Ministarstva unutarnjih poslova. Nakon toga će se podaci i analize policijske delinkvencije usporediti s delinkvencijom ostatka populacije, tj. kaznenih djela počinjenih od strane ostalih građana, ujednačit će se skupovi te će se testirati statistička značajnost razlika iz koje će se vidjeti jesu li, u konačnici, policijski službenici uopće „pošteniji" od ostatka populacije i je li razlika statistički značajna. Nesumnjivo će i nakon takvog presjeka kroz taj oblik delinkvencije ostati neosvijetljeni neki aspekti pojave, ali ćemo svakako biti barem korak bliže razumijevanju, a time i realnoj osnovi za njeno preveniranje. Posebno će se analizirati nove tehnologije koje se uvode u postupanje policije i njihova uloga i potencijal za prevencije te specifične delinkvencije.

2. FENOMENOLOGIJA POLICIJSKE DELINKVENCIJE

Što se fenomenologije policijske delinkvencije tiče, valja naglasiti da se policijski službenik može naći u ulozi počinitelja bilo kojeg općeg kaznenog djela, no za neka djela, tzv. *delicta propria,* odnosno posebna kaznena djela, su svojstvo službene osobe, u našem slučaju policijskog službenika, posebno istaknuta u biću kaznenog djela. Kod tih djela razlikujemo prava i neprava posebna kaznena djela. Kod pravih posebnih kaznenih djela svojstvo počinitelja utječe na samo postojanje kaznenog djela, dok neprava posebna kaznena djela može počiniti svatko, ali djelo postaje kvalificirano ako ga počini službena osoba u obavljanju službe ili javne ovlasti.[412]

U tablici 1 dat će se cjeloviti prikaz svih pravih i nepravih posebnih kaznenih djela koje, kao takve, može počiniti policijski službenik.

Tablica 6: Prikaz prijavljenih/evidentiranih posebnih kaznenih djela počinjenih od strane policijskih službenika u RH u periodu od 2002. do 2011. godine[413]

Red br./god.	Kazneno djelo	2002.	2003.	2004.	2005.	2006.	2007.	2008.	2009.	2010.	2011.	Uku Ukupno
1.	Povreda prava na podn. pravn. lijekova i predst.	0	0	0	0	0	0	0	0	0	0	0
2.	Protuzakonita pretraga	0	0	0	0	0	0	0	0	0	0	0
3.	Iznuđivanje iskaza	0	0	2	1	0	2	0	0	2	0	7
4.	Zlostavljanje u obavljanju službe	5	3	3	5	2	7	3	3	4	2	37
5.	Mučenje i dr. okrutno neljuds. ili poniž. post.	0	0	0	0	0	0	0	0	0	0	0
6.	Krivotvorenje službene isprave	0	1	0	0	0	0	0	0	0	0	1
7.	Zlouporaba položaja i ovlasti	26	28	26	13	24	17	26	84	23	35	302
8.	Nesvjestan rad u službi	3	6	1	3	1	1	5	0	1	0	21
9.	Neizvršavanje zapovijedi	0	0	0	0	0	0	0	0	0	0	0
10.	Povreda čuvanja državne granice	0	0	0	0	0	0	0	0	0	0	0
11.	Protuz. oslobođ. osob. kojoj je oduz. sloboda	0	0	0	0	0	0	0	0	0	0	0
12.	Prijevara u službi	0	0	3	0	2	0	0	1	2	5	13
13.	Primanje mita	6	8	5	6	8	3	13	3	4	18	74
14.	Protuz. prisv. stvari prilikom pretr. ili pregl.	1	0	1	1	0	0	0	0	0	0	3

[412] Horvatić, Ž., Novoselec, P.: Kazneno pravo, opći dio, MUP RH, Zagreb, 1999., 176.

[413] Podaci se temelje na godišnjim izvješćima Odjela za unutarnju kontrolu Ministarstva unutarnjih poslova i odnose se na prijavljena/evidentirana kaznena djela s poznatim počiniteljem. Pod ovom formulacijom misli se na osnovanu sumnju da je počinjeno kazneno djelo. Na žalost, zbog različitih sudbenih nadležnosti, dugotrajnosti postupaka koji su u opreci s kratkotrajnošću praćenja ove problematike u MUP-u, ne praćenju kriminaliteta po zanimanju, odnosno svojstvu osobe od strane Statističkog zavoda (samo punoljetni-maloljetni i muško-ženski počinitelji) i drugih objektivnih razloga nije bilo moguće pratiti tijek postupaka i presuda od strane sudova, odnosno, nije nam poznato kako su postupci okončani i koji je njihov krajnji rezultat.

Red br./god.	Kazneno djelo	2002.	2003.	2004.	2005.	2006.	2007.	2008.	2009.	2010.	2011.	Uku Ukupno
15.	Protuzakonita naplata i isplata	0	0	0	0	0	1	0	0	0	0	1
16.	Narušavanje nepovredivosti doma	1	0	0	0	0	0	0	0	1	0	2
17.	Protuzakonito oduzimanje slobode	1	1	0	1	2	0	2	1	1	0	9
18.	Povreda tajnosti pisama i dr. pošiljaka	0	0	0	0	0	0	0	0	0	0	0
19.	Neovlašteno snimanje i prisluškivanje	0	0	0	0	0	0	0	0	0	0	0
20.	Dovođenje u opasnost općeop. radnj. ili sred.	3	5	0	3	3	3	2	0	4	1	24
21.	Neprijavljivanje počinjenja kaznenog d.	1	0	0	1	0	0	0	0	0	1	3
Ukupno		**47**	**52**	**41**	**34**	**42**	**34**	**51**	**92**	**42**	**62**	**497**

Budući je u tablici 1 dan prikaz pravih i nepravih[414] posebnih kaznenih djela (*delicta propria*) za čije je biće djela svojstvo službene osobe (policijskog službenika), nužni preduvjet, odnosno predstavlja teži oblik osnovnog djela, donekle (ugodno) iznenađuje podatak da u nekim kaznenim djelima u promatranom razdoblju policijski službenici uopće nisu participirali. Tako je razvidno da nije evidentirano ni jedno kazneno djelo povrede prava na podnošenje pravnih lijekova i predstavki, protuzakonite pretrage, nezakonitog snimanja i prisluškivanja, mučenja i drugog okrutnog, neljudskog ili ponižavajućeg postupanja, te nekih drugih kaznenih djela čije bi se počinjenje, zbog prirode posla, gotovo moglo očekivati od policijskih službenika. Evidentno je da su najzastupljenija kaznena djela zlouporaba položaja i ovlasti, primanje mita, zlostavljanje u obavljanju službe, te dovođenje u opasnost općeopasnom radnjom ili sredstvom. Brojčano najzastupljenije kazneno djelo, zlouporaba položaja i ovlasti, osim u situacijama kad je jasno razvidna sumnja da je riječ upravo o tom kaznenom djelu, treba promatrati i u kontekstu mogućnosti da je riječ o supsidijarnom kaznenom djelu, u situacijama kad kriminalističkim istraživanjem nije bilo moguće utvrditi i dostatno potkrijepiti specifična obilježja nekog drugog kaznenog djela, kao npr. primanja mita i sl.

[414] U tablici prava posebna kaznena djela se nalaze u prvome dijelu od broja 1 do 15, a neprava posebna kaznena djela od broja 16 do 21, odvojeni trima crtama.

Tablica 7: prikaz prijavljenih/evidentiranih općih kaznenih djela počinjenih od strane policijskih službenika u rh u periodu od 2002. Do 2011. Godine[415]

Red br./god.	Kazneno djelo	2002.	2003.	2004.	2005.	2006.	2007.	2008.	2009.	2010.	2011.	Uku Ukupno
Opća kaznena djela kod kojih svojstvo policijskog službenika ima poseban značaj												
1.	Ubojstvo	0	1	0	0	0	0	0	0	1	0	**2**
2.	Teško ubojstvo	0	1	0	0	0	0	0	0	0	0	**1**
3.	Prouzročenje smrti iz nehaja	0	0	0	0	0	0	0	0	0	0	**0**
4.	Tjelesna ozljeda	0	0	0	0	0	1	3	0	0	0	**4**
5.	Teška tjelesna ozljeda	5	5	1	2	3	6	2	3	4	0	**31**
6.	Tjelesna ozljeda na mah	0	0	0	0	0	0	0	0	0	0	**0**
7.	Tjelesna ozljeda iz nehaja	0	0	0	0	0	0	0	0	0	0	**0**
8.	Povreda ravnopravnosti građana	0	0	0	0	0	0	0	0	0	0	**0**
9.	Povreda prava na okupljanje i javni prosvjed	0	0	0	0	0	0	0	0	0	0	**0**
10.	Nedozvoljena uporaba osobnih podataka	0	0	0	0	0	0	0	0	0	0	**0**
11.	Odavanje državne tajne	0	0	0	0	0	0	0	0	0	0	**0**
12.	Rasna i druga diskriminacija	0	0	0	0	0	0	0	0	0	0	**0**
13.	Spolni odnošaj zlouporabom položaja	0	0	0	0	0	0	0	0	0	1	**1**
14.	Lažno prijavljivanje kaznenog djela	0	2	0	0	0	1	0	0	1	0	**4**
15.	Otkrivanje identiteta zaštićenog svjedoka	0	0	0	0	0	0	0	0	0	0	**0**
16.	Odavanje službene tajne	1	2	2	2	4	4	13	6	12	2	**48**
Ukupno		**6**	**11**	**3**	**4**	**7**	**12**	**18**	**9**	**18**	**3**	**91**
Ostala opća kaznena djela												
17.	Protuzakonito posredovanje	1	0	0	0	0	0	0	0	0	2	**3**
18.	Pronevjera	5	9	3	2	2	4	2	1	5	4	**37**
19.	Otmica	0	0	0	0	0	1	0	0	0	0	**1**
20.	Neovlaštena uporaba	5	2	0	0	3	0	0	0	1	1	**12**
21.	Krivotvorenja[416]	24	30	19	7	18	10	9	67	24	12	**220**
22.	Krivotvorenje novca	0	0	0	0	0	0	0	0	0	1	**1**
23.	Prijetnja	13	12	7	12	12	7	9	7	7	3	**89**
24.	Ratni zločin protiv civilnog pučanstva	2	0	0	0	0	1	0	0	0	0	**3**
25.	Zlouporaba opojnih droga	5	4	9	1	1	1	1	4	1	1	**28**

[415] Podaci bazirani na godišnjim izvješćima Odjela za unutarnju kontrolu Ministarstva unutarnjih poslova i odnose se na prijavljena/evidentirana kaznena djela s poznatim počiniteljem.

[416] U izvješćima se koristi zajednički stavak za krivotvorenja isprava, kao i za posebne slučajeve krivotvorenja isprava iz čl. 311. i čl. 313. KZ RH.

Red br./god.	Kazneno djelo	2002.	2003.	2004.	2005.	2006.	2007.	2008.	2009.	2010.	2011.	Uku Ukupno
26.	Protuzakonito prebaciv. osoba preko granice	0	0	0	0	0	0	0	1	1	0	**2**
27.	Međunarodna prostitucija	0	0	1	0	0	0	0	0	0	0	**1**
28.	Bludne radnje	0	0	2	0	1	1	0	0	0	0	**4**
29.	Silovanje	1	5	0	1	2	0	0	0	0	1	**10**
30.	Prisila na spolni odnošaj	0	0	0	0	1	0	0	0	0	0	**1**
31.	Spolni odnošaj s djetetom	0	0	0	0	0	0	1	0	0	0	**1**
32.	Upoznavanje djece s pornografijom	0	0	0	0	0	0	2	0	0	1	**3**
33.	Iskorištavanje djece ili maloljetn. osoba za pornografiju	0	0	0	0	0	0	0	0	0	1	**1**
34.	Dječja pornografija na račun. sustavu ili mreži	0	0	0	0	1	0	0	0	0	0	**1**
35.	Povreda dužnosti uzdržavanja	0	0	0	0	2	1	0	0	1	0	**4**
36.	Podvođenje	1	0	0	0	0	0	0	0	0	1	**2**
37.	Zapuštanje i zlostavlj. djeteta ili malolj. osobe	5	7	3	5	14	6	8	4	11	1	**64**
38.	Nasilničko ponašanje u obitelji	0	8	0	12	0	0	0	0	0	6	**26**
39.	Sprječavanje i neizvrš. mjera za zaštitu djece i maloljetne osobe	4	0	7	0	8	8	8	5	4	0	**44**
40.	Krađa	2	2	2	3	5	4	1	1	0	3	**23**
41.	Teška krađa	3	24	3	6	4	1	1	1	0	0	**43**
42.	Oduzimanje tuđe pokretne stvari	0	0	0	0	0	0	0	1	0	0	**1**
43.	Razbojništvo	2	2	8	0	0	1	0	0	4	0	**17**
44.	Uništavanje ili oštećenje tuđe stvari	0	4	0	2	1	1	0	2	1	1	**12**
45.	Utaja	0	0	1	0	0	0	0	0	1	0	**2**
46.	Prijevara	14	12	5	5	1	3	5	0	8	12	**65**
47.	Zlouporaba čeka i kreditne kartice	0	2	2	0	0	0	0	0	1	0	**5**
48.	Zlouporaba osiguranja	0	0	0	0	0	0	0	0	1	0	**1**
49.	Iznuda	0	0	1	1	0	0	0	1	0	0	**3**
50.	Ucjena	0	1	0	0	0	0	0	0	0	0	**1**
51.	Prikrivanje	0	1	2	0	1	0	0	2	0	0	**6**
52.	Protuzakoniti lov	1	2	0	0	0	1	0	0	0	0	**4**
53.	Protuzakoniti ribolov	0	0	1	0	0	0	1	0	0	0	**2**
54.	Teška k. d. protiv opće sigurnosti	2	0	0	0	0	1	0	0	1	1	**5**
55.	Izazivanje prometne nesreće	23	11	11	13	7	8	12	13	11	8	**117**

Red br./god.	Kazneno djelo	2002.	2003.	2004.	2005.	2006.	2007.	2008.	2009.	2010.	2011.	Uku Ukupno
56.	Nepružanje pomoći osobi teško ozlijeđenoj u p.n.	0	0	0	0	0	0	0	0	1	1	**2**
57.	Izigravanje zabr. iz sig. mjera i pr. poslj. osude	0	0	0	0	0	0	0	1	0	1	**2**
58.	Utaja poreza i dr. davanja	0	1	0	0	0	0	0	0	0	0	**1**
59.	Zlouporaba ovlasti u gospodars. poslovanju	0	2	0	0	0	0	0	0	0	0	**2**
60.	Nedozvoljena trgovina	3	2	0	0	0	1	0	0	0	0	**6**
61.	Izbjegavanje carinskog nadzora	2	3	3	1	3	1	0	0	1	0	**14**
62.	Davanje lažnog iskaza	1	0	2	0	0	0	1	0	0	0	**4**
63.	Sprječavanje dokazivanja	1	0	0	0	1	0	0	0	0	0	**2**
64.	Oduzimanje ili uništenj služb. pečata ili spisa	0	0	0	0	1	0	0	0	0	0	**1**
65.	Ovjerovljavanje neistinitog sadržaja	7	0	2	1	0	0	0	0	2	1	**13**
66.	Sprječavanje sl. osobe u obavljanju sl. dužn.	1	1	0	2	0	1	0	0	0	0	**5**
67.	Napad na službenu osobu	0	2	1	0	0	0	1	0	0	1	**5**
68.	Lažno predstavljanje	0	0	0	1	0	0	0	0	0	0	**1**
69.	Skidanje i povreda služb. pečata i znaka	1	0	0	0	0	0	0	0	0	0	**1**
70.	Protupravna naplata	0	0	0	0	0	0	0	1	0	0	**1**
71.	Nasilničko ponašanje	1	4	0	0	2	1	0	4	0	0	**12**
72.	Dogovor za počinjenje k. djela	0	0	0	0	0	0	0	0	0	1	**1**
73.	Udruživanje za počinjenje k. djela	0	1	0	1	0	0	1	0	0	0	**3**
74.	Nedozvoljeno držanje oružja i eksploz. tvari	3	6	0	2	1	7	6	5	5	1	**36**
75.	Davanje mita	0	0	0	0	0	0	2	0	0	0	**2**
Ukupno		**133**	**159**	**94**	**78**	**94**	**70**	**71**	**121**	**110**	**69**	**999**
Sveukupno - posebna plus opća k. d.		**186**	**222**	**138**	**116**	**143**	**116**	**140**	**222**	**152**	**131**	**1566**
Broj policijskih službenika - počinitelja		**131**	**162**	**107**	**90**	**91**	**90**	**104**	**89**	**87**	**92**	**1043**

U smislu preveniranja kažnjivih ponašanja policijskih službenika, valja imati predodžbu o tome kod kojih kaznenih djela policijski službenici dolaze u obzir kao češće potencijalni i, pa shodno tomu poduzimati adekvatne preventivne aktivnosti. Nije pri tome osobito bitno spadaju li ta kaznena djela u kategoriju specijalnih, odnosno općih kaznenih djela, bitno je samo da su policijski službenici, po prirodi svog posla, češće u situaciji počiniti ta djela od drugih građana, odnosno da svojstvo policijskog službenika i samom kaznenom djelu daje posebnu dimenziju, odnosno predstavlja posebnu „društvenu opasnost“.

Kako je iz tablice 2 vidljivo, najzastupljenija kaznena djela u skupini općih kaznenih djela kod kojih svojstvo policijskog službenika ima poseban značaj su „odavanje službene tajne“ i

„teška tjelesna ozljeda“. No, i kod ove grupacije kaznenih djela iznenađuje činjenica da u promatranom razdoblju nije zabilježeno niti jedno (očekivano) kazneno djelo „povrede ravnopravnosti građana“, „povreda prava na okupljanje i javni prosvjed“, „nedozvoljena uporaba osobnih podataka“, „rasne i druge diskriminacije“ i sl. Razlog za to zasigurno može biti dvojak: ili policijski službenici ne čine takva kaznena djela, ili nisu razvijeni mehanizmi i metodologija otkrivanja takvih kaznenih djela i njihovih počinitelja u policijskim redovima. Vrlo je vjerojatno da je i kod ovih, kao i kod drugih kaznenih djela, prisutna tzv. tamna brojka počinjenih a neotkrivenih kaznenih djela, ali upuštanje u procjenu broja takvih djela, bez relevantnih parametara – bila bi vrlo nezahvalna zadaća.

Što se tiče ostalih općih kaznenih djela vidljivo je da je najzastupljenije kazneno djelo krivotvorenje isprava, odnosno posebni slučajevi krivotvorenja isprava. Kako je iz prethodne tablice vidljivo, u promatranom razdoblju je evidentirano samo jedno kazneno djelo krivotvorenja službene isprave, pa se onda ovi brojni slučajevi krivotvorenja ne mogu dovesti u svezu sa policijskom službom i službenim ispravama. Preostaje stoga zaključak, da se ti slučajevi krivotvorenja u pretežnom broju slučajeva odnose na isprave iz područja građanskopravnih odnosa, kao npr. isprave kojima se dokazuje kreditna i jamstvena sposobnost, prebivalište na određenom području, potvrde o imovnom stanju i sl. Valja također napomenuti da je u promatranom periodu provedena i revizija dokumenata o stečenoj stručnoj spremi propisanoj za radno mjesto, odnosno obavljanje poslova policijskog službenika i utvrđen stanoviti broj krivotvorina što je bilo medijski intenzivno popraćeno, pa onda ta brojka od 220 slučajeva dobiva svoj smisao.

Nadalje je u značajnoj mjeri zastupljeno kazneno djelo „prijetnje“ i „prijevare“, što je podatak koji izaziva zabrinutost. Također zabrinjava značajan broj kaznenih djela protiv braka, obitelji i mladeži, kao što su „zapuštanje i zlostavljanje djeteta ili maloljetne osobe“, „sprječavanje i neizvršenje mjera za zaštitu djece i maloljetne osobe“, te „nasilničkog ponašanja u obitelji“. No, ta se brojka može dovesti i u vezu s prirodom policijskog posla. Poznato je da je taj posao zahtjevan i stresan, da je policijskom službeniku vrlo teško unaprijed planirati slobodno vrijeme i obiteljske obveze, pa posljedično, obiteljski život često trpi zbog toga, a počesto dolazi i do obiteljskih nesuglasica, svađa, pa i razvoda.[417] Također valja izraziti zabrinutost i zbog broja „pronevjera“, „krađa“ i „teških krađa“ počinjenih od strane policijskih službenika, ali i kaznenih djela „izazivanja prometne nesreće“, te „nedozvoljenog držanja oružja i eksplozivnih tvari“.

Što se tiče odnosa između broja počinitelja i počinjenih djela, u prvih 7 godina se ne mogu uočiti neke značajke koje bi imale obilježja sustavnosti, niti bi se iz njih mogli izvoditi određeni zaključci i zakonitosti, no posljednje tri godine se od toga ponešto razlikuju. Moglo

[417] Riječ je o radu u smjenama, radu noću, radu koji po potrebi službe može biti duži od radnim vremenom planiranog, rad subotama, nedjeljama, praznicima i drugim neradnim danima, dežurstvima i pripravnosti za rad, posebnostima i teškoćama kod planiranja godišnjeg odmora a nerijetko i prekidanjem istog, čestih promjena u dnevnom rasporedu službe izazvanog događanjima koje je teško unaprijed planirati, kao što mogu biti pobjede ili porazi u športskim susretima, pa slijedom toga dobronamjerni ili zlonamjerni dočeci aktera, najavljenim ili nenajavljenim prosvjedima ili drugim nemirima, i dr., čemu se policijske snage moraju „u hodu“ prilagođavati, posebnostima i tajnošću određenih poslova, a time i zabrani razgovora o tome i sa članovima obitelji, što zasigurno može biti remetilački faktor stabilnog braka ili bilo koje druge zajednice u smislu remećenja mogućnosti policijskog službenika da ispuni očekivanja ostalih članova zajednice.

bi se reći da relativno manji broj policijskih službenika čini veći broj kaznenih djela, odnosno da su kriminalno aktivniji. To je svakako podatak koji bi mogao biti od koristi svakom onom tko se kani baviti suzbijanjem policijske delinkvencije. Istodobno, ne treba ispustiti iz vida činjenicu da su sva navedena kaznena djela kriminalistički istražili i kaznene prijave podnijeli policijski službenici, dakle kolege protiv kolega.

Tablica 8: usporedni prikaz broja prijavljenih/evidentiranih posebnih kaznenih djela počinjenih od strane policijskih službenika i ostalih počinitelja u rh u razdoblju od 2002. do 2011. godine

Red. br./g.	**Kazneno djelo**	**Policijski službenici**	**Svi počinitelji**	**Udio policijskih službenika u %**
1.	Povreda prava na podn. pravn. lijekova i predst.	**0**	**0**	**0**
2.	Protuzakonita pretraga	**0**	**1**	**0**
3.	Iznuđivanje iskaza	**7**	**14**	**50**
4.	Zlostavljanje u obavljanju službe	**37**	**78**	**47,43**
5.	Mučenje i dr. okrutno neljuds. iIi poniž. post.	**0**	**0**	**0**
6.	Krivotvorenje službene isprave	**1**	**10393**	**0,009**
7.	Zlouporaba položaja i ovlasti	**302**	**7320**	**4,12**
8.	Nesvjestan rad u službi	**21**	**449**	**4,67**
9.	Neizvršavanje zapovijedi	**0**	**0**	**0**
10.	Povreda čuvanja državne granice	**0**	**1**	**0**
11.	Protuz. oslobođ. osob. kojoj je oduz. sloboda	**0**	**0**	**0**
12.	Prijevara u službi	**13**	**193**	**6,73**
13.	Primanje mita	**74**	**644**	**11,49**
14.	Protuz. prisv. stvari prilikom pretr. ili pregl.	**3**	**5**	**60**
15.	Protuzakonita naplata i isplata	**1**	**20**	**5**
16.	Narušavanje nepovredivosti doma	**2**	**1311**	**0,15**
17.	Protuzakonito oduzimanje slobode	**9**	**695**	**1,29**
18.	Povreda tajnosti pisama i dr. pošiljaka	**0**	**59**	**0**
19.	Neovlašteno snimanje i prisluškivanje	**0**	**63**	**0**
20.	Dovođenje u opasnost općeop. radnj. ili sred.	**24**	**4453**	**0,53**

Red. br./g.	Kazneno djelo	Policijski službenici	Svi počinitelji	Udio policijskih službenika u %
21.	Neprijavljivanje počinjenja kaznenog d.	**3**	**35**	**8,57**
Ukupno		**497**	**25734**	**1,93**

Iz tablice 3 je razvidno da udio policijskih službenika u populaciji počinitelja posebnih kaznenih djela iznosi 1,93 %. Pri tom ne treba smetnuti s uma da se glavnina tog udjela odnosi na prava posebna kaznena djela[418] gdje je svojstvo policijskog službenika nužno obilježje počinitelja, a kad se sagledaju obilježja nekih djela nametne se pitanje tko bi drugi uopće i mogao počiniti predmetno djelo, kao što je slučaj sa kaznenim djelima iznuđivanja iskaza, zlostavljanja u obavljanju službe, protuzakonitom prisvajanju stvari prilikom pretrage ili pregleda, gdje se udio policijskih službenika kreće od 47 do 60 %. No, i kod tih djela je vidljivo da gotovo polovina počinitelja otpada na neke druge službene osobe koji nisu policijski službenici. Iznenađuje i relativno mali udio policijskih službenika kod kaznenih djela zlouporaba položaja i ovlasti (4,12 %), nesavjesnog rada u službi (4,67 %) te prijevara u službi (6,73 %), iz čega proizlazi da su neke druge „službe“ tim kaznenim djelima znatno izloženije od policijske službe. Ne treba zanemariti niti ranije spomenutu činjenicu da kod znatnog broja tih djela nisu uopće zabilježeni policijski službenici kao počinitelji. Kod nepravih posebnih kaznenih djela situacija je slična, s time da je participacija policijskih službenika u delinkventskoj populaciji još i manja.

Tablica 9: usporedni prikaz broja prijavljenih/evidentiranih općih kaznenih djela počinjenih od strane policijskih službenika i ostalih počinitelja u rh u razdoblju od 2002. do 2011. godine

Red. br./g.	Kazneno djelo	Policijski službenici	Svi počinitelji	Udio policijskih službenika u %
Kaznena djela kod kojih svojstvo policijskog službenika ima poseban značaj				
1.	Ubojstvo	**2**	**438**	**0,45**
2.	Teško ubojstvo	**1**	**206**	**0,48**
3.	Prouzročenje smrti iz nehaja	**0**	**57**	**0**
4.	Tjelesna ozljeda	**4**	**4055**	**0,09**
5.	Teška tjelesna ozljeda	**31**	**11009**	**0,28**
6.	Tjelesna ozljeda na mah	**0**	**69**	**0**
7.	Tjelesna ozljeda iz nehaja	**0**	**233**	**0**

[418] U tablici prava posebna kaznena djela nalaze se u prvome dijelu od broja 1 do 15, a neprava posebna kaznena djela od broja 16 do 21, odvojeni trima crtama.

Red. br./g.	Kazneno djelo	Policijski službenici	Svi počinitelji	Udio policijskih službenika u %
8.	Povreda ravnopravnos. građana	**0**	**0**	**0**
9.	Povreda prava na okuplj. i javni prosvjed	**0**	**24**	**0**
10.	Nedozvoljena uporaba osobnih podataka	**0**	**45**	**0**
11.	Odavanje državne tajne	**0**	**1**	**0**
12.	Rasna i druga diskriminacija	**0**	**52**	**0**
13.	Spolni odnošaj zlouporabom položaja	**1**	**65**	**1,53**
14.	Lažno prijavljivanje kaznenog djela	**4**	**1421**	**0,28**
15.	Otkrivanje identiteta zaštićenog svjedoka	**0**	**0**	**0**
16.	Odavanje službene tajne	**48**	**67**	**71,64**
Ukupno		**91**	**17742**	**0,51%**
Ostala opća kaznena djela				
17.	Protuzakonito posredovanje	**3**	**200**	**1,5**
18.	Pronevjera	**37**	**3521**	**1,06**
19.	Otmica	**1**	**131**	**0,76**
20.	Neovlaštena uporaba	**12**	**245**	**4,89**
21.	Krivotvorenja[419]	**220**	**36162**	**0,6**
22.	Krivotvorenje novca	**1**	**3078**	**0,03**
23.	Prijetnja	**89**	**26577**	**0,33**
24.	Ratni zločin protiv civilnog pučanstva	**3**	**329**	**0,91**
25.	Zlouporaba opojnih droga	**28**	**79218**	**0,03**
26.	Protuzakonito prebaciv. osoba preko granice	**2**	**2126**	**0,09**
27.	Međunarodna prostitucija	**1**	**80**	**1,25**
28.	Bludne radnje	**4**	**2009**	**0,19**
29.	Silovanje	**9**	**900**	**1**

[419] U izvješćima se koristi zajednički stavak za krivotvorenja isprava, kao i za posebne slučajeve krivotvorenja isprava čl. 311. i čl. 313. KZ RH.

Red. br./g.	Kazneno djelo	Policijski službenici	Svi počinitelji	Udio policijskih službenika u %
30.	Prisila na spolni odnošaj	**1**	**35**	**2,85**
31.	Spolni odnošaj s djetetom	**1**	**645**	**0,15**
32.	Upoznavanje djece s pornografijom	**3**	**242**	**1,23**
33.	Iskorištavanje djece ili maloljet. osoba za pornografiju	**1**	**316**	**0,31**
34.	Dječja pornografija na račun. sustavu ili mreži	**1**	**333**	**0,3**
35.	Povreda dužnosti uzdržavanja	**4**	**6037**	**0,06**
36.	Podvođenje	**2**	**360**	**0,55**
37.	Zapuštanje i zlostavlj. djeteta ili malolj. osobe	**64**	**17614**	**0,36**
38.	Nasilničko ponašanje u obitelji	**26**	**13815**	**0,18**
39.	Sprječavanje i neizvrš. mjera za zaštitu djece i maloljetne osobe	**44**	**621**	**7,08**
40.	Krađa	**23**	**137762**	**0,01**
41.	Teška krađa	**43**	**247707**	**0,01**
42.	Oduzimanje tuđe pokretne stvari	**1**	**3823**	**0,02**
43.	Razbojništvo	**17**	**12627**	**0,13**
44.	Uništavanje ili oštećenje tuđe stvari	**12**	**16280**	**0,07**
45.	Utaja	**2**	**1198**	**0,16**
46.	Prijevara	**65**	**21190**	**0,30**
47.	Zlouporaba čeka i kreditne kartice	**5**	**1501**	**0,33**
48.	Zlouporaba osiguranja	**1**	**99**	**1,01**
49.	Iznuda	**3**	**1595**	**0,18**
50.	Ucjena	**1**	**178**	**0,56**
51.	Prikrivanje	**6**	**5320**	**0,11**
52.	Protuzakoniti lov	**4**	**1955**	**0,20**
53.	Protuzakoniti ribolov	**2**	**1952**	**0,10**
54.	Teška k. d. protiv opće sigurnosti	**5**	**524**	**0,95**
55.	Izazivanje prometne nesreće	**117**	**22439**	**0,52**

Red. br./g.	Kazneno djelo	Policijski službenici	Svi počinitelji	Udio policijskih službenika u %
56.	Nepružanje pomoći osobi teško tjelesno ozlijeđenoj u p. n.	**2**	**562**	**0,35**
57.	Izigravanje zabr. iz sig. mjera i pr. poslj. osude	**2**	**9189**	**0,02**
58.	Utaja poreza i dr. davanja	**1**	**613**	**0,16**
59.	Zlouporaba ovlasti u gospodars. poslovanju	**2**	**4570**	**0,04**
60.	Nedozvoljena trgovina	**6**	**2759**	**0,21**
61.	Izbjegavanje carinskog nadzora	**14**	**6989**	**0,2**
62.	Davanje lažnog iskaza	**4**	**1148**	**0,34**
63.	Sprječavanje dokazivanja	**2**	**189**	**1,05**
64.	Oduzimanje ili uništenje služb. pečata ili spisa	**1**	**37**	**2,7**
65.	Ovjerovljavanje neistinitog sadržaja	**13**	**3581**	**0,36**
66.	Sprječavanje sl. osobe u obavljanju sl. dužn.	**5**	**3045**	**0,16**
67.	Napad na službenu osobu	**5**	**1889**	**0,26**
68.	Lažno predstavljanje	**1**	**233**	**0,42**
69.	Skidanje i povreda služb. pečata i znaka	**1**	**752**	**0,13**
70.	Protupravna naplata	**1**	**1105**	**0,09**
71.	Nasilničko ponašanje	**12**	**2517**	**0,47**
72.	Dogovor za počinjenje k. djela	**1**	**78**	**1,28**
73.	Udruživanje za počinjenje k. djela	**3**	**263**	**1,14**
74.	Nedozvoljeno držanje oružja i eksploz. tvari	**36**	**5281**	**0,68**
70.	Davanje mita	**2**	**738**	**0,27**
Ukupno		**978**	**716282**	**0,13**
Sva opća kaznena djela		**1069**	**734024**	**0,145**

Red. br./g.	Kazneno djelo	Policijski službenici	Svi počinitelji	Udio policijskih službenika u %
Sveukupno opća i posebna kaznena djela		**1566**	**759758** **777566**[420]	**0,206** **0,201**

Ni kod općih kaznenih djela kod kojih svojstvo policijskog službenika ima poseban značaj nije uočena posebna opasnost od policijskih službenika kao možebitnih počinitelja tih djela, osim kod kaznenog djela odavanja službene tajne gdje je njihov udio 71,64 % (tablica 4). Naime, izuzev tog djela i spolnog odnošaja zlouporabom položaja (1,53 %), udio policijskih službenika je znatno ispod 1 %, a kod velikog broja djela uopće ne participiraju. Udio od 0,51 % u ukupnom zbroju uglavnom je rezultat tako velikog udjela odavanja službene tajne, što je više nego alarmantan podatak za policijsko vodstvo, ali i građanstvo. Naime, počinjenjem tog kaznenog djela ne povređuje se samo službena dužnost kao štićeno pravno dobro, nego se dovodi u pitanje i povjerenje javnosti ali još više i samih policijskih službenika u cijeli policijski i državni sustav. Kod ostalih općih kaznenih djela policijski službenici participiraju u udjelu od 0,13 %, odnosno kod svih općih kaznenih djela u udjelu od 0,14 %, što samo po sebi nije alarmantan podatak. Ali svakako se ne može šutke prijeći preko podatka da su policijski službenici u promatranom desetogodišnjem razdoblju počinili i 17 razbojništava, 89 prijetnji, 9 silovanja, kao i određeni broj drugih teških kaznenih djela. To je „šamar“ policijskoj službi ma kako se taj udio u usporedbi s ostalim počiniteljima kaznenih djela činio statistički malen i neznačajan.

Ukupno uzevši, udio od 0,20 % policijskih službenika u delinkventnoj populaciji dopušta izvođenje određenih zaključaka tek u komparaciji s ostalim izvršiteljima kaznenih djela. S obzirom na to da u odnosu na ukupni broj stanovnika RH udio policijskih službenika iznosi oko 0,40 %, a u populaciji radno aktivnog stanovništva oko 1 %, olako bi se mogao izvući zaključak o znatno manjoj kriminalnoj aktivnosti policijskih službenika od ostatka populacije u državi. No, kako je nemoguće da netko postane policijskim službenikom prije osamnaeste godine života, a s obzirom na beneficirani radni staž, puno ranije odlaze u mirovinu i prestaju biti policijski službenici, ne mogu se dobiti relevantni podaci ako ih se uspoređuje s ukupnom populacijom ali ni populacijom radno aktivnog stanovništva, jer su ostali radno aktivni do 65-e godine života, odnosno prijevremenog umirovljenja. Isto tako je potrebno uzeti u obzir zastupljenost žena u ukupnoj i policijskoj populaciji. Tek ujednačavanjem usporednih skupova možemo dobiti relevantne pokazatelje i podatke.

Iz Ministarstva unutarnjih poslova dobiven je podatak, da je prosječna starost policijskih službenika koji su u razdoblju od 2002. do 2011. godine otišli u mirovinu, 43 godine. Kako je jasno da ipak ne idu svi policijski službenici te dobi a i nešto stariji u mirovinu, odnosno da

[420] Tablice sadržavaju sva kaznena djela policijskih službenika počinjenih u promatranom razdoblju ali ne obuhvaća i kaznena djela kod kojih kao počinitelji nisu evidentirani policijski službenici. Stoga prvi broj predstavlja kaznena djela svih građana u kojima su participirali i policijski službenici, a drugi broj označava sva kaznena djela počinjena u promatranom desetogodišnjem razdoblju.

neki ostaju u službi do pune mirovine[421], lako se dalo izračunati da većina policijskih službenika u punu mirovinu odlazi do 50-e, odnosno 49-e godine života. Kako se ta dob podudara s dobnim razredima po kojima se u Ministarstvu prati stanje kriminaliteta (od 18 do 49 godina), može se načiniti sljedeća tablica koja odražava to stanje:

Tablica 10: Usporedni prikaz policijskih službenika i ostalih počinitelja kaznenih djela počinjenih u razdoblju od 2002. do 2011. godine

Svojstvo počinitelja	**2002.**	**2003.**	**2004.**	**2005.**	**2006.**	**2007.**	**2008.**	**2009.**	**2010.**	**2011.**	**Ukupno**
Polic. služb.	131	162	107	90	91	90	104	89	87	92	**1043**
Ostali počin.	31162	32845	30222	31745	32845	32260	32052	32819	31658	31369	**318977**
Ostali poč. od 18 do 49 g.	23915	24636	23256	23867	24636	23630	21390	23996	22839	22609	**234774**
Udio policij.službe-nika[422]	0,42 0,54	0,49 0,65	0,35 0,46	0,28 0,37	0,27 0,36	0,28 0,38	0,32 0,48	0,27 0,37	0,27 0,38	0,29 0,40	**0,32** **0,44**

Da bi se dobiveni podaci mogli međusobno komparirati i tumačiti, bilo je potrebno pribaviti prosječan broj stanovnika te dobi te prosječan broj policijskih službenika za promatrano razdoblje, te udio žena u toj populaciji (tablica 5). Naime, poznato je da je udio žena u ukupnoj populaciji viši od 50 %, a da u delinkventnoj populaciji sudjeluju u udjelima manjim od 10 %[423], a nasuprot tome da je populacija policijskih službenika pretežno muškog roda, s tek oko 15 % policijskih službenica[424]. No, kako se u Ministarstvu unutarnjih poslova ne vode posebne evidencije počinitelja kaznenih djela iz redova policijskih službenika po spolu, nije

[421] Odlazak u mirovinu policijskih službenika je uređen Zakonom o pravima iz mirovinskog osiguranja djelatnih vojnih osoba, policijskih službenika i ovlaštenih službenih osoba, NN 128/99., 16/01., 22/02., 41/08., 71/010., 97/012., 118/012.

[422] Prvi broj se odnosi na udio (%) policijskih službenika u cjelokupnoj delinkventskoj populaciji, a drugi broj se odnosi na udio policijskih službenika u populaciji počinitelja kaznenih djela u dobnoj skupini između 18 i 49 godina.

[423] Prema Derenčinoviću, po novijim podacima udio žena u kriminalitetu iznosi 9,8 % s tendencijom rasta. Derenčinović, D.: Uvod u kriminologiju i socijalnu patologiju s osnovama kaznenog prava, Pravni fakultet Sveučilišta u Zagrebu, 2004., 177.

[424] Mandić. M., Vojković. A. M.: Policajke kroz povijest, Žene u policiji, posebno izdanje MUP mir ugled povjerenje, br. 46/011., MUP RH 2011., 5., navodi udio od 14,7 %.

moguće provesti komparaciju na razini muškarci – policijski službenici u odnosu na muškarce – ostale građane, odnosno žene – policijske službenice u odnosu na žene – ostale građanke, već će se radi izračuna u statističke metode i izračune morati uvesti ponderi, odnosno ponderiranje uzoraka. Izjednačavanje bilo kojeg uzorka i populacije uobičajeno se radi ponderiranjem odnosno dodjeljivanjem veće važnosti svojstvu koje je podcijenjeno i dodjeljivanjem manje važnosti izučavanom svojstvu koje je precijenjeno.

Podaci o broju stanovnika dobiveni su putem Statističkog zavoda RH, a za izvor podataka o broju policijskih službenika poslužila je tiskovina „MUP mir ugled povjerenje“, kao službeno glasilo Ministarstva unutarnjih poslova. Tamo stoji da je u Ministarstvu bilo 20 821 policijska službenika[425]. S obzirom na to da se radi o jednokratnim podacima potrebno je, na temelju objektivnih parametara obaviti procjenu prosječnog broja policijskih službenika u promatranom desetogodišnjem razdoblju. Imajući u vidu broj kandidata koje se primalo na školovanje za policijske službenike na temelju javno raspisanih (i javno dostupnih) natječaja za školovanje policijskih službenika u promatranom razdoblju, a koji je znatno intenziviran u posljednjih nekoliko godina, te prosječnom godišnjem napuštanju policijske službe, prosječan broj policijskih službenika u promatranom periodu procijenjen je na 17 500. Istom logikom došlo se do prosječnog broja žena u policijskoj populaciji te je on za promatrano razdoblje procijenjen na 10 %.

Imajući te brojke u vidu, onda je procjena da žena u policiji ima oko 1 750, a muškaraca 15 750. U populaciji, prema podacima Državnog zavoda za statistiku, omjer muškaraca i žena u RH je 48,3 : 51,7[426], dakle vrlo blizak odnosu 50 : 50, pa ćemo radi ujednačavanja skupova i olakšavanja izračuna tretirati taj približan odnos kao relevantan. Ako želimo ujednačiti uzorak policijskih službenika s populacijom po spolu, u policiji bi trebao biti pet puta veći broj žena i upola manje muškaraca. Dakle, da bi omjer bio kao u populaciji, žena bi trebalo biti 1 750 × 5 = 8 750 a muškaraca upola manje 15 750 × 0,55556 = 8 750. Na taj način bi uzorak policajaca bio izjednačen po spolu s populacijom unutar dobne skupine od 18 do 49 godina.

Tablica 11: Postotak muškaraca i žena i ponderi

	Populacija	**Policija**	**Ponderi**
m 18-49	50,0	90	0,56
ž 18-49	50,0	10	5,00

Da je proporcija žena u policiji jednaka proporciji žena u populaciji, u policiji bi bilo 5 puta više kaznenih djela koje su počinile žene te upola manje kaznenih djela koje su počinili muškarci. Da bismo izračunali o kojem broju počinitelja se radi, trebali bismo znati podatak koliko kaznenih djela od ukupnog broja počinjenih kaznenih djela u policiji su počinile policijske službenice a koliko policijski službenici. Budući da su ti brojevi nepoznati, moramo poći od populacije jer su ti podaci poznati. Koristit ćemo istu logiku samo je potrebno

[425] Mandić. M., Vojković. A. M.: Policajke kroz povijest, Žene u policiji, posebno izdanje MUP mir ugled povjerenje, br. 46/011., MUP RH 2011., 7.; godinu dana ranije u istom časopisu br. 45/010, MUP RH, 70, navodi se podatak od 20934 policijska službenika.
[426] http://www.dzs.hr/Hrv_Eng/publication/2011/07-01-04_01_2011.htm

dodijeliti druge pondere kako bi ove dvije skupine bile usporedive. Dakle, kad bi omjer žena i muškaraca u populaciji bio jednak omjeru muškaraca i žena u policiji omjer bi bio 10 : 90 umjesto 50 : 50. Da bismo dobili takav omjer potrebno je pomnožiti ukupan broj žena i ukupan broj muškaraca u populaciji sa ponderima koji su izračunati kao omjer proporcije policijskih službenika/ica i proporcije muškaraca/žena u populaciji. Pondere je potrebno računati za svaku godinu posebno jer se i omjeri muškaraca i žena razlikuje po godinama. Prosječni ponderi za izračun pretpostavljene spolne strukture u populaciji kada bi omjer muškaraca i žena bio kao u policiji, prikazani su u tablici 7, a izračun spolne strukture (tablica 8) napravljen je prema ponderima posebno za svaku godinu radi točnije procjene.

Tablica 12: Postotak muškaraca i žena u populaciji i uzorku

	Policija	**Populacija**	**Ponderi**
m 18-49	90,0	50	1,788
ž 18-49	10,0	50	0,201

Stvarna spolna struktura u populaciji za dobnu skupinu 18 - 49 godina prema Državnom zavodu za statistiku izgleda ovako.

Tablica 13: Broj stanovnika RH, dobna skupina 18-49, procjena sredinom godine i pretpostavljena spolna struktura policije iste dobi (pomnoženo s ponderima)

God./spol (opća populacija)	**muškarci**	**žene**	**Ukupno**
2002.	1.012.043	999.911	2.011.954
2003.	1.009.409	997.407	2.006.816
2004.	1.006.256	994.865	2.001.121
2005.	1.000.884	989.403	1.990.287
2006.	996.355	983.320	1.979.675
2007.	991.196	977.158	1.968.354
2008.	986.862	971.634	1.958.496
2009.	980.662	964.453	1.945.115
2010.	971.616	954.088	1.925.704
2011.	966.563	948.360	1.914.923[427]
God./spol (pretpostavljena spolna struktura policije)	**muškarci**	**žene**	**Ukupno**
2002.	1.810.759	201.195	2.011.954
2003.	1.806.134	200.682	2.006.816
2004.	1.801.009	200.112	2.001.121
2005.	1.791.258	199.029	1.990.287

[427] U podacima Državnog zavoda za statistiku RH za 2011. godinu, broj stanovnika po dobi nije, kao ranijih godina, objavljen na godišnjoj razini već u petogodišnjim razredima. Budući je dob od 18. do 20. godine utopljena u dobni razred od 15 – 19 godina, podaci za 2011. godinu su procijenjeni na način da su brojevi umanjeni za prosjek pada broja stanovnika u prethodnim godinama.

2006.	1.781.708	197.968	1.979.675
2007.	1.771.519	196.835	1.968.354
2008.	1.762.646	195.850	1.958.496
2009.	1.750.604	194.512	1.945.115
2010.	1.733.134	192.570	1.925.704
2011.	1.723.431	191.492	1.914.923

Pretpostavljena spolna struktura policije primijenjena na opću populaciju dobi između 18 i 49 godina sa značajno većim brojem muškaraca nego žena nalazi se u donjem dijelu tablice 8. Znači, žena bi bilo 5 puta manje a muškaraca 1,79 puta više pa bi i broj kaznenih djela koje bi počinile žene bio 5 puta manji, a broj kaznenih djela koje bi počinili muškarci 1,79 puta veći. Ukupan broj počinitelja bio bi očekivano veći jer je broj muškaraca veći s obzirom na činjenicu da muškarci čine značajno više kaznenih djela od žena.

Ako uzmemo u obzir da su žene u ukupnom kriminalitetu u populaciji zastupljene sa 10 %, onda procijenjen broj počinjenih kaznenih djela u populaciji od strane žena iznosi kao u tablici 9.

Tablica 9: Broj počinjenih kaznenih djela u općoj populaciji za dobnu skupinu između 18 i 49 godina po spolu, neujednačeno po spolu i izjednačeno po spolnoj strukturi s policijskim službenicima

Neujednačeno po spolu	**Počinitelji u populaciji od 18 do 49 g. MUŠKARCI**	**Počinitelji u populaciji od 18 do 49 g. ŽENE**	**Počinitelji u populaciji od 18 do 49 g. UKUPNO**
2002.	21524	2392	**23915**
2003.	22172	2464	**24636**
2004.	20930	2326	**23256**
2005.	21480	2387	**23867**
2006.	22172	2464	**24636**
2007.	21267	2363	**23630**
2008.	19251	2139	**21390**
2009.	21596	2400	**23996**
2010.	20555	2284	**22839**
2011.	20348	2261	**22609**
Ukupno	**211297**	**23477**	**234774**
Ujednačeno po spolu (prema spolnoj strukturi policije)	**Počinitelji u populaciji od 18 do 49 g. ŽENE**	**Počinitelji u populaciji od 18 do 49 g. MUŠKARCI**	**Počinitelji u populaciji od 18 do 49 g. UKUPNO**
2002.	478	38.313	38.791
2003.	493	39.466	39.959
2004.	465	37.255	37.721
2005.	477	38.234	38.712

2006.	493	39.466	39.959
2007.	473	37.855	38.328
2008.	428	34.267	34.695
2009.	480	38.441	38.921
2010.	457	36.588	37.045
2011.	452	36.220	36.672
Ukupno	**4.696**	**376.105**	**380.801**

Kao što je ranije navedeno, ako uzmemo u obzir spolnu strukturu policijskih službenika primijenjenu na opću populaciju, broj počinitelja kaznenih djela u populaciji bio bi znatno veći. Točnije, broj kaznenih djela koje počine žene bio bi pet puta manji a broj kaznenih djela koje počine muškarci bio bi 1,79 puta veći.

Ukupan broj počinitelja u populaciji bio znatno veći kad bi spolna struktura populacije bila kao spolna struktura u policiji, tj. da je u populaciji znatno više muškaraca nego žena. Dakle, broj počinitelja znatno ovisi o spolnoj strukturi populacije koju promatramo. U policiji, bilo je 99,4% nepočinitelja i svega 0,6% počinitelja kaznenih djela. U općoj populaciji, bilo je 97,6% nepočinitelja i 2,4% počinitelja kaznenih djela.

2. RAZLIKE U BROJU POČINJENIH KAZNENIH DJELA U POLICIJI I U OPĆOJ POPULACIJI UVAŽAVAJUĆI RAZLIKE U SPOLNOJ STRUKTURI

Postotak počinitelja kaznenih djela u policiji kreće se od 0,5% 2010. godine do najviše 0,93% 2003. godine. Broj počinitelja kaznenih djela u populaciji s omjerom muškaraca i žena kakav je u stvarnoj populaciji nešto je veći nego u policiji te se kreće od 1,09 % u 2008. godini do 1,24 % u 2006. godini. Međutim, kako smo ranije prikazali, broj počinitelja znatno ovisi o spolnoj strukturi. Vodeći brigu o tome da je u populaciji znatno manje muškaraca nego u policiji – broj počinitelja kaznenih djela u populaciji znatno je podcijenjen (tablica 10).

Tablica 14: Broj počinitelja kaznenih djela među policijskim službenicima i u općoj populaciji

Policijski službenici	počinitelji	% počinitelji	nepočinitelji	% nepočinitelja	**Ukupan broj policijskih službenika**
2002.	131	0,75	17369	99,25	**17500**
2003.	162	0,93	17338	99,07	**17500**
2004	107	0,61	17393	99,39	**17500**
2005.	90	0,51	17410	99,49	**17500**
2006.	91	0,52	17409	99,48	**17500**
2007.	90	0,51	17410	99,49	**17500**
2008.	104	0,59	17396	99,41	**17500**
2009.	89	0,51	17411	99,49	**17500**
2010.	87	0,50	17413	99,50	**17500**

2011.	92	0,53	17408	99,47	**17500**
Ukupno	**1043**	**0,60**	**173957**	**99,40**	**175000**
Opća populacija	počinitelji	% počinitelji	nepočinitelji	% nepočinitelja	**Broj stanovnika RH**
2002.	23915	1,19	1988039	98,81	**2011954**
2003.	24636	1,23	1982180	98,77	**2006816**
2004	23256	1,16	1977865	98,84	**2001121**
2005.	23867	1,20	1966420	98,80	**1990287**
2006.	24636	1,24	1955039	98,76	**1979675**
2007.	23630	1,20	1944724	98,80	**1968354**
2008.	21390	1,09	1937106	98,91	**1958496**
2009.	23996	1,23	1921119	98,77	**1945115**
2010.	22839	1,19	1902865	98,81	**1925704**
2011.	22609	1,18	1892314	98,82	**1914923**
Ukupno	**189326**	**1,19**	**15672492**	**98,81**	**15861818**

Kada bismo vodili računa o spolnoj zastupljenosti policije, nasuprot općoj populaciji, broj počinitelja kaznenih djela u općoj populaciji, kada bi omjer muškaraca i žena bio kao u policiji bio bi znatno veći tj. kretao bi se u rasponu od 1,9 % do 2,0 % (tablica 11).

Tablica 15: Broj počinitelja kaznenih djela u populaciji vodeći brigu o spolnoj strukturi kao u policiji

Svojstvo počinitelja	počinitelji	% počinitelji	nepočinitelji	% nepočinitelja	**Broj stanovnika RH**
2002.	38.791	1,9	1.973.163	98,1	**2011954**
2003.	39.959	2,0	1.966.857	98,0	**2006816**
2004	37.721	1,9	1.963.400	98,1	**2001121**
2005.	38.712	1,9	1.951.575	98,1	**1990287**
2006.	39.959	2,0	1.939.716	98,0	**1979675**
2007.	38.328	1,9	1.930.026	98,1	**1968354**
2008.	34.695	1,8	1.923.801	98,2	**1958496**
2009.	38.921	2,0	1.906.194	98,0	**1945115**
2010.	37.045	1,9	1.888.659	98,1	**1925704**
2011.	36.672	1,9	1.878.251	98,1	**1914923**
Ukupno	**380.801**	2,4	15.481.017	97,6	**15861818**

Hi - kvadrat testom testirana je razlika između broja počinitelja/ nepočinitelja kaznenih djela u populaciji policije od broja počinitelja/ nepočinitelja kaznenih djela u općoj populaciji, vodeći brigu o razlikama u spolnim strukturama policijskih službenika i opće populacije (tablica 12).

Tablica 16: Rezultati provedenih hi - kvadrat testova

	2002.	**2003.**	**2004.**	**2005.**	**2006.**	**2007.**	**2008.**	**2009.**	**2010.**	**2011.**
Počinitelji fo	131	162	107	90	91	90	104	89	87	92
Nisu počinitelji fo	17369	17338	17393	17410	17409	17410	17396	17411	17413	17408
Očekivani broj počinitelja ft	337	348	330	340	353	341	310	350	337	335
Očekivani broj nepočinitelja ft	17163	17152	17170	17160	17147	17159	17190	17150	17163	17165
Hi - kvadrat	128,7*	101,8*	153,5*	187,8*	198,7*	188,2*	139,4*	198,8*	188,8*	179,8*

**p < 0,05; df = 1, Hi - kvadrat granični = 3,84*

Broj počinitelja kaznenih djela u policiji kreće se od 87 do najviše 162 u promatranom razdoblju. Prema očekivanjima, broj kaznenih djela počinjenih u populaciji znatno su veći. Dobiveni Hi-kvadrat testovi statistički su značajni uz p<0,05 te se može zaključiti da je broj počinitelja kaznenih djela u policiji statistički značajno manji nego u populaciji u svim analiziranim razdobljima (tablica 12).

Iz netom iznesenih podataka proizlazi da su policijski službenici u kriminalnim statistikama višestruko manje zastupljeni od ostatka građanske populacije. Naravno, same brojke, ma koliko bile statistički značajno manje, same po sebi otvaraju određena pitanja. U prvome redu postavlja se pitanje realnih izračuna, odnosno procjena tamnih brojki za obje „delinkventne“ skupine, ali i društvena očekivanja od jednih i drugih a napose, očekuje li se od policijskog službenika apsolutna moralna neupitnost? I bez obzira na to kakav odgovor bio, kolika se briga i značaj pridaje tom pitanju i kolika su ulaganja potrebna za tako visoka očekivanja od jedne, htjeli ili ne htjeli priznati, kriminalitetu izložene profesije? Takva pitanja postavljena u trenutku pisanja ovoga rada, kada se kaznenopravno procesuiraju neki bivši vodeći ljudi države, mogu čudno odzvanjati ali itekako imaju smisla. Nedvojbeno će svaki građanin osuditi svaki protuzakoniti čin bilo kojeg policijskog službenika, a naročito počinitelje kaznenih djela kao najtežih delikata, jer se od policijskog službenika, kao „čuvara zakona“ naprosto očekuje da ne čini nego da sprječava i otkriva kažnjiva djela i njihove počinitelje i na taj način osigurava sigurnost cjelokupnog društva. Nije moguće cjelovito objasniti uzroke tog fenomena bez provođenja temeljite znanstvene analize mnogih elementa općenito u društvu a napose policijskom sustavu, mnogih odnosa i relacija između policijskih službenika i ostatka zajednice te mnogih drugih socijalnih i inih relacija. Pri tome bi valjalo imati na umu da je

ponekad vrlo tanka linija razgraničenja između zakonitog i nezakonitog postupka policijskog službenika kod primjene značajnog broja policijskih ovlasti. Intervencija koja je otpočela opravdano i zakonito, ovisno o prirodi i dinamici provođenja mjere začas izmakne kontroli i sklizne na područje neopravdanog i nezakonitog postupka. Moguće je da bi poneko objašnjenje glasilo i da su policijski službenici samo ljudi s čime bismo se mogli složiti. No, tim ljudima nikako nije mjesto u policiji, pa je, kao i za druge počinitelje kaznenih djela iz policijskih redova potrebno razraditi učinkovite mehanizme kako da tako predisponirani pojedinci i ne uđu u policijski sustav, a ako uđu, da ga napuste uz što manje štete.

Ovdje svakako treba naglasiti mjesto i ulogu policijskog sustava u okviru kojeg djeluje svaki policijski službenik. On mora biti izgrađen, organiziran i vođen ne na način da svojom tajnovitošću, zatvorenošću u sebe i netransparentnošću svoga rada stvara uvjete i pruža zaklon za različite nezakonitosti i njihove počinitelje, već naprotiv, otvorenošću i transparentnošću onemogućavati povoljno okruženje za različite nezakonitosti i neprofesionalnosti. U takvim uvjetima se i kriminalna ponašanja lakše uočavaju i otkrivaju.

4. NOVE TEHNOLOGIJE I PREVENCIJA POLICIJSKE DELINKVENCIJE

Opravdano se može postaviti pitanje je li moguće utjecati na smanjenje tzv. policijske delinkvencije uvođenjem novih tehnologija u postupanje policije? Mnoštvo je tehnoloških noviteta koji se uvode u rad policije na različitim razinama, ali pod novim tehnologijama s takvim „antidelinkvencijskim“ potencijalom, može se smatrati projekt e–policije, odnosno oni njegovi segmenti koji obuhvaćaju sustav kamera koje policijski službenici nose na sebi i sustav korištenja prijenosnih računala, tj. tableta umjesto papirnatih notesa, obrazaca i slično koji su se aktualizirali unatrag godinu-dvije. U istu grupu se može svrstati i sustav geografskog pozicioniranja policijskih službenika na terenu koji je u više ili manje uspješnoj primjeni već nekoliko posljednjih godina. Medijsku pozornost su najviše privukle kamere na prsima policijskih službenika, posebno nakon slučaja tzv. policijske brutalnosti u Osijeku koja se dogodila 16. 12. 2015. godine, kad je javno objavljena snimka postupanja policijskog službenika prema gospođi koja je prešla cestu za vrijeme trajanja crvenog svjetla na semaforu, a koja je izazvala mnoge kontroverze u stručnoj i široj javnosti. Stoga je o svakom od tih noviteta i njegovim preventivnim kapacitetima potrebno nešto više reći. Pri tome se nećemo baviti tehničkim i drugim svojstvima takvih tehnoloških rješenja već ćemo se fokusirati na njihove preventivne antikorupcijske i „antidelinkvencijske“ kapacitete.

4.1. Geografsko pozicioniranje

Kad govorimo o geografskom pozicioniranju, mislimo na sustav koji omogućuje lociranje policijskih jedinica na terenu u realnom vremenu. U dnevnoj policijskoj praksi to znači da, zahvaljujući GPS signalu komunikacijskog uređaja na zaduženju policijske ophodnje ili pojedinca, operativno dežurstvo odnosno operativno – komunikacijski centar ili rukovoditelj određene razine može na ekranu u realnom vremenu vidjeti poziciju svake jedinice na terenu te im dodjeljivati zadaće i pratiti tijek njihove realizacije. Uvođenje ove tehnologije nije prošlo bez problema zbog mnogih tehničkih problema, ali u ovome trenutku sustav u dnevnoj policijskoj praksi solidno funkcionira. Na prvi pogled ovaj sustav nema prevelik

antikorupcijski, tj. antidelinkvencijski kapacitet, ali to tako izgleda samo na prvi pogled i samo onima koji ne znaju previše o tzv. policijskoj delinkvenciji[428]. Ovaj sustav nesumnjivo ima značajnu ulogu u suzbijanju policijske delinkvencije jer su policijski službenici takvih sklonosti svjesni da je njihova pozicija razvidna u realnom vremenu, a i naknadno lako dokaziva ukoliko dođe do propitivanja ili istraživanja njihova postupanja. Takva informacija, doduše, ima vrijednost indicije, ali u korelaciji sa drugim dokazima ili indicijama, može značajno doprinijeti utvrđivanju možebitno spornih činjenica. Stoga samo postojanje takvog sustava može odvratiti policijskog službenika od nezakonitih i nepravilnih postupanja ili ponašanja. Taj sustav ima i mnoge druge benefite u smislu organizacije policijske službe, upućivanja pomoći policijskim službenicima i sl., ali to nije predmet bavljenja ovog rada.

4.2. Sustav policijskih kamera (eKiosk)

Pod sustavom policijskih kamera misli se na pilot-projekt E-sigurnost u okviru kojeg se provodi pilot-projekt „Sustav za upravljanje policijskim kamerama eKiosk“, a koji se provodi u četiri najveće policijske uprave u RH. Deklarirani ciljevi provođenja projekta su zaštita policijskih službenika ali i građana prilikom policijskog postupanja, minimiziranje mogućnosti korupcije, opremanje policijskih službenika ICT opremom, probitak kriminalističkog istraživanja te automatiziranje radnih procesa u postupanju policijskih službenika[429]. Za potrebe ovog rada fokusirat ćemo se na deklarirani cilj minimiziranja mogućnosti korupcije. Valja napomenuti da nije propisana obveza kontinuiranog snimanja svih postupaka policijskog službenika od početka pa do kraja smjene[430]. Pitanje je bi li to bilo potrebno i opravdano sve kad bi i bilo tehnički moguće, no, bilo kako bilo, policijski službenici kameru koriste ili po zapovijedi nadređenog službenika ili samoinicijativno. Dužni su, uvijek kad je to moguće snimati: kada je to naloženo radnim nalogom ili planom posebnog osiguranja, kada se primjenjuje ili se očekuje primjena sredstava prisile, kada se osobu uhićuje, privodi ili dovodi ili se očekuje takvo postupanje, kod postupanja koja mogu biti incidentna, kažnjive radnje koje se čine prema policijskom službeniku, dolazak na mjesto događaja koje treba osigurati, događaje kod kojih se može očekivati da će uslijediti pritužba građana na postupanje policijskog službenika, te u situacijama kad po procjeni policijskog službenika snimljeni materijal može poslužiti kao dokaz u kriminalističkom istraživanju[431]. Vidljivo je da izvan nabrojenih situacija ne postoji obveza snimanja, odnosno u značajnom broju slučajeva ovisi o procjeni policijskog službenika kako će se neka, možda banalna situacija i intervencija u budućnosti razvijati. Uza sve poštovanje policijske intuicije, neke od nabrojenih situacija od policijskih službenika očekuju posebne sposobnosti predviđanja budućih događaja, da ne kažemo proročke sposobnosti. Može se očekivati da policijski službenici koji se u određenu intervenciju upuštaju motivirani koruptivnim razlozima, takvu intervenciju neće snimati. Naravno da će se takvi pravdati da nisu nikako mogli predvidjeti da

[428] Više o policijskoj delinkvenciji na primjeru korumpiranja prometne policije vidi Mršić: Je li borba protiv korupcije realnost ili iluzija, Policija i sigurnost, br. ¾/2006. str. 109-152.
[429] Raspis Ravnateljstva policije broj:511-01-50-72786/17-2'15., od 10. veljače 2016.
[430] U ovom trenutku postoje određena tehnička ograničenja, tj. ograničena memorija i trajanje baterije kamere koji su tehnički lako rješivi. Autoophodnje već sad imaju mogućnost dopunjavanja baterije u službenom vozilu a to nije neizvedivo i za pješačke ophodnje, kao i za proširenje memorijskih kartica.
[431] Ibid. Fn. 19.

će „banalna“ intervencija završiti kao incidentna. Pitanje je koliko se „prirodno“ ponašaju policijski službenici kada snimaju svoje postupanje i znaju to. Naime, mnogi ljudi, pa time i policijski službenici imaju jako izražen strah od javnog nastupa čemu je ovakva situacija prilično bliska, no to je pitanje za neki drugi kontekst koji nije predmet ovoga rada. Činjenica je da hrvatska policija ovim pilot-projektom pravi značajan iskorak u svjetskim razmjerima, budući da se najveća većina policija svijeta ne upušta u ovako nešto. To bi možda moglo značiti da se u tim državama, od kojih su mnoge tehnički naprednije od Republike Hrvatske, ima više povjerenja u postupanje policije ili u tome prepoznaju više problema nego benefita. Takva iskustva su poznata u pojedinim državama u SAD-u, gdje su neki odjeli instalirali razne oblike sustava videonadziranja ili audionadziranja kako bi zabilježili susrete policije s građanima.[432] Videonadziranje je postavljeno u vozila, gdje postoje videokamere koje se aktiviraju svaki put kada se policijski službenik zaustavi ili susretne građanina ili se uključuje u neku vrstu razgovora. Premda su policijski službenici u postupanju pružili otpor ovakvoj vrsti nadzora, on se, prema riječima autora, pokazao kao učinkoviti nadzor službenika u odnosu s građanima. Policijski službenici, svjesni snimanja, suzdržavaju se od govora ili aktivnosti koje mogu povrijediti građane ili koje oni mogu interpretirati kao neprofesionalno ponašanje ili ponašanje izvan policijskih granica i procedura. Audionadgledanje u biti funkcionira na isti način. Ovdje su službenici izloženi audiosnimačima koji su postavljeni tako da snime sve susrete s građanima. Audionadzor je, prema istom autoru koristan, jeftiniji i dobra je alternativa videonadziranju. Audiosnimke mogu registrirati bitne činjenice kako bi se naknadno detaljno inspicirao događaj. Problem ovakvog nadzora je ponajprije trošak. Videokamere su prilično skupe za instaliranje, posebice u vozilima koje mogu razviti velike brzine. Održavanje uređaja može također biti skupo.

Primjera radi, u Knoxvilleu, Tennessee, policijski odjel instalirao je videokamere u svoja vozila. Njihova politika bila je da te kamere trebaju biti aktivirane i ostanu uključene cijelo vrijeme tijekom smjene a državni pravobranitelj Tennesseea je inzistirao da snimke trebaju biti sačuvane trajno. Doslovno, odjel sada ima na tisuće uskladištenih snimki. U Riversideu, California, policijski odjel implementirao je sustav koristeći videokamere i sumnjive susrete pohranjuje na računalo u odjelu. Ovo je bitno smanjilo probleme pohrane, ali je rezultiralo potrebom za dodatnom radnom snagom koja će uređivati i pohranjivati snimke na čuvanje. Kod njih nije bilo slučajeva istraživanja audiosnimaka ili videosnimaka kako bi se utvrdilo je li građanska pritužba osnovana, a ustrojena je i stvarna evidencija policijske administracije prema kojoj je broj pritužbi smanjen a istraživanje građanskih pritužbi postalo mnogo lakše i poštenije.

Mada takva američka iskustva imaju svoju vrijednost, valja napomenuti da je informatička tehnologija u međuvremenu uznapredovala do te mjere da kamere mogu nositi policijski službenici – pojedinci, te da, u fizičkom smislu, kamera ne ograničava značajnije policijskog službenika. Također je riješen ili rješiv problem čuvanja takvih snimki što je također rezultat razvoja informatičke tehnologije. Problem održavanja u ovoj fazi projekta još nije došao do izražaja, a u budućnosti će se, po svoj prilici, morati rješavati. Vrlo je vjerojatno da će se u budućnosti morati voditi brigu i o pojačanoj antivirusnoj i drugovrsnoj informatičkoj zaštiti,

[432] Larry K. G.: Controlling The Police: The American Experience (*nadzor policije – američka iskustva*), California State University, Criminal Justice Department, San Bernardino, CA USA, 2006., 4-16.

jer bi „provaljivanje“ u sustav i uvid u te snimke mogao postati zanimljiv osobama kojima to nije namijenjeno, tzv. hakerima i drugima.

Svakom razumnom su jasne prednosti ovakvog sustava i lako je zamislivo razvijanje ovog sustava po scenariju koji već dugo gledamo u nekim „špijunskim“ filmovima ili serijama, gdje su operativci snabdjeveni minijaturnim kamerama usmjeravani od strane svoga vodstva i tehničke potpore, koji putem te kamere imaju uvid u sve ono što ima i operativac na terenu. No, jasno je da ovaj model ima i određenih nedostataka. Naime, niti je moguće „organizirati“ sigurnosne događanja da se odvijaju u fokusu kamere, ispred policijskog službenika snabdjevenog kamerom, odnosno u dometu mikrofona, niti je ovakav način primjenjiv u brojnim praktičnim situacijama kad je npr. potrebna brza intervencija i djelovanje, a posebno je ovakav način neprimjenjiv kod poslova kriminalističke policije, odnosno kriminalističkog istraživanja. Opravdano se može postaviti pitanje kako će policijski službenik doći do operativno interesantne informacije s upaljenom kamerom na prsima? A znamo da je nedostatak ovakvih informacija dugogodišnja rak-rana ne samo hrvatske policije. S druge pak strane, svaka policijska intervencija koja iz ovih ili onih razloga ne bi bila snimljena, tu bi intervenciju opteretila dodatnom sumnjom jer, eto, nije snimljena. Uporaba sredstava prisile od strane policijskog službenika snabdjevenog kamerom također bi mogla biti problematična, posebno kod fizičke snage gdje se ostvaruje neposredan kontakt tijela policijskog službenika s tijelom osobe prema kojoj se primjenjuje određeni zahvat, npr. ključ na laktu. Može se pretpostaviti da će se u budućnosti sve više tražiti preciznost snimanja, bolja kvaliteta snimljenog materijala, veća razlučivost spornih detalja i sl., na što će se policijski službenici morati više fokusirati. Hoće li to fokusiranje ići na štetu kvalitete intervencije ostaje nam vidjeti, a o tome koliko je „snimateljski posao“ zahtjevan, lako bi se moglo doznati od svakog profesionalnog snimatelja, kamermana ili kako god nazivali tu zahtjevnu profesiju. Može se također postaviti pitanje je li moguće učinkovito „servisirati“ ovaj sustav s postojećim kadrovskim potencijalima ili je potrebno otvoriti neka nova radna mjesta koja bi „pokrivala“ ove poslove? Naravno da je ove poslove uvijek moguće dodati nekom službeniku ili rukovoditelju koji već ima svoj djelokrug poslova i zadataka. No, do kad će se na određenim razinama, uz „stare“ poslove moći dodavati „novi“, a da to ne bude na štetu razumno dobro odrađenog posla, ostaje upitno. Najgori mogući scenarij jest da se policija instaliranjem ovakvog sustava „samoobrambeno“ ponaša, odnosno snima postupanje svojih službenika kako bi opravdala njihov postupak. To bi značilo da se nema povjerenja u policijske službenike, da se njihova krivnja i malicioznost podrazumijevaju, odnosno da se suprotno svim drugim građanima mora dokazivati njihova nedužnost i profesionalnost kod službenog postupanja. Osnovni pravni i demokratski postulat jest da nitko nije dužan dokazivati svoju nedužnost, da se ona presumira, odnosno da teret dokazivanja nečije krivnje leži na onom tko optužuje. Ako bi filozofija snimanja policijskog postupanja išla za tim da unaprijed pravda postupak policijskog službenika, to bi mogao biti početak kraja policije kakvu poznajemo. Tim više što i provedeno istraživanje policijske delinkvencije ne daje za pravo takvom nepovjerenju u policijske službenike. Valja se prisjetiti da je usporedba policijske i građanske delinkvencije pokazala da su policijski službenici, ipak, uza sve ograde od onih koji se u to upuštaju, višestruko „pošteniji“ od ostatka populacije i nema nikakvog opravdanog razloga s generalnim nepovjerenjem gledati na službenike koji u velikoj većini časno i odgovorno rade

jedan izuzetno težak posao. Valja naglasiti da kod uvođenja ove tehnologije nitko nije posebno vodio brigu o tome što o tome misle ili kako se osjećaju policijski službenici koji će nositi ili nose kamere na prsima. Stoga bi tako nešto u sljedećoj razvojnoj fazi ovog projekta svakako trebalo učiniti. Naime, imajući u vidu sve teškoće policijskog posla i poziva, pritiske kojima su izloženi, evidentno nedovoljnu pravnu i stvarnu zaštitu, plaće koje im ne omogućavaju osnovnu egzistenciju, i drugo, može se pretpostaviti da ovakav projekt doživljavaju kao dodatan teret na svojim plećima[433]. Imajući u vidu sve navedeno, čini se da je opravdan strah da će neki policijski službenici, koji su u konačnici ipak samo ljudi, često satjerani između čekića i nakovnja, potražiti izlaz iz takve situacije na način da će se suzdržati od intervencije koju bi trebali snimati, pučki rečeno okrenuti glavu, a to je najopasnije što se može dogoditi i što u konačnici može dovesti u pitanje sigurnost svih građana. Što se tiče normativnog uređenja članka 3.a Zakona o policijskim poslovima i ovlastima[434], koji ovlašćuje policiju da, u mjeri u kojoj je to potrebno, kao i radi nadzora zakonitosti postupanja policijskih službenika, zvučno i vizualno ili na drugi način snima obavljanje policijskih poslova i primjenu policijskih ovlasti, moglo bi doći do stanovitih preklapanja i kolizija sa zakonima koji uređuju kaznenu i prekršajnu proceduru. Stoga bi to područje bilo potrebno temeljitije urediti i izbalansirati potrebe policijskog posla na koji se poziva članak 3.a s tim propisima.

Brojni upitnici koji lebde nad ovim projektom dopuštaju zaključak da je potrebno dodatno analizirati i preispitati sve segmente projekta, odnosno dobro procijeniti sve njegove posljedice.

4.3. Korištenje prijenosnih računala

Dok sustav prijenosnih kamera može izazvati dvojbe i nedoumice, ovom dijelu projekta e-policije, zamjerka teško da se može naći. Naime, načelno je riječ o zamjeni različitih obrazaca, naloga, notesa, zakonskih propisa i druge „papirnate galanterije“ informatiziranom opremom, tj. tabletom, putem kojeg policijski službenik elektroničkim putem komunicira s bazom, izvješćuje, unosi i pohranjuje sigurnosne događaje, zauzima adekvatne urudžbene brojeve i drugo. Uređaj omogućuje i automatsko upoznavanje s operativno interesantnim događajima, s dnevnim rasporedom te redovnim i posebnim zadaćama; uvid u standardne operativne postupke za pojedine situacije, izbor između standardiziranih obrazaca za sve situacije pred kojima se naći policijski službenik, mogućnost korištenja prevoditelja radi lakše komunikacije sa stranim državljanima te brojne druge aplikacije i mogućnosti koje pruža korištenje informatičke tehnologije. Gotovo da je nepotrebno elaborirati koliko ovakav način rada unaprjeđuje i racionalizira policijsko postupanje, ali valja napomenuti da u značajnoj mjeri umanjuje mogućnost potencijalno koruptivnih situacija. Tako zauzimanje urudžbenog broja na terenu, odnosno unošenje prekršajnog naloga i slično, onemogućava bilo kakvo kasnije manipuliranje, odnosno „malverzaciju“. Također, ostaje u evidenciji gotovo svaki postupak policijskog službenika koji je odrađen uz korištenje tableta, što također ima nemjerljiv preventivni učinak za određene policijske zlouporabe. Slijedom toga, ovu tehnološku novinu na korištenju u policijskom sustavu valja podržati i poželjeti da se i dalje razvija u smjeru olakšavanja policijskih poslova i zadaća, rasterećenja policijskih službenika

[433] Više o položaju policijskih službenika vidi: Mršić, Nadzor nad radom policije; MUP RH, 2016. str. 126-138.
[434] NN 76/09., 92/14.

od svake nepotrebne „papirologije“, ali i adekvatnoj kontroli zakonitog i profesionalnog postupanja.

5. ZAKLJUČAK

Nesumnjivo su kaznena djela najteža djela kojima se povređuju ustavna i konvencijska prava građana, radi kojih države osnivaju i održavaju tijela državne reakcije na takve događaje, među kojima je policija „sama oštrica mača“. Kad kaznena djela čine pripadnici policije, kao službe ustanovljene da štiti te građane i njihova prava, koji zapravo na taj način krše i povređuju ta zaštićena pravna dobra koja bi trebali čuvati i štititi, oni ruše tu zamišljenu idejnu paradigmu i negiraju ideju svojeg postojanja. Život nas uči da nisu potrebne velike brojke da bi se oživotvorilo zlo, i mali brojevi i količine budu dostatni za to. Tako je dovoljna samo kap tinte da bazen bistre vode više ne bude bistar, i da je potreban samo jedan truli krumpir u vreći zdravih krumpira da u dovoljno dugom vremenu u vreći više ne bude ni jednog zdravog krumpira. Na žalost, suprotna formula ne vrijedi, jedna kap bistre vode ne izbistri zamućeni bazen niti jedan zdravi krumpir u vreći trulih ne ozdravi one trule. Stoga i „male brojeve“ policijskih službenika koji se upuštaju u određene delinkvencijske odnose treba uzimati krajnje ozbiljno. Pri tome ne trebamo zapasti u zamku da bi policijski službenici trebali biti nepogrješivi.

Provedeno istraživanje policijske delinkvencije pokazalo je da je 1 043 policijskih službenika u deset godina počinilo 1 566 kaznenih djela, od kojih su neka takve prirode da zvono za uzbunu, ne da zvoni, nego ječi, ali je također usporedba s građanskom populacijom pokazala da su i takvi, višestruko „pošteniji“ od ostatka populacije.

Postavili smo nadalje pitanje, bi li se i u kolikoj mjeri moglo na smanjenje policijske delinkvencije utjecati uvođenjem i uporabom nove tehnologije kod obavljanja policijskih poslova? Izdvojili smo tri tehnološke mjere koje su posljednjih godina uvedene ili se uvode u policijsko postupanje koje imaju ili mogu imati takav naboj odnosno potencijal. Za dvije od tih mjera, geografsko pozicioniranje i uvođenje prijenosnih računala – tableta, našli smo brojne prednosti i antidelinkvencijske potencijale, dok se treća razmatrana mjera, uvođenje prenosivih kamera, pokazala spornom, pa i problematičnom. Naime, pokazalo se da taj tehnološki novitet trenutačno nema značajniji „antidelinkvencijski“ kapacitet, ali otvara mnoga sporna pitanja i dvojbe, što ga u budućnosti može učiniti upitnim.

LITERATURA

Derenčinović, D. (2004). *Uvod u kriminologiju i socijalnu patologiju s osnovama kaznenog prava*. Zagreb: Pravni fakultet Sveučilišta u Zagrebu.

Horvatić, Ž., Novoselec, P. (1999). *Kazneno pravo - opći dio*. Zagreb: MUP RH.

Larry K.G. (2006). *Controlling The Police: The American Experience* (*nadzor policije – američka iskustva*). San Bernardino, CA USA: California State University, Criminal Justice Department.

Mandić, M., Vojković, A.M. (2011). *Policajke kroz povijest - Žene u policiji*. Posebno izdanje MUP Mir, ugled, povjerenje, br. 46(11): 5. Zagreb: MUP RH.

Mršić, Ž. (2006). Je li borba protiv korupcije realnost ili iluzija? *Policija i sigurnost*, br. 3-4.

Mršić, Ž. (2016). *Nadzor nad radom policije*. Zagreb: MUP RH.

Raspis Ravnateljstva policije broj: 511-01-50-72786/17-2'15, od 10. veljače 2016.
Zakon o policijskim poslovima i ovlastima. NN 76/09., 92/14. Zagreb: Narodne novine.
Web-stranica. http://www.dzs.hr/Hrv_Eng/publication/2011/07-01-04_01_2011.htm

Željko Mršić

THE ROLE OF NEW TECHNOLOGIES AND METHODS IN PREVENTION OF CRIMES COMMITTED BY POLICE OFFICERS

Summary

This paper presents the results of investigations of crimes committed by police officers during a ten-year period. A comparison has been made to the crimes committed by the rest of the population. After the unification of the samples, the results of the research have indicated that police officers are still several times less criminally active, i.e. more law-abiding than the rest of the population. Moreover, a new technology that is being introduced into the work of police officers has been considered, and in that sense, three technical measures have been identified which have a certain anti-corruption, i.e. anti-delinquent potential. These measures are: geographical positioning of police officers in the field, the introduction of laptops instead of "paper" equipment, and portable cameras that police officers are wearing. The first two measures are rated as a significant step forward, while the third measure (camera) raises many issues.

Keywords: *police delinquency, prevention, cameras, geographical positioning, laptop.*

STRUČNI RAD

Gojko Pavlović[435]

SUPROTSTAVLJANJE SAJBER KRIMINALU U EVROPSKOJ UNIJI U SVJETLU EVROPSKE BEZBJEDNOSNE AGENDE

Sažetak

U radu se ukazuje na savremene izazove, rizike i prijetnje bezbjednosti Evropske unije u polju unutrašnje bezbjednosti, sa posebnim osvrtom na sajber kriminal. Najprije je predstavljena analiza dosadašnjih dostignuća Evropske unije na sprečavanju ove prijetnje kroz implementaciju Unutrašnje strategije bezbjednosti koje je ostvarivana u periodu 2010.-2014. godine. Strateški ciljevi na čijoj je realizaciji Evropska unija radila u ovom periodu su: podizanje nivoa bezbjednosti za građane i preduzeća u sajber prostoru, rad sa industrijom radi osnaživanja i zaštite građana, poboljšanje sposobnosti za suočavanje sa sajber prijetnjama. Posebna pažnja u radu se posvećuje budućim koracima Evropske unije na sprečavanju ove prijetnje, a koji su predstavljeni u Evropskoj agendi bezbjednosti (2015.-2020), kao strateškom dokumentu Evropske unije u ostvarivanju unutrašnje bezbjednosti.

Ključne riječi: *Evropska unija, bezbjednosne prijetnje, sajber kriminal.*

1. UVODNA RAZMATRANJA

Sajber kriminal[436] kao savremena bezbjednosna prijetnja doživljava svoju ekspanziju. Kao vrste ove prijetnje u literaturi se uglavnom navode: državno-sponzorisani sajber napadi; ideološki i politički ekstremizam; organizovani sajber kriminal i sajber kriminal na nivou pojedinaca (Cornish, Hughes, Livingstone, 2009: 3–11). Takođe, sajber kriminal pokriva širok spektar krivičnih djela, uključujući hakovanje kompjutera, podataka i sistema, kompjuterske prevare, te krivična djela vezana za sadržaj kao što su dječija pornografija i autorska prava (Schreier, Weekes, Winkler, 2010: 9). Međunarodnopravni okvir borbe protiv ovog vida kriminala ogleda se u brojnim dokumentima, rezolucijama i konvencijama koje su usvojile Ujedinjene nacije, Savjet Evrope, Evropska unija i druge organizacije, a koje za cilj imaju upravo borbu protiv sajber kriminala i drugih oblika kriminala povezanih sa njim. Od pravnih instrumenata koji su nastali u okvirima Evropske unije u oblasti borbe protiv sajber kriminala, mogu se izdvojiti Direktiva o pravnoj zaštiti kompjuterskih programa i Direktiva o

[435] Dr. Gojko Pavlović, Asistent na Katedri bezbjednosnih nauka, Visoka škola unutrašnjih poslova, RS, pavlovicgojko@gmail.com, gojko.pavlovic@education.muprs.org

[436] S obzirom na to da se u Konvenciji Savjeta Evrope koristi izraz sajber criminal on je i najzastupljeniji, tj. najviše se koristi. Izrazi „visokotehnološki kriminal“, “kibernetički kriminal” i „sajber kriminal“ imaju isto značenje, u pitanju je samo terminološka razlika (Komlen-Nikolić i dr., 2010: 30).

čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža (Ivetić, Pavlović, 2012: 54-55).[437]

Takođe, kao bitan strategijski instrument u borbi protiv savremenih bezbjednosnih prijetnji EU, potrebno je istaći Evropsku strategiju bezbjednosti koja je usvojena 12. decembra 2003. godine pod nazivom „Bezbjedna Evropa u boljem svijetu".[438] Ovom strategijom su po prvi put uspostavljeni principi i postavljeni jasni ciljevi za unapređenje Evropskih bezbjednosnih interesa. Strategija je organizovana u tri poglavlja, i to: analiza bezbjednosnog okruženja, u kojem su predstavljeni globalni izazovi i ključne prijetnje[439], definisanje tri strateška cilja, od kojih je jedan upravo borba protiv navedenih prijetnji i procjena političkih implikacija za Evropu (Ivetić, Pavlović, 2012: 55).

U izvještaju Havijera Solane pod nazivom „Pružanje bezbjednosti u svijetu koji se mijenja", podnesenom Evropskom savjetu, od 11. decembra 2008. godine, koji u stvari predstavlja Izvještaj o implemenataciji Evropske strategije bezbjednosti iz 2003. godine, naglašava se da izazovi i prijetnje koji su tada identifikovani nisu nestali, već naprotiv, da su postali još složeniji, a pored starih su se javili i neki novi, među kojima je i *sajber kriminalitet* (Javier, 2008: 3–6). Takođe, navodi se i da su navedene prijetnje postale složenije i međusobno povezane, te da bi Evropa u vezi sa tim, tj. da bi bila aktivnija i sposobnija da se nosi sa prijetnjama, morala da razvija podstrategije i akcione planove za sprečavanje navedenih prijetnji (Vasconcelos, 2009: 57).

Tako je, istovremeno sa usvajanjem Lisabonskog ugovora[440] i promjenama koje je ugovor donio na području slobode, bezbjednosti i pravde (ukidanje stubova), 02. decembra 2009. godine usvojen je tzv. Štokholmski program za period od 2010. do 2014. godine.[441] Štokholmski program predstavlja nastavak na Haški program *(Hague Programme*[442] - koji je realizovan u periodu od 2005. do 2010. godine), a u vezi je sa daljim razvojem strateških smjernica i politika razvoja EU na polju unutrašnje bezbjednosti. Kao bitni politički prioriteti na čijoj je realizaciji EU proteklih godina radila, u skladu sa ovim programom, su: promovisanje statusa građanina i osnovnih prava; Evropa prava i pravde; Evropa koja štiti; pristup Evropi u globalizovanom svijetu; Evropa odgovornosti, solidarnosti i partnerstva na području migracija i azila; te Evropa u vrijeme globalizacije, tj. vanjske dimenzije slobode,

---

[437]Council Directive of 14 may 1991 on the Legal Protection of Computer Programs, Directive 91/250/EEC, Official Journal no L 122/42; Directive 2006/24/EC of the European Parliament and of the Council: on the retention of data generated or processed in connection with provision of publicly available electronic communications services or of public communications networks and amending, Directive 2002/58/EC, Official Journal of the European Union, 13. 4. 2006.

[438] European security strategy, A secure Europe in a better world, Brussels, 12 December 2003.

[439] Kao globalni izazovi u strategiji se ističu: siromaštvo, bolesti, migracije, ekološki problemi, nadmetanje za prirodne resurse, posebno vodu, energetska zavisnost i dr., a kao glavne prijetnje se navode: terorizam, profilerizacija oružja za masovno uništenje, regionalni sukobi, neuspjeh država i organizovani kriminalitet (Javier, 2003: 5–9).

[440]Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, Official Journal of the European Communities, 2007/C 306. Potpisan 13. decembra 2007. godine u Lisabonu, a stupio na snagu 1. decembra 2009. godine nakon ratifikacije u svim zemljama članicama Europske unije.

[441]The Stockholm programme — an open and secure Europe serving and protecting citizens, Official Journal of the European Union, 2010/C 115.

[442]The Hague programme: Strengthening freedom, security and justice in the European Union, Official Journal 2005/C 53.

bezbjednosti i pravde (Bilandžić, 2012). Između ostalog, programom je zatraženo da se definiše sveobuhvatna unutrašnja bezbjednosna strategija EU.[443]

2. DOSTIGNUĆA UNUTRAŠNJE BEZBJEDNOSNE STRATEGIJE EU U PERIODU 2010.-2014. GODINE U VEZI SA OSTVARIVANJEM STRATEŠKOG CILJA „PODIZANJE NIVOA ZAŠTITE ZA GRAĐANE I POSLOVNA PREDUZEĆA U SAJBER PROSTORU“

Na osnovu Štokholmskog programa početkom 2010. godine usvojena je najprije Unutrašnja bezbjednosna strategija EU[444], a potom i akcioni plan za njenu realizaciju[445]. Akcionim planom identifikovani su najurgentniji izazovi i prijetnje za bezbjednost EU, te pet strateških ciljeva i po nekoliko konkretnih koraka za svaki od ovih ciljeva, čija je realizacija bila u periodu 2010.–2014. godine.

Pet strateških ciljeva koji su bili definisani ovom strategijom su (Ivetić, Pavlović, 2012: 56)[446]:

1. poremetiti međunarodne kriminalne mreže;
2. prevencija terorizma, radikalizacije i regrutovanja terorista;
3. *podizanje nivoa zaštite za građane i poslovna preduzeća u sajber prostoru*;
4. jačanje bezbjednosti kroz bolje upravljanje granicama i
5. povećanje evropske otpornosti na krize i katastrofe.

U strategiji i akcionom planu se, između ostalog, isticalo da je bezbjednost IT mreže jedan od ključnih faktora za dobro funkcionisanje informacionog društva. Naglašavalo se da su brzi razvoj i primjena novih informacionih tehnologija stvorili nove oblike kriminalnih aktivnosti, kao i da je sajber kriminal globalni fenomen, koji izaziva značajnu štetu unutrašnjem tržištu Evropske unije. Ukazivalo se na to da struktura interneta ne poznaje granice i istovremeno upozoravalo da se nadležnost za krivično gonjenje sajber kriminala zaustavlja na nacionalnim granicama. S tim u vezi su pozivane države članice, ali i druge zemlje, da udruže svoje napore u borbi protiv ovog vida kriminaliteta (European Commission, 2010: 9; Ivetić, Pavlović, 2012: 56-57).

Kao jedan izuzetno značajan korak koji je proistekao iz Unutrašnje bezbjednosne strategije EU jeste razvoj evropskog bezbjednosnog modela, baziranog na načelima i

---

[443] Za realizaciju ove strategije je zadužen Stalni odbor za operativnu saradnju u unutrašnjoj bezbjednost (*The Standing Committee on operational cooperation on internal security - COSI*). Ovaj organ unutar Savjeta nastao je na osnovu člana 71 Lisabonskog ugovora upravo s ciljem jačanja i promovisanja operativne saradnje koja se odnosi na unutrašnju bezbjednost, kao i da olakša saradnju nacionalnih organa država članica u ovom domenu (Čavoški, Reljanović, 2009: 210–211).

[444] *Internal Security Strategy for the European Union: „Towards a European Security Model“*. Bruxeles: Council of European Union, 8.3.2010.

[445] *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe,* COM (2010) 673 final, Brussels, 22.11.2010.

[446] O dostignućima EU u vezi sa ovim ciljevima vidjeti izlaganje sa skupa: Pavlović, G., Ivetić, S., Maričić, G. (2015), Achievements of the European Internal Security Strategy and future challenges of the European Union in the field of Internal security for the period 2015-2020, Presented on International scientific conference *Researching Security: Approaches, Concepts and Policies*, University “St. Kliment OhridskI”, Fakulty of Security – Skopje, Ohrid, Macedonia, 2-3 June 2015.

vrijednostima Evropske unije (Bilandžić, 2012: 60). Taj model daje usmjerenje na integraciju četiri oblasti, i to: policijskog djelovanja *(law enforcement),* pravosudnog djelovanja *(judicial),* kontrolu granice *(border management)* i zaštitu civila *(civil protection),* dok su vrijednosti i načela na osnovu kojih se ovaj model razvio: poštovanje ljudskih prava i osnovnih sloboda, vladavina prava, demokratija, dijalog, tolerancija, transparentnost i solidarnost. Novi evropski model bezbjednosti je centralni okvir kojim Evropska unija nastoji realizovati tzv. integrisani pristup bezbjednosti. Prema ovoj strategiji koncept unutrašnje bezbjednosti objedinjuje više sektora u cilju rješavanja prijetnji koje imaju direktan uticaj na život, bezbjednost i dobrobit građana.

Unutrašnja bezbjednosna strategija EU i akcioni plan za njenu realizaciju su, u vezi sa trećim strateškim ciljem označenim kao "*Podizanje nivoa zaštite za građane i poslovna preduzeća u sajber prostoru*", utvrdili tri ključna pravca djelovanja, i to: jačanje kapaciteta tijela za sprovođenje zakona i pravosudnih tijela; saradnja sa industrijom radi jačanja i zaštite građana; i jačanje sposobnosti za borbu protiv sajber napada (Ivetić, Pavlović, 2012: 56-58).

Koraci koji su bili predviđeni za ispunjavanje ovoga cilja kao i rokovi za njihovo provođenje, te odgovorni subjekti prikazani su u Tabeli 1.

Tabela 1: Koraci Evropske unije u borbi protiv sajber kriminaliteta (European Commission, 2010: 20)

Cilj i koraci	**Odgovorni subjekt**	**Vrijeme**
Cilj 3: Podizanje nivoa bezbjednosti za građane i preduzeća u sajber prostoru		
Korak 1: Izgradnja kapaciteta za primjenu zakona i u pravosuđu		
osnivanje Evropskog centra za sajber kriminal	Subjekti iz studije izvodljivosti Evropske komisije iz 2011. godine	2013.
razvijanje kapaciteta za istrage i krivično gonjenje počinilaca sajber kriminala	Države članice u saradnji sa CEPOLOM, Europolom i Eurojustom	2013.
Korak 2: Rad sa industrijom radi osnaženja i zaštite građana		
uspostavljanje rješenja vezanih za izvještavanja o incidentima povezanim sa sajber kriminalom i pružanje smjernica građanima o sajber bezbjednosti i sajber kriminalu	Države članice, Evropska komisija, Europol, ENISA i privatni sektor	2010.
smjernice o saradnji u rukovanju ilegalnim online sadržajima	Evropska komisija sa državama članicama i privatnim sektorom	2011.
Korak 3: Poboljšati sposobnost za suočavanje sa sajber napadima		
uspostavljanje mreže tzv. *Computer Emergency Response Teams* u svakoj državi članici i jednog tima za institucije Evrpopske unije, kao i nacionalnih rezervnih planova, te vježbi za odgovore i oporavak	Države članice i institucije Evropske unije sa ENISA[447]	2012.
uspostavljanje Evropskog sistema za razmjenu informacija i upozorenja – *European information sharing and alert system* (EISAS)	Države članice sa Evropskom komisijom i ENISA	2013.

[447] ENISA – European Network and Information Security Agency.

U vezi sa ostvarivanjem navedenih ciljeva treba naglasiti najprije da je Evropski centar za borbu protiv sajber kriminala (*The European Cybercrime Centre* - EC3) pri Evropolu počeo sa radom 2013. godine. EC3 je centralna tačka za sva pitanja povezana sa sajber kriminalom i po tom osnovu ostvaruje saradnju sa državama članicama, Eurojustom, kao i trećim zemljama u vezi sa krivičnim istragama. Također, sarađuje i sa privatnim sektorom putem savjetodavnih grupa o internetskoj bezbjednosti i financijskim uslugama.

Takođe, EU je usvojila Direktivu o napadima na informacione sisteme[448] kojom se usklađuje kazneno pravo država članica u vezi sa tim krivičnim djelima (npr. o nezakonitom pristupu informacionim sistemima, nezakonitom ometanju sistema i podataka i nezakonitom presretanju), te olakšava saradnja između agencija i tijela za sprovođenje zakona.

Nadalje, početkom 2013. godine usvojena je Strategija EU za sajber bezbjednost[449], u kojoj se, između ostalog, naglašava važnost saradnje između javnog i privatnog sektora u cilju jačanja prevencije i bezbjednosti uopšte. Također je predloženo donošenje Direktive o mrežnoj i informacijskoj bezbjednosti[450] a čiji je cilj jačanje nacionalne otpornosti i povećanje saradnje u slučaju sajber napada.

Krajem 2012. godine osnovan je stalni CERT tim za EU (*Emergency Computer Response Team* - CERT-EU), odnosno za EU institucije, agencije i tijela. Tim se sastoji od IT stručnjaka za bezbjednost iz glavnih institucija EU (Evropske komisije, Generalnog sekretarijata Vijeća EU, Evropskog parlamenta, Odbora regija, Ekonomskog i socijalnog odbora). Tim blisko sarađuje sa drugim CERT timovima u državama članicama i šire, kao i sa specijalizovanim IT bezbjednosnim kompanijama.[451] Urađena je studija izvodljivosti o uspostavljanju Evropskog sistema za razmjenu informacija i upozorenja (*European information sharing and alert system* - EISAS) izvan okvira ENISA.[452]

Nastavljena je promocija Konvencije iz Budimpešte o sajber kriminalu, kao pravnog okvira za međunarodnu saradnju u borbi protiv ove vrste kriminala i kao modela za nacionalne zakone. Tokom 2012. godine, u saradnji sa SAD, pokrenut je Svjetski savez za suzbijanje seksualnog zlostavljanja djece na internetu. Ovaj Savez trenutno okuplja oko 50 zemalja koje rade na poboljšanju identifikacije žrtava, krivičnom progonu počinitelja, jačanju svijesti i smanjenju količine pornografskog materijala dostupnog na internetu (*The final implementation report of the EU Internal Security Strategy*, 2014: 7–8).

---

[448] *Directive on attacks against information systems,* Directive 2013/40/EU.
[449] *The Cybersecurity Strategy for the EU,* JOIN(2013) 1, 07.02.2013.
[450] *Directive on network and information security,* COM(2013) 48.
[451] https://cert.europa.eu/cert/plainedition/en/cert_about.html, Pristup: 18. 2. 2016. godine u 11.30.
[452] https://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas-deployment-feasibility-study, Pristup: 18.02.2016. godine

3. BUDUĆI IZAZOVI EU NA POLJU UNUTRAŠNJE BEZBJEDNOSTI ZA PERIOD 2015.-2020. GODINE

EU je usvajanjem Unutrašnje strategije bezbjednosti i njenom dosljednom realizacijom kroz Akcioni plan, u periodu 2010.-2014. godine, u mnogome unaprijedila svoje, u ranijem periodu, projektovane normativne i institucionalne kapacitete za upravljanje bezbjednosnim izazovima, rizicima i prijetnjama na polju unutrašnje bezbjednosti. Kao logičan nastavak daljnjih planskih aktivnosti EU, u ovoj oblasti, nametnula se potreba ponovnog donošenja nove Unutrašnje strategije bezbjednosti za period 2015.-2020. godine[453].

S tim u vezi, u martu 2014. godine je uspostavljena komunikacija Evropske komisije sa relevantnim subjektima EU te je izrađen dokument pod nazivom „Put ka ostvarenju otvorene i bezbjedne Evrope“[454], a potom su u junu iste godine usvojene „Strateške smjernice za zakonodavno i operativno planiranje u području slobode, bezbjednosti i pravde”[455]. Nadalje su, do kraja 2014. godine, usvojeni “Zaključci Savjeta EU o razvoju obnovljene EU unutrašnje strategije bezbjednosti”[456], kao i “Rezolucija Evropskog Parlamenta”[457] o ovoj temi.

U ovim dokumentima se, između ostalog, naglašava da je jedan od ključnih ciljeva EU izgradnja područja slobode, bezbjednosti i pravde uz potpuno poštovanje osnovnih prava građana. Prioritet je pronaći način kako efikasno konsolidovati i dosljedno sprovoditi postojeće pravne instrumente i mjere iz politika u oblasti azila, imigracije, granica, te policijske i pravosudne saradnje. Od ključne važnosti će biti jačanje operativne saradnje, uz iskorištavanje potencijala inovacija u području informacionih i komunikacionih tehnologija, poboljšanje uloga različitih agencija EU, kao i obezbjeđenje strateške upotrebe fondova EU (Strategic guidelines in the area of internal security, 2014:1–2).

Na osnovu svih navedenih dokumenata u aprilu 2015. godine usvojena je Evropska agenda bezbjednosti kao budući strateški dokument u oblasti unutrašnje bezbjednosti za period od 2015. do 2020. godine.[458] Evropska agenda bezbjednosti je zajednički program država članica i institucija EU koja služi kao osnov saradnje i njihovog zajedničkog djelovanja. Ovom agendom policiji i drugim agencijama za sprovođenje zakona u državama članicama nastoji se olakšati razmjena podataka, kao i uspostaviti bolja operativna saradnja u borbi protiv savremenih prijetnji bezbjednosti. Agenda se zasniva na pet načela: obezbjeđenju potpunog ostvarivanja ljudskih prava; transparentnosti, odgovornosti i demokratskoj kontroli s ciljem ostvarivanja povjerenja građana; boljoj primjeni postojećih EU pravnih instrumenata;

---

[453] Vidjeti: Pavlović, G., Đurovski, M. (2015), Izgradnja zajedničke unutrašnje bezbjednosti EU (Evropska bezbjednosna agenda 2015.-2020.), Izlaganje sa Međunarodne naučne konferencije *Srbija i Evropska unija – pripreme za pregovore o poglavljima 23. i 24*, Institut za međunarodnu politiku i privredu, Hans Zajdel fondacija, Beograd, Republika Srbija, 29.-30. septembra 2015. godine.

[454] *An open and secure Europe: making it happen*, COM(2014) 154 final, Brussels, 11. 3. 2014.

[455] *Strategic guidelines in the area of internal security*, EUCO 79/14, European Council, Brussels, 27.6.2014.

[456] *Draft Council conclusions on the development of a renewed European Union Internal Security Strategy*, 15670/14, Council of the European Union, Brussels, 19.11.2014.

[457] *European Parliament resolution on renewing the EU Internal Security Strategy*, (2014/2918(RSP)), Brussels, 17.12.2014.

[458] *The European Agenda on Security*, COM(2015) 185 final, European Commission, Strasbourg, 28.4.2015.

uspostavljanju među-agencijskog i među-sektorskog pristupa u radu; i povezivanju svih unutrašnjih i spoljašnjih dimenzija bezbjednosti. Pri tome su agendom istaknuta tri strateška cilja, tj. prioriteta kojima će se EU u budućnosti baviti, a to su: terorizam i pojava stranih boraca terorista; organizovani i prekogranični kriminal; i sajber kriminal (Đurovski, Pavlović, 2015: 6).

Koraci EU na sprečavanju sajber kriminala, tj. trećeg strateškog cilja, su (The European Agenda on Security, 2015: 19–20):

- stavljanje akcenta na sprovođenje postojećih politika EU u oblasti sajber kriminala (naročito kada je u pitanju napad na informacione sisteme i borba protiv seksualnog iskorišćavanja djece);
- razmatranje i eventualno proširenje zakonodavstva o borbi protiv prevara i falsifikovanja bezgotovinskih sredstava plaćanja (noviji oblik kriminala; falsifikovanja u finansijskim instrumentima sa prijedlozima u 2016. godine);
- otklanjanje prepreka u krivičnim istragama o sajber kriminalu (posebno o pitanjima o nadležnosti i pravila o pristupu dokazima i informacijama);
- izgradnja sajber kapaciteta pod instrumentima spoljne politike EU.

Evropska agenda bezbjednosti je propisala korake koje je potrebno preduzeti na sprečavanju sajber kriminala, odnosno na dostizanju visokog nivoa unutrašnje bezbjednosti EU. Međutim, njeno uspješno sprovođenje zavisi prije svega od političke volje svih aktera koji učestvuju u njenoj realizaciji, odnosno od njihove međusobno dobre saradnje. Agenda prestavlja osnovu za takvu saradnju i za zajedničke akcije unutar EU.

4. ZAKLJUČNA RAZMATRANJA

Potrebu da se adekvatna pažnja posveti pravnoj i institucionalnoj borbi protiv sajber kriminala EU je davno prepoznata. S tim u vezi, je krajem 2010. godine usvojena tzv. Unutrašnja bezbjednosna strategija, u kojoj je kao jedan od ključnih ciljeva navedena upravo pravna i institucionalna izgradnja kapaciteta u okviru EU, ali i država članica na sprečavanju savremenih bezbjednosnih izazova, rizika i prijetnji. Dosljednom realizacijom predviđenih aktivnosti EU je u mnogome unaprijedila svoje normativne i institucionalne kapacitete za suprotstavljanje izazovima, rizicima i prijetnjama na polju unutrašnje bezbjednosti, a posebno u odnosu na sajber kriminal.

EU je dio globalizovanog i međusobno povezanog svijeta u kojem se očekuje povećanje međunarodne mobilnosti. Tako se EU već sada suočava sa demografskim promjenama, sve različitijim društvima, ali istovremeno i nestašicama na tržištu rada. Zbog toga se planira maksimalno korišćenje politika u području unutrašnjih poslova koje treba da utiču, između ostalog, na podsticanje privrednog rasta i privlačenje u EU obrazovanih kadrova. Pitanja unutrašnjih poslova će biti ugrađena u opštu spoljnu politiku EU, a time će se omogućiti i snažnija saradnja sa trećim zemljama.

S tim u vezi bi Bosna i Hercegovina, u skladu sa svojim ustavnim uređenjem, trebala da preduzme aktivnosti na usklađivanju zakonodavstva s pravnim tekovinama (*Acquis Communautaire*) EU, između ostalog, i na polju unutrašnje bezbjednosti. Ovo posebno imajući u vidu Stupanje na snagu Sporazuma o stabilizaciji i pridruživanju, u kojem je u poglavlju VII. Pravda, sloboda i sigurnost, u članu 84. Sprečavanje i borba protiv organizovanog kriminala i drugih nezakonitih aktivnosti, stav 1. tačka (j) kompjuterski kriminal taksativno naveden kao oblast zajedničke saradnje u sklopu koje će se promovisati regionalna saradnja i poštovanje međunarodnih standarda.

Jedna od oblasti koja će se morati dodatno unaprijediti u budućnosti jeste svakako pravni sistem koji treba da pruži podršku policijskim i pravosudnim tijelima u istragama sajber kriminala, prvenstveno kroz propisivanje novih, različitih krivičnih djela sajber kriminala, kao i sankcija za njih, te usaglašavanja pravne prakse sudova u primjeni zakona na krivična djela ove vrste. Istovremeno, potrebno je raditi na razvoju institucionalnih kapaciteta po uzoru na EU, a koji su neophodni za prevenciju predstavljenih bezbjednosnih izazova, rizika i prijetnji. Posebna pažnja se mora posvetiti dodatnoj edukaciji i usavršavanju zaposlenih u ovoj oblasti, ali i građana uopšte, kao i opremanju visokosofisticiranom opremom koja može zadovoljiti tehničke standarde i uslove za borbu protiv ovog vida kriminaliteta.

LITERATURA

Bilandžić, M. (2012). Prema strategiji „nacionalne“ sigurnosti Europske unije? - Analiza Strategije unutarnje sigurnosti Europske unije. *Policija i Sigurnost, 21* (1), 49–69.

Cornish, P., Hughes, R., Livingstone, D. (2009). *Cyberspace and the National Security of the United Kingdom – Threats and Responses*. London: Royal Institute of International Affairs.Chatham House Report.

Čavoški, A., Reljanović, M. (2009). *Pravosuđe i unutrašnji poslovi u Evropskoj uniji*. Beograd: Pravni fakultet Univerziteta Union i Službeni glasnik.

Đurovski, M., Pavlović, G. (2015). Dostignuća Evropske unutrašnje strategije bezbjednosti (2010–2014) i budući izazovi Evropske unije (2015–2020) na polju borbe protiv terorizma. u: Zborniku radova *Suprotstavljanje savremenim oblicima kriminaliteta – analiza stanja, evropski standardi i mere za unapređenje, Tom 2*. Beograd: Kriminalističko-policijska akademija i Hans Zajdel fondacija, 1–8.

Ivetić, S., Pavlović, G. (2012). Borba protiv sajber kriminala u Evropskoj Uniji sa osvrtom na Republiku Srpsku. u: Zborniku radova *Suzbijanje kriminala i evropske integracije sa osvrtom na visokotehnološki kriminalitet*. Laktaši: Visoka škola unutrašnjih poslova i Hans Zajdel fondacija, 53–64.

Javier, S. (2003). *A safer Europe in a better world, European security strategy*. Brussels: European Commission.

Javier, S. (2008). *Report on the Implementation of the European Security Strategy, Providing Security in a Changing World (S407/08)*. Brussels: European Council.

Komlen-Nikolić, L., Gvozdenović, R., Radulović, S., Milosavljević, A., Jerković, R., Živković, V., Živanović, S., Reljanović, M., Aleksić (2010). *Suzbijanje visokotehnološkog kriminala*. Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije.

Pavlović, G., Ivetić, S., Maričić, G. (2015). Achievements of the European Internal Security Strategy and future challenges of the European Union in the field of Internal security for the period 2015-2020. Presented on International scientific conference *Researching Security:*

Approaches, Concepts and Policies, University "St. Kliment OhridskI", Fakulty of Security – Skopje, Ohrid, Macedonia, 2-3 June 2015.
Pavlović, G., Đurovski, M. (2015). Izgradnja zajedničke unutrašnje bezbjednosti EU (Evropska bezbjednosna agenda 2015.-2020.). Izlaganje sa Međunarodne naučne konferencije *Srbija i Evropska unija – pripreme za pregovore o poglavljima 23. i 24*, Institut za međunarodnu politiku i privredu, Hans Zajdel fondacija, Beograd, Republika Srbija, 29.-30. septembra 2015. godine.
Schreier, F., Weekes, B., Winkler, T. (2010). *Cyber Security: The Road Ahead*. Geneva: DCAF.
Vasconcelos, Á. ed., (2009). *The European security strategy 2003–2008, Building on common interests - Report No. 05*. Paris: European Union Institute for Security Studies.
*** (2003). *European Security Strategy, A Secure Europe in a Better World*, Brussels, 12. 12.2003.
*** (2007). *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community*, Official Journal of the European Communities, 2007/C 306.
*** (2009). *The Stockholm programme — an open and secure Europe serving and protecting citizens*, Official Journal of the European Union, 2010/C 115.
*** (2010). *Internal Security Strategy for the European Union: „Towards a European Security Model"*. Bruxeles: Council of European Union, 8. 3. 2010.
*** (2010). *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, COM (2010) 673 final, Brussels, 22. 11. 2010.
*** (2014). *The final implementation report of the EU Internal Security Strategy 2010-2014*, COM(2014) 365, Brussels, 20. 6. 2014.
*** (2014). *An open and secure Europe: making it happen*, COM(2014) 154 final, Brussels, 11. 3. 2014.
*** (2014). *Strategic guidelines in the area of internal security*, EUCO 79/14, Brussels: European Council, 27. 6. 2014.
*** (2014). *Draft Council conclusions on the development of a renewed European Union Internal Security Strategy*, 15670/14, Brussels: Council of the European Union, 19. 11. 2014.
*** (2014). *European Parliament resolution on renewing the EU Internal Security Strategy*, (2014/2918(RSP)), Brussels, 17. 12. 2014.
*** (2015). *The European Agenda on Security*, COM(2015) 185 final, Strasbourg: European Commission, 28. 4. 2015.

Gojko Pavlović

COMBATING CYBERCRIME IN THE EUROPEAN UNION IN RELATION TO THE EUROPEAN AGENDA ON SECURITY

Summary

This paper points to the contemporary security challenges, risks and threats to the European Union in the field of internal security, with particular emphasis on cybercrime. First, it provides an analysis of the European Union achievements in the field of countering this threat through the implementation of the Internal Security Strategy of the European Union in the period 2010 to 2014. The strategic objectives that the European Union has worked on in this period are the following: strengthening the capacity of law enforcement and judicial bodies; cooperation with the industry to strengthen the protection of citizens; and strengthening capacity to combat cyber-attacks. Special attention is paid to future actions of the European Union to counter this type of security threat, which are presented in the European Agenda on Security (2015-2020) as a strategic document of the European Union in achieving homeland security.

Key words: *European Union, security threats, cybercrime.*

PREGLEDNI ZNANSTVENI RAD

Damir Kulišić[459]

O AKTUALNIM MOGUĆNOSTIMA I PROBLEMIMA PROTUEKSPLOZIJSKE DETEKCIJE I IDENTIFIKACIJE EKSPLOZIVNIH TVARI/NAPRAVA

Sažetak

Sigurnosno protueksplozijsko, kao i kriminalističko (prijeeksplozijsko ili posteksplozijsko), otkrivanje, prepoznavanje i forenzično dokazivanje vrste i podrijetla (rabljenih sirovina za izradu) eksplozivne tvari i inih sastavnica strukture eksplozivne naprave, u sklopu mnogobrojnih zločinačkim eksplozijskim napadima potencijalno ugroženih, odnosno napadanih, (skupina) osoba, građevina, javnih prostora i prijevoznih sredstava, oduvijek je tvorilo poseban taktički i tehnički izazov, čak i za tehnički dobro opremljene, stručno obrazovane, uvježbane i vrlo iskusne djelatnike službi protueksplozijske/protudiverzijske sigurnosti, obrane i zaštite, a nerijetko i za timove u vještačenje predmeta/tragova takve vrste kaznenog djela uključenih forenzičara. Na osnovi raščlambe sadržaja dostupne suvremene inozemne i domaće stručne literature iz područja taktike i tehnike protueksplozijske detekcije, prijeeksplozijske i posteksplozijske identifikacije eksplozivnih naprava/tvari, izrađen je sažet pregled sigurnosno, istražno i dokazno važnih mogućih vrsta, oblika i inačica takvih vrsta naprava/tvari, pregled suvremeno rabljene i razvijane tehnike za protueksplozijsku detekciju eksplozivnih naprava/tvari, kao i pregled aktualno prepoznatih ključnih problema/čimbenika koji mogu skoro posve onemogućiti ili bitno umanjiti djelotvornost sustava protueksplozijske sigurnosti, obrane i zaštite, odnosno djelotvornost prijeeksplozijske ili posteksplozijske identifikacije vrsta i podrijetla zlorabljenih eksplozivnih tvari i pojedinih sastavnica mogućih konstrukcija zlorabljenih eksplozivnih naprava. Rad je prilog nužnom proširivanju i produbljivanju stručnih znanja, kako u svih djelatnika službi sigurnosti i zaštite tako i u kriminalista i forenzičara novaka, poglavito u svim terorističkim bombaškim kampanjama diljem svijeta i/ili u našem okružju vrlo bremenitim vremenima.

Ključne riječi: *kemijske eksplozije u kondenziranoj fazi, improvizirane eksplozivne naprave, eksplozivne tvari, protueksplozijska detekcija, identifikacija eksplozivnih tvari/naprava, forenzika eksplozivnih tvari/naprava.*

[459] Mr. sc. Damir Kulišćić, Policijska akademija MUP-a RH, Visoka policijska škola, nastavnik – vanjski suradnik, e-mail: dkulisic@fkz.hr

1. UVOD

Francuski znanstvenik Pierre Curie (1859.–1906.), jedan od troje zajedničkih dobitnika Nobelove nagrade za fiziku 1903. g.,[460] prilikom prigodnog govora u Stockholmu, proročki je (više od 40 godina prije eksplozije atomske bombe u Hirošimi) javno iskazao svoju veliku zabrinutost glede mogućnosti da plodovi znanstvenih otkrića budu zlorabljeni: "Pitam se je li korisno dopustiti čovjeku saznati sve tajne prirode. Ja sam jedan od onih, poput Alfreda Nobela, koji se pitaju hoće li buduća otkrića donijeti čovječanstvu više dobra nego li zla. … Pronalasci Alfreda Nobela su znakoviti; snažni eksplozivi mogu pomoći čovjeku u izvedbi zadaća dostojnih divljenja. Oni su, također, sredstvo za zastrašujuća razaranja u rukama velikih zločinaca“ (Demortier, 2003., 120.).

Može se reći kako suvremeni, eksponencijalno rastući broj otkrića, pronalazaka i inovacija u mnogim područjima suvremene znanosti i tehnologije, pored jednako brzo rastućih mogućnosti (pa i već mnogobrojnih primjera) njihove zločinačke zloporabe, realno omogućuje i postizanje iznimno visokih razina sigurnosti, obrane i zaštite i od mnoštva suvremenih pogibelji takve naravi. Unatoč aktualnoj, sve učestalijoj terorističkoj i inoj organizirano kriminalnoj i individualnoj zločinačkoj uporabi eksplozivnih naprava, tomu na putu stoje dvije ključne, aktualno sve teže savladive, prepreke:

- skromna/ograničena raspoloživa financijska/proračunska sredstava za takve namjene i
- stanovita zakonska ograničenja za primjenu mnogih vrsta takvih tehnika/tehnoloških rješenja ili nepostojanje znanstveno provjerenih i propisanih kriterija za njihovu dovoljno sigurnu primjenu, posebice s motrišta njihova možebitnog/izvjesnog škodljivog utjecaja na ljudsko zdravlje ili glede lako moguće zloporabe, posebice u smislu mogućeg nekontroliranog kršenja prava na privatnost i nekih inih zakonom štićenih ljudskih prava od strane sigurnosno-obavještajnih službi, korporacijskih i inih privatnih službi protuobavještajne, tjelesne i tehničke sigurnosti i zaštite, ili od strane za sigurnosni nadzor nepovlasnih detektivskih agencija i inih osoba.[461]

Zbog ratova koji se vode ili su nedavno vođeni na području Bliskog i Srednjeg istoka, na sjeveru i u unutarnjosti afričkog kontinenta, masovnih migracija stanovništva iz tih područja prema zemljama EU i zbog djelatnog izravnog ili posrednog vojnog i političkog sudioništva američkih i europskih čimbenika u tim sukobima, sve više raste pogibelj od još organiziranijih, taktički i bojno još spektakularnijih i/ili smrtonosnijih (samoubilačkih) terorističkih napada vatrenim oružjem i/ili eksplozivnim,[462] zapaljivim, otrovnim, biološki ili

[460] Dodijeljena je ujedno i njegovoj supruzi, glasovitoj znanstvenici poljskog podrijetla, Mariji Curie-Sklodowskoj (1867.-1934.), te francuskom znanstveniku Henriju A. Becquerelu (1852. -1908.).

[461] Suvremeni primjer spomenutih sigurnosnih ograničenja/zabrinutosti u području protueksplozijske sigurnosti je razvitak i primjena *terahertz* (THz) *tehnologije* koja inače omogućuje vrlo kvalitetno skeniranje površine tijela osoba i pouzdano otkrivanje, pod odjećom ili unutar prtljage i raznovrsnih pakiranja, skrivenih predmeta poput pakiranja naboja eksploziva, konstrukcija eksplozivnih naprava, pakiranja droge i bilo kakvog možebitnog oružja izrađenog od nemetalnih materijala, kojeg ne mogu otkriti detektori metala [Cutolo i Mignani (ur.), 2014.,vii]. Slično vrijedi i za tehnologiju analize *rendgenskim zrakama* tipa *povratnog raspršenja* (vidi detaljnije u Sk. a., 2015.).

[462] Vrh liste najstrašnijih modusa operandi (MOS) terorističke taktike čvrsto drže *samoubilački bombaški napadi*. Procjenjuje se kako se u razdoblju između 1981. i 2015. g. u svijetu dogodilo oko 5.000 napada takve vrste, u više od 40 zemalja, uzrokujući smrt oko 50.000 osoba. Prosječna čestina (frekvencija) takvih napada u svijetu

radiološki opasnim sredstvima ili putem aktiviranja/ispuštanja takvih opasnih tvari u sklopu istraživačkih, procesnih, skladištenih ili transportiranih jedinica/pogona na ozemlju vojno-politički ili gospodarski utjecajnijih članica EU, kao i na ozemlju njoj istočnih, politički (možebitno) nestabilnijih susjednih država, suočenih s dugogodišnjim (prikrivenim ili privremeno prigušenim) zaoštravanjem međudržavnih, međunacionalnih i/ili međureligijskih odnosa.[463] Vrlo vjerojatno poput onih eksplozijskih, paležnih i/ili vatrenim oružjem izvedenih, primjerice, na američki zrakoplov iznad škotskog Lockerbiea (1988. g.), u New Yorku (1993. i 2001. g.), u Oklahoma Cityju (1995. g.), u Dahranu (1996. g.), na razarač SAD-a „Cole" i francuski supertanker „Limburg" u Adenskom zaljevu (2000. g.), u Kuti, na Baliju (2002. g.), u Moskvi, Dagestanu i Čečeniji (1999., 2003., 2010. i 2011. g.), u Madridu (2004. g.), u Londonu (2005. g.), u Mumbaiu (2008. g.), u vlaku između Moskve i Petrograda (2009. g.), u Kampali (2010. g.), u Nairobiju i Volgogradu (2013. g.), u Oslu i na otoku Utøya (2011. g.), u Bostonu (2013. g.), u Tunisu, Kuvajtu, Keniji i Parizu (tijekom 2015. g.), na ruski zrakoplov iznad Sinaja (2015. g.), u Istanbulu i Ankari (tijekom 2003., 2015. i 2016. g.), u Bruxellesu i na Uskrs u pakistanskom Lahoreu (2016. g.) itd.[464]

Suvremena *koncepcija sučeljavanja s prijetnjama suvremenog terorizma*, koju se, s više ili manje uspjeha, aktualno pokušava primijeniti u pojedinim dijelovima svijeta, zasniva se na: (1) *društvenoj prevenciji pojavnosti* (eliminiranju uzroka terorizma djelovanjem na same korijene fenomena terorizma); (2) *defenzivnom djelovanju* (*antiterorizmu*), tj. smanjivanjem izloženosti terorističkim napadima, izbjegavanjem terorističkih napada, smanjivanjem ranjivosti na terorističke napade i ublažavanjem učinaka i posljedica eventualno izvedenih napada i (3) *ofenzivnom djelovanju* (*protuterorizmu*), tj. sprječavanjem izvedbe terorističkih napada, odvraćanjem od napada, odbijanjem poduzetih pokušaja napada te uhićenjem ili bojnim eliminiranjem terorista ili njihove organizacije.

Suvremena *tehnologija defenzivnog djelovanja* obuhvaća: (1) *prikupljanje i upravljanje informacijama* metodama i tehnikama nadzora te procedurama koje službama nacionalne sigurnosti, obrane i zaštite omogućuju: pribavljanje informacija o ekstremistima, teroristima i njihovim jatacima te društvenim/medijskim i političkim podupirateljima, o njihovu kretanju i ponašanju, o izvorima njihova financiranja i opskrbe oružjem, o rabljenim skrovištima i prijevoznim sredstvima; nadziranje kritično važnih objekata, prostora i osoba (uključujući

---

pokazuje eksponencijalan rast, od prosječno tri napada godišnje 1980-ih godina do jednog napada mjesečno 1990-ih, pa sve do jednog napada tjedno u razdoblju od 2001. do 2003. g. te već po jednog dnevno u razdoblju od 2003. do 2015. g. Analitičari terorizma tvrde kako se ova napadajna taktička inačica terorizma sve šire usvaja i rabi jer generira (dovoljno) velik unutardržavni i svjetski publicitet, ne zahtijeva previše visokostručnog znanja, materijalnih resursa i truda oko planiranja, i što je vjerojatno najvažnije, skoro nemoguće ju je *defenzivnim* i *ofenzivnim mjerama, aktivnostima* i aktualno raspoloživim *sredstvima prevenirati* (vidi *Domestic Preparedness Journal,* March 01, 2016).

[463] Nadovezujući se na nešto ranije dano slično upozorenje sigurnosno-obavještajnih službi NATO-a i Europol je 25. siječnja 2016. izdao priopćenje prema kojemu bi Islamska država i njima skloni lokalni ekstremisti mogli vrlo vjerojatno izvesti nove terorističke napade u državama članicama EU-a koji bi 'ponajprije mogli biti usmjereni na civilne mete, zbog posljedica koje bi imali', oslanjajući se na zajednicu od oko 5.000 europskih građana koji su se bojno usavršili sudjelujući u sukobu u Siriji i Iraku i lokalno radikaliziranih osoba koje dobro poznaju teren (parafrazirano prema izvješću Hine).

[464] Pritom su izostavljeni primjeri skoro bezbrojnih slučajeva terorističkih napada s velikim brojem žrtava u područjima trajnijih ratnih i gerilskih sukoba. Prema zadnjem javnom priopćenju JIEDDO COIC MID iz kolovoza 2012. g. ("Global IED monthly summary report"), samo u razdoblju od 2008. do 2011. g., napadi eksplozivnim sredstvima u Afganistanu su ranili ili usmrtili skoro 10.000 vojnika SAD-a, a diljem svijeta su od eksplozija eksplozivnih naprava mjesečno ginule prosječno 310 i bivale ozlijeđene 833 osobe.

nadzor državne granice); otkrivanje mjesta skrivanja oružja i terorističkih aktivnosti u tijeku te obradu, distribuciju, stalno ažuriranje i pohranu informacija;[465] (2) *preventivno djelovanje* uz pomoć raspoloživih metoda i tehnika za prevenciju terorističkih napada, poput onih za prevenciju/sprječavanje mogućnosti uporabe pojedinih vrsta terorističkog oružja te tehnika i procedura za onemogućavanje pristupa novcu, oružju, lako zlorabivim tehnologijama i znanjima; (3) *odvraćanje od poduzimanja napada* uz pomoć raspoloživih metoda, tehnika i snaga za ojačavanje otpornosti lako mogućih meta napada;[466] (4) *djelotvoran odgovor na napad* raspoloživim snagama, metodama i tehnikama prevencije posljedica terorističkih napada;[467] (5) *učinkovitu kriminalističku istragu*, primjenom takve taktike i tehnike istraživanja koja omogućuje što brže i forenzično što pouzdanije otkrivanje i uhićenje svih počinitelja i organizatora terorističkih napada[468] (Kulišić, 2007.; Jackson i dr., 2007., 4-6.).
Za što djelotvornije *preventivno defenzivno djelovanje* u području protueksplozijske i ukupne protudiverzijske sigurnosti, obrane i zaštite te za što učinkovitiju *kriminalističku istragu* nužno je, pored ostalog, i što bolje poznavanje detekcijski i identifikacijski važnih obilježja mogućih inačica konstrukcija eksplozivnih naprava i njihovih sastavnica, mogućih načina ili sredstava izvedbe eksplozijskih napada, kao i uporabno važnih obilježja (prednosti i nedostataka), uvjeta i mogućnosti primjene raspoloživih metoda i tehnika za prijeeksplozijsko otkrivanje i identifikaciju eksplozivnih naprava/tvari te svih onih pogodnih za poslijeeksplozijsku detekciju i forenzičnu identifikaciju njihovih ostataka.

[465] Preporučane i već uspješno iskušane i rabljene suvremene taktičke inačice, metode i tehnike nadzora vidi primjerice u radovima Havens et al., 2016., Petersen, 2013. i Sk. a., 2007.

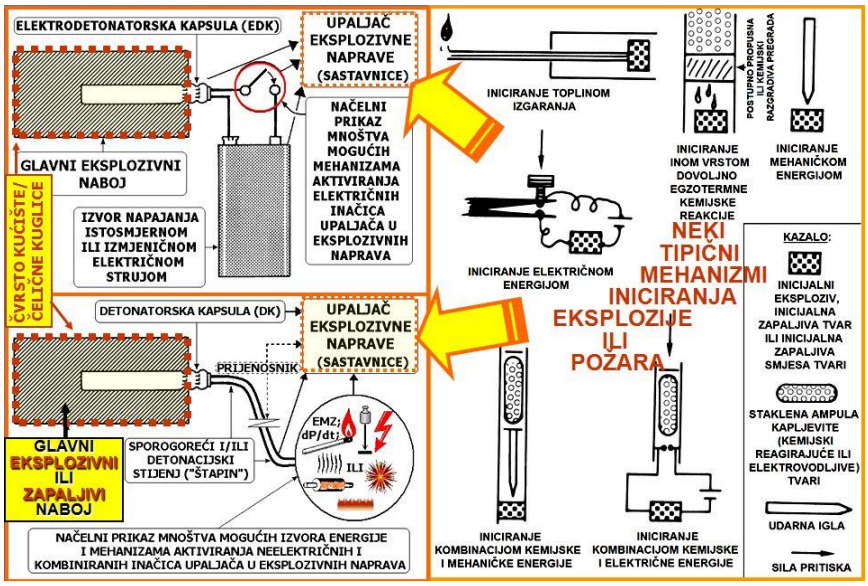
[466] Primjerice, primjenom sigurnosnih udaljenosti/otežavanjem pristupa mogućoj meti napada izvedbom daljinski podižućih protuprodornih cestovnih pristupnih čeličnih rampi ili stupova, izvedbom protueksplozijskih pregradnih/zaštitnih zidova, oblaganjem i ostakljenjem građevina i vozila proizvodima u stanovitoj mjeri otpornima na zrna streljiva, kumulativne projektile i na udarni zračni val eksplozije, povećanjem robusnosti infrastrukturnih objekata i instalacija, ojačavanjem morala pučanstva (psihološkim pripremama, cijepljenjem, uvježbavanjem u sklanjanju, samospašavanju i pružanju pomoći najugroženijima) i raspoređivanjem zadaćama primjereno uvježbanih i opremljenih snaga sigurnosti, obrane i zaštite (glede mjera sigurnosti i zaštite „mekih meta“ vidi npr. Hesterman, 2015.).

[467] Kao što je: žurna i djelotvorna uporaba uvježbanih i dobro opremljenih timova specijalne policije te stručnjaka protueksplozijske ili radiološke, kemijske i biološke (RKB) zaštite; žurna i djelotvorna uporaba uvježbanih i dobro opremljenih timova hitne medicinske pomoći i timova za spašavanje iz ruševina i njihovo uklanjanje; djelotvorna koordinacija svih aktivnosti na mjestu događaja; osigurane količine antidota, antibiotika i ostalih sredstava za pružanje hitne medicinske pomoći ugroženim/ozlijeđenim osobama; pravodobno i djelotvorno informiranje javnosti radi onemogućavanja daljnjih štetnih posljedica i ublažavanja psiholoških učinaka napada.

[468] Ponajprije žurnom, taktički i operativno djelotvornom uporabom iskusnih, uvježbanih i dobro opremljenih timova forenzičara, kriminalista i ostalih vrsta istražitelja (vidi npr. MUP RH, 2010., 97-104.; MUP RH, 2005.; Sk. a., 2012.; Thurman, 2006.) te žurnom i djelotvornom uporabom obavještajnih, redarstvenih, diplomatskih i ostalih metoda progona za onemogućavanje daljnjeg opstanka i neometanog funkcioniranja preostalih članova terorističke organizacije i pripadnika njihove djelatne potpore.

2. O DETEKCIJSKI I IDENTIFIKACIJSKI ZNAKOVITIM OBILJEŽJIMA MOGUĆIH KONSTRUKCIJA EKSPLOZIVNIH NAPRAVA, NJIHOVIH SASTAVNICAMA TE MOGUĆIH NAČINA I SREDSTAVA IZVEDBE EKSPLOZIJSKIH NAPADA

Općenito, prema vrsti izrade, razlikujemo tri osnovne vrste eksplozivnih naprava (EN): *vojno-formacijske eksplozivne naprave* (VFEN), *improvizirane eksplozivne naprave* (IEN) i eksplozivne naprave specijalne namjene, tj. *specijalne eksplozivne naprave* (SEN).
Stručnjacima službi/odjela protudiverzijske (poglavito svim specijalistima protueksplozijske) sigurnosti i zaštite su uglavnom vrlo dobro poznate sastavnice konstrukcija novijih i starijih (iz ratova zaostalih) vrsta standardnih *vojno-formacijskih* eksplozivnih naprava (VFEN),[469] s kojima se često susreću ili mogu susresti pri obavljanju svojih zadaća na ozemlju, građevinama i prostorima koje redovito, izvanredno ili po potrebi (po možebitnoj dojavi ili po službenom zahtjevu) cjelovito protudiverzijski/protueksplozijski pregledavaju, pretražuju, nadziru i/ili osiguravaju.
Međutim, situacija s drugim, nestandardnim vrstama konstrukcija eksplozivnih naprava može biti znatno složenija, jer se tu može raditi o eksplozivnim napravama *improvizirane* ili *specijalne izvedbe*, s mnoštvom (neuobičajenih ili još neviđenih) konstrukcijskih rješenja njihovih sastavnica, kako glede vrste/sastava eksplozivnog naboja tako i glede vrste/konstrukcije njenog upaljačkog/aktivacijskog sklopa (vidi sliku 1).



Slika 1: Neki uopćeno (simbolički) prikazani primjeri konstrukcijskih sastavnica vojnih, gospodarstvenih i improviziranih eksplozivnih i zapaljivih naprava[470]

---

[469] *Vojno-formacijske eksplozivne naprave* (VFEN) su sve one koje se tvornički serijski proizvode u (stotinama) tisućama komada za vlastite potrebe (i potrebe izvoza). Svaka vrsta takve eksplozivne naprave ima na sebi i/ili barem na pakiranju službene identifikacijske oznake [najčešće slovne i brojčane oznake modela, tipa, proizvođača, godine proizvodnje i serijski broj (svakog ili skupine sitnijih) proizvoda, ponekad (fragmentarno)] prepoznatljive/čitljive na nekim njenim metalnim krhotinama pronađenim na mjestu eksplozije.
[470] Za neke od improviziranih eksploziva nije potreban detonator u sklopu upaljača IEN, dok je za neke potreban i pojačivač (*buster*, od eng. *booster*) eksplozije inicijalnog eksploziva u sklopu detonatorske kapsule.

Pod pojmom *improvizirana eksplozivna naprava* (*IEN,* eng. *IED*) razumijeva se svaka ona *cjelovita IEN* ili njena *autonomno eksplozivna sastavnica* (primjerice improvizirani upaljač) koju izrađuju pojedinci ili skupine osoba od gradiva, kemikalija i tehničkih sredstava pogodnih za izradu eksplozivnih naprava. Unatoč možebitno istomu konstruktoru ili istoj „školi“[471] izrade improviziranih eksplozivnih naprava te unatoč možebitno jednakom tipu, možebitno približno jednakim gabaritima i možebitno jednakim sastavnicama sklopa takvih naprava, one ne moraju izgledati i *najčešće ne izgledaju* (posve, navlas) *jednako* (za razliku od VFEN). Izgled i konstrukcija im je uvijek (u većoj ili manjoj mjeri, ovisno o znanjima, vještinama i iskustvima te možebitnim inovacijama konstruktora) prilagođena aktualnom bombaškom zadatku, odnosno meti predstojećeg napada i željenim učincima i posljedicama bombaškog napada. Takve naprave tvore posebnu opasnost jer su nerijetko, više ili manje znalački i vješto, posve samostalno (individualno ili skupno) izrađene te ugrađene ili prikriveno (upakirano, maskirano) postavljene. Mogu biti ugrađene (zamaskirane ili skrivene) u pismo, paketić/paket, aktovku, torbu, kofer, pojas, prsluk, ruksak, bocu pića ili kozmetičkog/farmacijskog preparata, bezazlenu (plišanu, plastičnu, drvenu ili metalnu) dječju igračku, vreć(ic)u ili u kantu za smeće; u prtljažnik, spremnik za gorivo, naslon / pod sjedište ili u nutarnju/vanjsku oblogu vozila; u transportni kanistar/kontejner; u naslon / pod sjedište fotelje/trosjeda ili ležaja; pod odjećom osobe; umetnute u potplate obuće[472] ili u šupljine tijela osobe;[473] pričvršćene na tijelima dresiranih životinja; ukopane u tlo (kolnik ili pločnik); pa čak i ugrađene u zid (ispod slike), pod, strop, ventilacijski otvor/kanal, rasvjetno tijelo, posudu za ukrasno raslinje, vodokotlić, ukrasni kip(ić), šupljinu metalne/betonske ograde ili u stolariju vrata ili prozora prostorije, u donje rublje,[474] u lažni trudnički trbuh, u staračko ili invalidsko pomagalo[475] ili kao svojevrsni tjelesni usadak (implantat) bombaša/bombašice samoubojice (npr. za povećanje obujma grudi);[476] u bilo koji kućanski aparat/uređaj ili u (prijenosno) osobno računalo; u drvenu cjepanicu ili grudu ugljena za loženje; u građevni blok/ciglu ili u bilo koji drugi predmet (skoro) svakodnevne uporabe, tj. unutar različitih

[471] Misli se na: vojne škole za pirotehnologe, izvidnike, obavještajce i protuobavještajce; vojne diverzantske tečajeve; redarstvene protudiverzijske i protuterorističke te obavještajne i protuobavještajne tečajeve; skrivene/prikrivene gerilske i terorističke kampove za obrazovanje i uvježbavanje; samoobrazovanje putem mnogobrojnih specijaliziranih tiskanih i e-priručnika te internetskih stranica s detaljnim naputcima na tu temu.

[472] Medijski je vrlo opsežno praćen slučaj samoubilačkog pokušaja rušenja zrakoplova od strane „bombaša obučenog u eksplozivne tenisice“ Richarda Reida (29 g., britanskog državljanina, sitnog kriminalca, koji je u zatvoru prešao na islam i koji je na sudu izjavio da je član Al-Qaede) koji je 22. prosinca 2001. g. pokušao srušiti zrakoplov tvrtke "American Airlines" tijekom leta iz Pariza za Miami tako da eksplozijom stvori rupu u trupu zrakoplova. Spriječio ga prikriveni nadzornik sigurnosti leta kad je uočen kako pokušava pripaliti sporogoreći stijenj (fitilj) koji je izvirao iz njegovih tenisica, u potplatima kojih je kao improvizirani inicijalni eksploziv vojnog/gospodarstvenog plastičnog eksploziva bio ugrađen vrlo razoran eksploziv triaceton triperoksid (TATP). Svladan je uz pomoć putnika i umiren injekcijom sedativa liječnika u zrakoplovu, tako da je zrakoplov sigurno sletio u Boston (gdje je skrenut radi Richardovog privođenja).

[473] Pokušaj zamalo uspješnog atentata na saudijskog princa Mohammeda Bin Nayefa, unutar kraljevske palače, kolovoza 2009. g., uz pomoć u rektumu skrivenog eksplozivnog naboja s detonatorom, taktička je inovacija Al-Qaede po uzoru na krijumčare droge.

[474] Poznat je slučaj samoubilačkog pokušaja “bombaša donjim rubljem” koji je 25. prosinca 2009. g. uspješno prošao suvremeni tehnički sustav protudiverzijske kontrole amsterdamske zračne luke „Schiphol“ i tijekom leta za Detroit (srećom neuspješno) pokušao u zrakoplovu detonirati plastični eksploziv na osnovi *pentrita* (PETN) ugrađen u donje rublje.

[475] O tomu vidi detaljnije u radu Krešić, 1998.

[476] Široj javnosti je manje poznat slučaj kirurške ugradnje vrlo snažnog eksploziva pentaeritritol tetranitrata (*pentrita*, PETN) u grudi žene (“Terrorists Could Use Explosives in Breast Implants to Crash Planes, Experts Warn”, *The Sun*, 24. ožujka 2010. – preneseno u Klitou, 2014., 76.).

prijenosnih, prijevoznih, pokretnih ili nepokretnih objekata ili predmeta uobičajenog ljudskog okružja.

Mehanizam za aktiviranje IEN može biti u cijelosti vojno-formacijski ili iskorišten od rastavljenih (skinutih) cijelih sklopova upaljača ili upaljačkih dijelova VFEN, ili može biti izrađen od materijala, sklopova, aparata ili uređaja svakodnevne (bezopasne, posve druge) namjene i uporabe (vidi primjere u NCC, 2005). U tom slučaju, prema ideji i načinu izvedbe mogu svojom kakvoćom i učinkovitošću daleko nadilaziti mehanizme aktiviranja VFEN.[477]

Kao *ubojito rasprskavajuće kućište* (*ubojita obloga*) eksplozivnog naboja IEN može biti zlorabljen praktično bilo koji čvrsti predmet ili čvrsto sredstvo poput stjenki kabine ili prtljažnika automobila, trupa plovila ili letjelice, metalne (čelične) bačve, čvrsto pregrađene sekcije čelične ili betonske cijevi, betonske obloge, kuhinjskog (ekspres) lonca, ispražnjene plinske boce ili plinske kartuše, metalnog (čeličnog) kanistra, staklenog balona, prazne konzerve, staklene boce, spremnika goriva, spremnika autocisterne, pogodne šupljine avio-, brodo- ili automodelarskih (daljinski upravljanih i navođenih) modela; ili poput mnoštva čavala, vijaka, matica, čeličnih kuglica iz kugličnih ležajeva, metalnih opiljaka, komada ili krhotina kamena ili stakla obloženih ili (dopunski) oblijepljenih oko tijela eksplozivnog naboja, ili čak u nj površinski utisnutog/utaljenog (neke od primjera vidi u TC 9-21, 2004.).

Kao *neubojita kućišta* IEN (samo pakirne posude ili obloge eksplozivnog naboja) zlorabe se posude, sanduci, kutije, koferi, aktovke, putne/športske ili poslovne torbe, ruksaci, vreće ili vrećice kojima su stijenke od materijala kao što su polimeri, drvo ili karton, odnosno koža, tekstil ili papir (Kulišić, 2003., 365-373.; Thurman, 2006., 121-171.).

S motrišta mogućeg *načina* ili *sredstva aktiviranja* pri napadu, sve IEN-e se razvrstava na:

- *IEN-e s vremenskom odgodom aktiviranja*, koje omogućuju počiniteljima sigurno udaljavanje/bijeg s mjesta postavljanja, prije trenutka eksplozije. Mehanizmi aktiviranja upaljača takvih naprava mogu biti pripaljujući (fitiljni), kemijski (odgođene kemijske reakcije), mehanički (satni) ili elektronički (satni brojači).
- *IEN-e s daljinskim aktiviranjem*, koje omogućuje izbor najpogodnijeg trenutka za eksplozijski napad s ranije potajice postavljenom prikrivenom IEN. Najčešće se rabe u napadu na mete u kretanju (na pogodnim mjestima uobičajenih ruta njihova kretanja). Mehanizam za aktiviranje njihova upaljača može biti dovoljno dugo, dobro maskirano/neuočljivo čvrsto potezno uže, dovoljno dug električni kabel ili digitalni/analogni elektromagnetski signal odabrane valne duljine upućen odgovarajućem digitalnom/analognom prijamniku u sklopu upaljača EN (ponajčešće mobitelom, primopredajnim komunikacijskim uređajem, daljinskim upravljačem nekim od pokretnih modela auto-, avio- ili brodskih igračaka, fokusiranim zračenjem milimetarske valne duljine ili bilo kojom inom vrstom elektroničnog sustava za daljinsko bežično aktiviranje ili upravljanje dovoljno dugog dometa signala).

[477] Najnaprednije, daljinski aktivirane, upaljače svojih bombi sjevernoirska PIRA („Provisional Irish Republican Army", tj. „Privremena irska republikanska vojska") je izrađivala uporabom policijskih ručnih radara za mjerenje brzine vozila, a malo kasnije i uređaja kakvi se rabe za profesionalna „foto-fleš session" snimanja, što je tada predstavljalo nerješiv problem za tehniku protudiverzijske sigurnosti i zaštite odjela protueksplozijske zaštite britanske policije zbog nemogućnosti blokiranja ili ometanja takvih signala za detoniranje skrivenih eksplozivnih naprava (Jackson i sur,., 2007., 98.).

– *IEN-e koje se aktiviraju samo na neku očekivanu/predvidljivu ili uobičajeno poduzimanu radnju žrtve*.[478] Mehanizam upaljača takve vrste naprava može aktivirati neka od radnji poput: udarca; pritiskanja/nagaza; povlačenja/potezanja, podizanja, naginjanja/pomicanja ili otvaranja/zatvaranja predmeta; uspostavljanja/zaustavljanja, ubrzavanja ili usporavanja kretanja vozila, predmeta ili protoka kapljevitih ili plinovitih fluida; podizanja/snižavanja razine temperature, tlaka ili relativne vlažnosti; isključivanja/uključivanja električne struje ili podizanja/snižavanja razine jakosti/napetosti struje, induktiviteta, impedancije ili kapaciteta (pojedinih sastavnica) strujnog kruga; paljenja/gašenja, zamračivanja ili propuštanja prirodnog svjetla; obasjavanja predmeta ionizirajućim zračenjem ili elektromagnetskim zračenjem izvan vidljivog spektra; pojave/nestanka zvuka bilo koje vrste, određene jakosti ili spektra frekvencija; pojave dima cigarete ili iz ložišta itd.
– *IEN-e s dva* ili *više upaljača različitog načina* i/ili *sredstva aktiviranja*.[479]
– S motrišta mogućeg *načina* ili *sredstva izvedbe napada*, sve IEN-e se razvrstava na:
– *Lansirne IEN*-e, koje se *ispaljuju* ili *lansiraju* i *samonavode* ili *daljinski navode* na metu napada sa stanovite udaljenosti iz improviziranog ili vojno-formacijskog minobacača,[480] topa ili bacača granata, odnosno iz improviziranog ili vojno-formacijskog ručnog, prijevoznog ili fiksnog lansera raketnih projektila ili torpeda, koje mogu biti ispaljene ili lansirane izravno ili daljinski po želji počinitelja, s vremenskom odgodom ili nekom radnjom prigodno iskorištene nezlonamjerne osobe.
– *Kopneno prijevozne IEN-e, dopremljene do mete napada pomoću nekog vozila*, poput kamiona, vagona, autobusa, kamp-prikolice, kombija, osobnog automobila, traktora ili

[478] Poput prije spomenute vrste IEN-a, nerijetko se zlorabe i protiv redarstvenih snaga i inih službi žurne intervencije (prvog zahvata) pri pristupu ili kretanju po mjestu stvarnog, simuliranog ili lažno dojavljenog terorističkog napada.

[479] Suvremeni, (samo)obrazovno i (individualno) proizvodno svjetski iznimno vrijedan program profesionalne i amaterske (hobi) elektronike i robotike „Arduino“ je, nažalost, ujedno otvorio i neslućene mogućnosti zloporabe programa njegovih komercijalno lako dostupnih gotovih konstrukcijskih sastavnica pogodnih i za mnoge, prije spomenute moguće improvizacije terorističke namjene. Slično, nažalost, vrijedi i za sve popularniju i komercijalno sve dostupniju tehnologiju „3D ispisa“, iznimno pogodnu i za (serijsku) izradu mnoštva lako zlorabivih vrsta i oblika (općeopasnih) predmeta posve odgovarajuće funkcionalnosti i kakvoće izrade za zločinačku primjenu/namjenu, ali sada i od *sigurnosno* (instrumentalno *defenzivno preventivno*) protudiverzijski *znatno teže detektabilnih* ili (skoro) *posve nedetektabilnih* vrsta gradiva (materijala) i netipičnih (naoko „posve bezopasnih“) geometrijskih oblika.

[480] Najpoznatiji je slučaj PIRA-inog, zamalo uspjelog napada na sjedište britanske vlade (u vrijeme trajanja snažne snježne oluje u Londonu, 7. veljače 1991. g., tijekom zasjedanja tadašnjeg premijera Johna Majora s članovima njegova užeg kabineta o planu britanskog vojnog angažmana u predstojećoj „I. pustinjskoj oluji“ u Kuvajtu) trima granatama izrađenim od tijela plinskih boca, punjenih s plastičnim vojnim eksplozivom „Semtex“ (prokrijumčarenim iz Libije). Ispaljene su preko krovova zgrade Horse Guards aktiviranjem kratkotrajnog tempirnog mehanizma iz tri improvizirano izrađena minobacača, dužine oko 1 m, nazivana “Mark 10” (svaki mase oko 55 kg s nabojem). Bili su prikriveni u unutarnjosti gotovinom kupljenog bijelog kombija „Ford Transit“ s izrezanim krovnim otvorom prekrivenim jednako obojanim krhkim pokrovom, minutu prije lansiranja parkiranog i žurno napuštenog na unaprijed točno određenom mjestu, 230 m zračne linije podalje od mete (bez njene izravne vidljivosti). Zbog neuračunatog malo većeg nagiba kombija, grane stabala trešnji u dvorištu zgrade Vlade su poremetile putanje leta projektila tako da jedna od improviziranih granata nije proletjela kroz prozor prostorije sastanka, već je udarivši u stablo pala i eksplodirala u vrtu, 4,5 m podalje od pročelja zgrade, a ostale dvije su pale nedaleko zgrade Ministarstva vanjskih i Commonwealth poslova. Nakon lansiranja projektila aktivirala se ugrađena paležna naprava namijenjena uništavanju forenzično važnih tragova koja je spalila kombi [Chalk (ur.), 2013., 195-198.]. Petersen (2012.) upozorava i na opasnosti od zloporabe improviziranih projektila punjenih *improviziranim aerosolnim eksplozivom*, pogodnim *pirofornim sredstvom* ili nekom od RKB opasnih vrsta tvari.

inog radnog vozila/stroja, motocikla, bicikla, turističke kočije ili rikše, invalidskih kolica itd., koje mogu biti aktivirane od strane bombaša samoubojice ili daljinski po želji počinitelja, s vremenskom odgodom ili nekom radnjom prigodno iskorištene nezlonamjerne osobe.

- *Plovno prijevozne IEN-e, dopremljene do mete napada pomoću nekog plovila*, poput otetog ili preuređenog rashodovanog teretnog broda (tankera, kontejnerskog, za rasuti teret), ribarice, turističke jahte/jedrilice, glisera, gumenjaka[481] itd., koje također mogu biti aktivirane na prije spomenut način.
- *Podpovršinski/podvodno prijevozne IEN-e, dopremljene do mete napada pomoću nekog podpovršinskog ili podvodnog plovila*, poput ukradene ili preuređene rashodovane male/manje turističke, vojne ili istraživačke ronilice, koje mogu biti aktivirane od strane bombaša samoubojice, daljinski po želji počinitelja ili s vremenskom odgodom.
- *Zračno prijevozne IEN-e, dopremljene do mete napada pomoću osobno upravljane letjelice bombaša samoubojice* ili pomoću *daljinski upravljane*, ili čak možebitno pomoću *samonavođene amaterske visokotehnološke bespilotne letjelice*.[482]
- *Nosive* ili *prijenosne IEN-e, na/u tijelu* ili *ručno donesene* unutar prostora građevine ili ine vrste kopnene, zrakoplovne, plovne[483] ili pored podvodne mete napada, koje mogu biti aktivirane od strane bombaša samoubojice ili daljinski po želji počinitelja, s vremenskom odgodom ili nekom radnjom žrtve ili prigodno iskorištene nezlonamjerne osobe.
- *Lažne IEN*, postavljene ili dopremljene na bilo koji prije spomenut način radi uzrokovanja panike, evakuacije i očekivanog prekida funkcioniranja tehničkog sustava i/ili procesa rada/proizvodnje objekta iz područja kritične nacionalne infrastrukture.[484]

Pod pojmom *specijalna eksplozivna naprava* (*SEN*) razumijeva se svaka ona *cjelovita specijalna eksplozivna naprava* ili njena autonomno eksplozivna sastavnica (npr. *specijalni upaljač*) koja je nastala u specijaliziranim radionicama (znanstvenim i stručnim institutima i laboratorijima) redarstvenih ili vojnih specijalnih protuterorističkih službi,[485] civilnih ili vojnih tajnih obavještajnih ili protuobavještajnih službi, ili u tajnim laboratorijima financijski i stručno (kadrovski) vrlo moćnih terorističkih organizacija, odnosno po tajnoj narudžbi

[481] Primjerice, slučajevi napada na američki razarač „Cole“ i francuski supertanker „Limburg“ u Adenskom zaljevu 2000. g.

[482] Postoji ozbiljna zabrinutost službi sigurnosti, obrane i zaštite diljem svijeta glede rastuće opasnosti od moguće terorističke zloporabe ove vrste već komercijalno dostupnih ili improvizirano izrađenih (visokotehnoloških) naprava u napadima eksplozivnim, kemijskim, biološkim i radiološkim sredstvima na posebno štićene osobe, građevine, političke skupove i na ina društvena okupljanja, poput religijskih, športskih i poslovnih. Na to upozoravaju već mnogobrojni incidenti padova *daljinski upravljanih bespilotnih letjelica* na takvim mjestima, pa i politički i sigurnosno provokativnih letova iznad takvih mjesta (vidi i Burns, 2016., 239.).

[483] Najpoznatiji je slučaj PIRA-inog smrtonosnog atentata s potajice unesenom i skrivenom, daljinski aktiviranom IEN s oko 23 kg eksploziva, 27. kolovoza 1979. g., na glasovitog britanskog lorda Louisa Mountbattena i 6 njegovih prijatelja tijekom jedrenja u irskom zaljevu Donegal na 9 metara dugoj jedrilici „Shadow V“.

[484] Moguće scenarije i mete napada na objekte kritične nacionalne transportne infrastrukture vidi npr. u Sk. a., 1999. Kod nas su svi sektori moguće kritične nacionalne i europske infrastrukture načelno obuhvaćeni čl. 4. i 15. *Zakona o kritičnim infrastrukturama* (NN, br. 56/13.).

[485] Uglavnom za potrebe izrade SEN za iznenadne redarstvene prodore (kumulativno oblikovanim nabojima) na posve neočekivanim mjestima u građevine/prostore u kojima se skrivaju (zabarikadirani) naoružani zločinci (nerijetko u talačkim situacijama).

terorističke organizacije ili organiziranog kriminala u onih osoba koje su im već poznate u kriminalnom miljeu kao dokazani eksperti za izradu takvih sofisticiranih eksplozivnih sredstava i kao osobe koje jako dobro znaju, ili imaju motiva, posve čuvati povjerenu im tajnu. One, jednim dijelom postojećih izvedbi, ujedno čine i jednu *posebnu* (*specijalnu*) *podskupinu „mina iznenađenja“*. Najčešće, za takvu namjenu, naprave ove vrste predstavljaju vrsne imitacije predmeta ili objekata (svakodnevne uporabe, potrošnje ili interijera prostora boravka ili kretanja) u posjedu ili u bliskom okružju budućih žrtava atentata.[486] Odjeli za „prljave / mokre poslove“ tajnih službi uglavnom izrađuju samo tri primjerka završne inačice, od kojih se prvi uništi u pokusu funkcioniranja i učinkovitosti. Drugi primjerak iskoriste u atentatu, a trećim primjerkom (bez opasnog/ubojitog sadržaja) se služe kao školskom specijalnom eksplozivnom napravom u svom internom muzeju specijalnih naprava za obrazovanje novih naraštaja agenata i atentatora. Skoro nikada se više ne služe jednakim inačicama takvih ubojitih sredstava. U najvećem broju slučajeva se radi o minijaturnim izvedbama napunjenim visokobrizantnim ili ultrabrizantnim eksplozivom (npr. poput *heksanitroheksaazaizovurcitana*/*CL-20* ili *oktanitrokubana*/*ONK*), koji ne ostavljaju (skoro) nikakve identifikacijski (kriminalistički) važne tragove.[487] Mogu biti postavljene poradi presijecanja čeličnih sajli, oštećenja hidrauličnih cijevi ili različitih prijenosnika (energije) u sklopu upravljačkih mehanizama zrakoplova ili osobnih vozila. Najčešće se tako uzrokovana oštećenja pri površno provedenom očevidu tumače „zamorom materijala“, „višom silom“ ili inim trivijalnim objašnjenjem, a kritične učinke eksplozije takve minijaturne eksplozivne naprave se ne raspoznaje (zbog nestručnosti i nesavjesnog rada istražitelja) ili pak prešućuje iz straha, tj. zbog tzv. urote šutnje i/ili sabotiranja istrage od strane možebitno upletenih ili zastrašenih ključnih istražitelja (pripadnika tajnih službi, kriminalista, državnih odvjetnika, sudaca), ključnih vještaka ili možebitnih ključnih svjedoka. Takve naprave se mogu pravodobno uspješno otkriti i na siguran način ukloniti samo kvalitetnim (ekspertnim) protudiverzijskim sigurnosnim pregledom, uz uporabu suvremene sofisticirane tehnologije za računalno (softverski) podržanu višestranu (višesenzorsku) kombiniranu detekciju, identifikaciju i analizu eksploziva i/ili pojedinih (ili cijelih) ključnih ili znakovitih sastavnica/sklopova eksplozivne naprave (skr. i dop. prema Kulišić, 1994.; 1997.; 2001.; 2003., 365-373. i 2007.).

---

[486] Izvorni se predmeti (pokretni ili prijenosni objekti) nakratko ukradu ili temeljito snime, na temelju čega se izrađuju vjerne kopije s ubojitim sadržajem.

[487] Znakovit i svjetskoj javnosti dobro poznat primjer izrade i primjene jedne *specijalne eksplozivne naprave* tipa posve funkcionalnog *satelitskog* ili običnog *GSM prijenosnog telefona bombe* (s malim visokobrizantnim eksplozivom ugrađenim unutar dijela obujma kućišta njegove baterije; uručenim meti od obiteljski vrlo bliske ali bezizlazno teško ucijenjene osobe) je slučaj atentata na palestinskog/Hamasovog glavnog konstruktora mnogih razornih automobila bombi, Yehiyu Ayasha (poznatog pod tajnim imenom „Inženjer“), 5. siječnja 1996. g. Bomba je daljinski aktivirana čim je prepoznat njegov glas na vezi. Atentat je izazvao bijes i masovne prosvjede Palestinaca diljem Palestine i svih arapskih zemalja masovnije palestinske imigracije te bio povodom pokretanja prvih dvaju iz serije samoubilačkih bombaških napada „Izz-ad-Din al-Qassam brigada“ (vojnog krila Hamasa) na gradske autobuse u Izraelu tijekom prvih mjeseci 1996. g. te napada kamenjem i zapaljenim gumama po ulicama Jeruzalema i inih gradova i naselja diljem Gaze i Zapadne obale (rijeke Jordan) protiv izraelskih civilnih, redarstvenih i vojnih vlasti, čija tajna služba Mossad je u palestinskoj javnosti odmah optužena za taj atentat [Chalk (ur.), 2013., 373.; Kulišić, 2003., 365-373].

Eksplozivne tvari (ET),[488] s kojima se nešto češće ili rjeđe susretalo u slučajevima terorističkih i inih organiziranih i individualnih zločinačkih napada eksplozivnom napravom, predočene su sljedećom tablicom.

Tablica 1: Pregled glavnine vrsta/naziva dosad zlorabljenih eksploziva i inih vrsta eksplozivnih tvari (prema stručnim i medijskim izvješćima o dosad izvedenim, pokušanim ili pripremanim terorističkim napadima).[489]

Ilegalno nabavljani standardni vojni eksplozivi	**Ilegalno nabavljani standardni komercijalni eksplozivi**	**Improvizirano kemijski sintetizirani ili na drugi način izrađivani ili dobivani eksplozivi (IE)**[490]
pakiranja plastičnih vojnih eksploziva (prirodnim ili sintetskim uljima ili mastima obrađeni RDX, PETN, HMX i/ili TATB), poput onih svjetski najpoznatijih kao što su C4, PE-4, Semtex i kod nas čest PEP-500	tipa granuliranog ANFO (amonijev nitrat - loživo ulje/dizelsko gorivo, ANDG, AN/DG, AN-DG ili inih komercijalno rabljenih akronima)	inačice tipa granuliranog ANFO s bilo kojom slabije isparljivom kapljevitom gorivom sastavnicom
pakiranja čvrstim ili tekućim polimerima povezanih eksploziva tipa PBX ili LX i sl. (polimerima obrađeni RDX, PETN, HMX i/ili	dinamiti (plastični, poluplastični i praškasti gospodarstveni eksplozivi sa sadržajem nitroglicerina i EGDN)[491]	praškasti eksplozivi na osnovi amonijevog nitrata (AN) i bilo koje vrste praškaste/usitnjene gorive tvari (uključujući Al u prahu[492])

[488] Pod složenicom *eksplozivne tvari* (ET), stručno nazivanim još i *energetskim* ili *visokoenergetskim tvarima*, razumijevamo sve one čvrste ili kapljevite tvari u prividno stabilnom (tzv. metastabilnom) stanju sposobne za iznimno brzu – eksplozivnu – kemijsku reakciju razlaganja (*endotermne ET*) ili razlaganja i izgaranja (*egzotermne ET*) u kondenziranoj fazi, bez potrebe da u njoj sudjeluju bilo kakvi vanjski reaktanti (poput kisika iz okolnog zraka). U *eksplozivne tvari* se ubraja sve *eksplozive* i sve ine, znatno brojnije, *kemijske proizvode* eksplozivnih svojstava, ali *neeksplozivne namjene* – vrlo lako zlorabive kao/za izradu IE.

[489] TNT, RDX, PETN, HMX, Tetril, TATB, NG (Ngl), EGDN, TATP i HMTD (HMTPDA) su uobičajeno rabljeni akronimi ili kratice za čiste homogene eksplozivne tvari sljedećih trivijalnih i/ili kemijskih naziva: *trotil* (2,4,6-trinitrotoluen), *heksogen* (1,3,5-trinitro-1,3,5-triazacikloheksan), *pentrit* (pentaeritritol tetranitrat), *oktogen* (1,3,5,7-tetranitro-1,3,5,7-tetraazaciklooktan), *tetril* (N-metil-n-2,4,6-tetranitroanilin), 1,3,5-triamino-2,4,6-trinitrobenzen, *nitroglicerin* (glicerol trinitrat), *nitroglikol* (etilenglikol dinitrat), triaceton triperoksid (u suvremenim bliskoistočnim i srednjeistočnim terorističkim organizacijama popularno nazivan „Sotoninom majkom“) te heksametilen triperoksi diamin.

[490] Vodeće mjesto među terorističkim improviziranim rušilačkim eksplozivima čvrste konzistencije, pogodnim za goleme terorističke eksplozivne naprave (tj. za goleme prijevozne eksplozivne naboje mase od nekoliko stotina kilograma pa do čak 20 ili više tona eksploziva), danas nedvojbeno pripada improvizirano izrađenim eksplozivima na osnovi *amonijevog nitrata* (NH_4NO_3), tipa ANFO, po modelu izrade gospodarstvenih *granuliranih* ili *praškastih/patroniranih ANFO eksploziva*, dobro poznatim kao vrlo jeftinima te za transport i rukovanje vrlo sigurnim eksplozivima, primarno gospodarske namjene, uz pomoć mineralna gnojiva tipa "KAN" s dovoljno visokim sadržajem NH_4NO_3. Otuda se mineralna gnojiva tog tipa, unatrag više od 40-ak godina, počinju sve ozbiljnije držati sigurnosno (obavještajno) i kriminalistički znakovitim sirovinama (kemijskim tzv. *prekurzorima*) za njegovu ilegalnu izradu (vidi Kulišić, 1992, 1992a i 1993.).

[491] Javnosti najpoznatiji slučajevi terorističkih napada eksplozivima iz ove skupine su slučaj zamalo uspješnog pokušaja atentata PIRA-e na tadašnju britansku premijerku Margaret Thatcher u predsjedničkom apartmanu hotela „Grand“, u Brightonu, 12. listopada 1984., i slučaj istodobnog napada s 11 eksplozivnih naprava na 4 vlaka prigradskih željeznica u Madridu, 11. ožujka 2004.

TATB)		
TNT (u obliku pakiranja inženjerijskih naboja, tzv. TNT metaka, ili izvađen iz neeksplodiranih vojnih eksplozivnih naprava)	plastični eksplozivi za gospodarstvo (prirodnim ili sintetskim uljima ili mastima obrađeni RDX, PETN, HMX i/ili TATB)	teroristički učinkovito flegmatiziran ili plastificiran TATP ili znatno rjeđe zlorabljen HMTD/HMTPDA[493]
lijevani naboji smjese TNT-a s amonijevim nitratom (AN), RDX, PETN, HMX i/ili s *tetrilom*, izvađeni iz neeksplodiranih vojnih eksplozivnih naprava	PBX eksplozivi različitih geometrijskih oblika ili načina pakiranja tekućine LX za gospodarstvo	nitrourea (NU) ili urea nitrat (UN) (npr. slučaj napada na WTC u New Yorku, 1993. g.)
vojni inženjerijski „dinamiti“ (praškasti eksplozivi na osnovi amonijevog nitrata/AN i TNT-a, uz eventualni dodatak Al u prahu – poput gospodarstvenih tipa *amatola* i *amonala*)	praškasti eksplozivi na osnovi amonijevog nitrata (AN) i određenih vrsta praškastih gorivih tvari odgovarajuće ogrjevne moći i sastava plinova izgaranja	nitroglicerin (za potrebe improvizirane izrade dinamita te za zloporabu u obliku pisama/paketa bombi i inih vrsta predmeta kao „mina iznenađenja“)
koloidni baruti (eksplozivni naboji izrađeni od barutnih zrna različitih geometrijskih oblika izvađenih iz kućišta neispaljenog vojnog streljiva)	dvokomponentni (binarni)[494] ili višekomponentni eksplozivi (eksplozivni naboji stvarani miješanjem neeksplozivnih sastojaka na mjestu željene primjene)	sastavom različite inačice improviziranog crnog baruta ili smjese slično eksplozivne strukture
kompozitni baruti (eksplozivni naboji izrađeni od blokova baruta izvađenih iz kućišta neispaljenih projektila većih dometa)	crni barut (uglavnom lovački ili rudarski)	dvokomponentni (binarni) ili višekomponentni eksplozivi (eksplozivni naboji stvarani miješanjem neeksplozivnih sastojaka na mjestu željene primjene), uključujući i one na osnovi ukapljenog kisika (tipa LOX)

[492] Takve improvizirane *amonale* (praškaste smjese AN i Al) je početkom 1990-ih godina u više navrata zlorabila teroristička skupina ETA.

[493] Približna snaga eksplozije HMTD-a (poznatom po zloporabi u bombaškom napadu u londonskom metrou 7. srpnja 2005. g.) je oko 60 % a TATP-a (posebno poznatog po zloporabi u vrlo velikim količinama u bombaškim napadima u Bruxellesu 22. ožujka 2016. g.) između 80 i 88 % snage eksplozije TNT-a.

[494] Komercijalne nazive i tipične sastave nekih od predstavnika iz ove skupine te njihove konzistencije vidi primjerice u Cooper, 1996., 59.

isporuke (industrijskih pakiranja) punjenja za vojno-formacijske aerosolne bombe (poput kerozina, etilen oksida, aluminija u prahu itd.)	patronirani vodoplastični „slurry“ (kašasti) eksplozivi i emulzijski eksplozivi (najrjeđe su traženi, otuđivani i zlorabljeni zbog slabije brizance/razornosti ili slabe prepoznatljivosti u većine terorističkih i inih zločinačkih krugova)	komercijalni plin acetilen (iniciran reagira kao endotermna eksplozivna tvar kada je nepomiješan s kisikom/zrakom)[495]
		ukapljeni gorivi plinovi ili zapaljive kapljevine primjenjive kao improvizirani aerosolni eksploziv[496]

Među najčešće zlorabljene *sirovine*[497] *pogodne za ilegalnu izradu improviziranih eksploziva (IE)*, tj. za njihovu kemijsku sintezu ili za njihovo pripravljanje miješanjem tvari, ubrajaju se primjerice [Beveridge (ur.), 2012., 498.; Crippin, 2006., 152. i 154.; CTTSO/TSWG, 2007.; Houghton, 2009., 105.; Kulišić, 2003., 462-487.; Schubert i Kuznetsov, (ur.), 2008., 38.; Sk. a., 1998a, 130.]:

a) za *kemijsku sintezu IE*: aceton, dušična kiselina (≥ 68 %), etilen glikol, heksamin, hidrazin, kalijev nitrat, klorovodična kiselina, limunska kiselina, metil etil keton, natrijev nitrat, sumporna kiselina, urea, vodikov peroksid (≥ 30 %)[498] itd.
b) za *pripravljanje miješanjem*, kao *goriva sastavnica IE*: alkoholi, antimonov trisulfid (Sb_2S_3), celuloza, dizelska goriva, drvena piljevina, energetska pogonska goriva (poput nitrobenzena, nitroceluloze, nitrometana, hidrazina i sl.), fosfor (P), karbonsko crnilo, kerozin, loživa ulja, ljuskaste ili praškaste kovine (poput Al, Mg, Zn, Fe, Cu, Zr itd.), organska otapala (poput acetona, metil etil ketona, nafte), parafin, prirodni/naftni plin (metan, propan, butan), sumpor (S), šećeri, ugljen, vazelin, vosak itd.
c) za *pripravljanje miješanjem*, kao *oksidacijska sastavnica IE*: amonijev nitrat, amonijev perklorat, dušična kiselina, kalijev klorat, kalijev nitrat, kalijev perklorat, kalijev permanganat, natrijev klorat, natrijev nitrat, ukapljeni kisik, vodikov peroksid itd.[499]

---

[495] Mnogobrojni su bili primjeri noćnog razbojničkog eksplozijskog razvaljivanja kućišta bankomata uz pomoć plina acetilena (uključujući i na ozemlju RH).

[496] Najpoznatiji je slučaj Al-Qaedinog terorističkog napada tom vrstom improviziranog eksplozivnog naboja na jednu od najstarijih i najpoznatijih židovskih sinagoga na sjevernoafričkom tlu („La Ghriba“), na otoku Djerba, u Tunisu, pomoću manje autocisterne s ukapljenim naftnim plinom, 11. travnja 2002. g.

[497] U našoj kriminalističkoj teoriji i praksi, ne samo glede nezakonite proizvodnje eksploziva, posve nepotrebno nazivane *prekurzorima* (zapravo, *pretečama* od eng. *precursors*).

[498] Poznato je kako koncentrirani vodikov peroksid (H_2O_2) u dodiru s gorivim tvarima poput drvene piljevine, papira ili ulja može uzrokovati njihovo spontano zapaljenje i izgaranje, a u slučaju njegova miješanja s nekim drugim gorivim tvarima, kao što su šećeri, alkoholi ili aceton, može doći do stvaranja snažno eksplozivne IET.

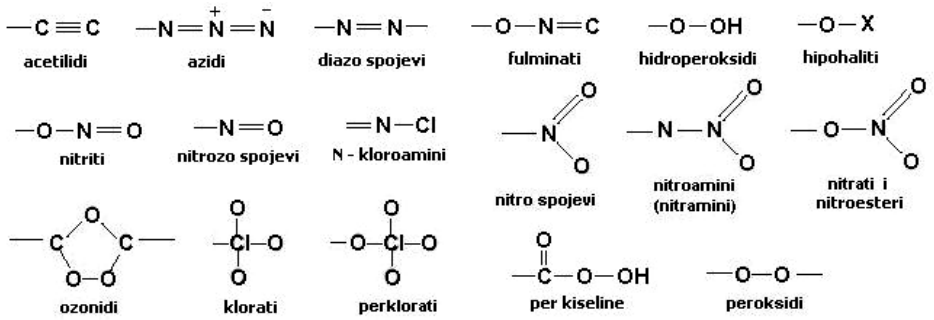
[499] Ocjenske čimbenike *polukvantitativnog sigurnosnog rizika* glede: moguće dostupnosti pojedinih sirovina (kemikalija) za izradu IET, moguće složenosti postupka njihove primjene pri izradi IET/IEN, mogućih troškova (ekonomičnosti) njihove izrade i statističke čestine (frekvencije) njihove dosadašnje primjene, uz prosudbu *polukvantitativnog rizika* (potencijala) od zloporabe svake takve kemikalije za potrebe izrade i zloporabe u sklopu IEN vidi u Sk. a., 1998a, 101.

3. NEKA DETEKCIJSKI I IDENTIFIKACIJSKI POSEBNO VAŽNA ZNAKOVITA OBILJEŽJA EKSPLOZIVNIH TVARI

Skoro svi standardni, tradicionalno rabljeni vojni i gospodarstveni eksplozivi sadrže eksplozivne tvari relativno jednostavnih građa molekula, sastavljenih od atoma vodika (H), ugljika (C), kisika (O) i dušika (N). Samo dio eksplozivnih organskih peroksida, poput TATP-a, ne sadrže atome N. Neki od eksploziva i inih vrsta eksplozivnih tvari (ovisno o građi i predviđenoj namjeni) mogu sadržavati i stanovitu količinu aluminija (Al), barija (Ba), bora (B), željeza (Fe), žive (Hg), olova (Pb), fluora (F), silicija (Si), fosfora (P) i/ili nekih inih kemijskih elemenata. Zahvaljujući tomu, mnoge spektroskopske metode su vrlo pogodne za otkrivanje i identifikaciju eksplozivnih tvari.

Među uobičajene opće značajke većine tradicionalno rabljenih eksploziva ubraja se:

- visok sadržaj i gustoća dušika;
- vrlo učestao sadržaj dušika u anorganskoj ili organskoj tvari vezanog u obliku nitro ($-NO_2$) ili nitratne ($-ONO_2$) funkcijske skupine (vidi sliku 2), kao nositelja kisika nužnog za eksplozivno izgaranje;
- relativno visok sadržaj kisika i dušika,[500] uz relativno niži sadržaj ugljika i vodika, u odnosu na ine organske tvari;



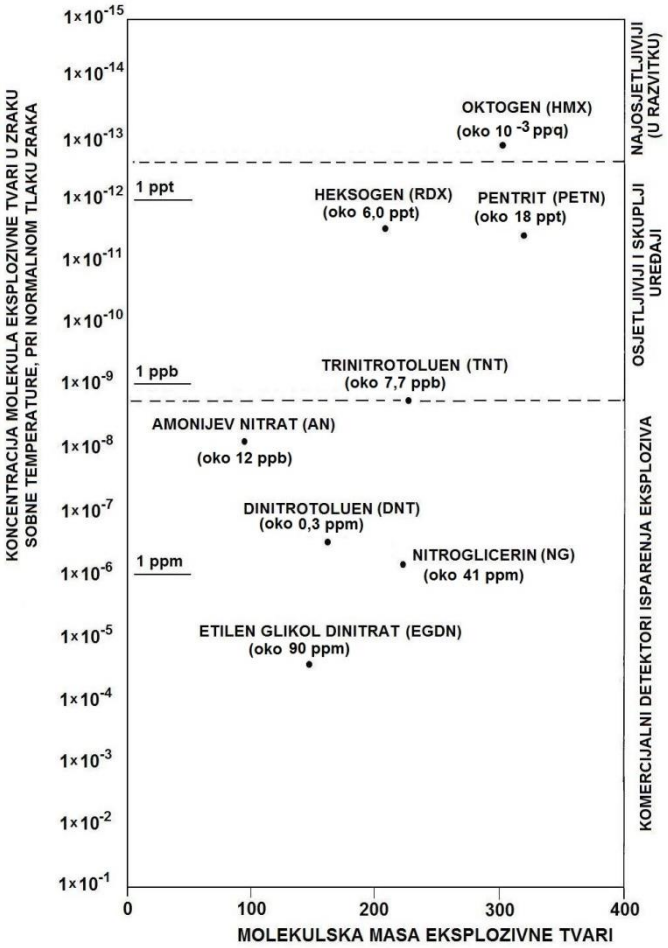
Slika 2: Sigurnosno, detekcijski i identifikacijski posebice znakovite kemijske funkcijske skupine najpoznatijih kemijski nestabilnih i eksplozivnih tvari koje u strukturi svoje molekule sadrži glavnina najčešće rabljenih inicijalnih, pojačivačkih i/ili razornih vojnih, gospodarstvenih i/ili improviziranih eksploziva[501]

- relativno velika gustoća tvari (gustoća naboja najčešće u rasponu od oko 1,2 do oko 1,8 puta veće gustoće od gustoće vode, a u pojedinim slučajevima do najviše oko 5 puta, kao u slučaju nekih anorganskih/inicijalnih eksploziva);

[500] Kod mnogih predstavnika sadržaj dušika se kreće između 20 % i 43 %, dok se sadržaj kisika kreće između 37 % i 53 %, što omogućuje znatno veću pouzdanost njihove detekcije u odnosu na metodu detekcije samo putem sadržaja dušika, premda je to znatno teže postići u slučaju improvizirano izrađenih eksploziva zbog moguće uporabe mnoštva različitih sastojaka, primjene nestehiometrijskih omjera sastojaka pri njihovoj izradi, lako moguće grubog i netočnog, često nepotpunog procesa proizvodnje. Detekcija istodobnog sadržaja O i N nije moguća u slučaju svih onih ET koje uopće ne sadrže atome N, kao primjerice u slučaju TATP-a [Cutolo, Mignani i Tajani (ur.), 2014., 124.].

[501] Još neke detekcijski i istražno relevantne funkcijske skupine eksplozivnih tvari vidi npr. u Sk. a., 2011., 71.

– iznimno slaba hlapljivost tvari (uglavnom vrlo slab ravnotežni tlak zasićenih para; <1 Pa pri 25° C) zbog njihove većinom relativno velike relativne molekulske mase (> 150) – vidi sliku 3;[502]
– visoka polariziranost molekula (elektronegativnost) zbog sadržaja nitro skupina (-NO_2) u građi;
– slaba stabilnost molekula na povišene temperature;
– krhkost građe molekula na mehanički udarac;



Slika 3: Približne razine koncentracije isparenja molekula pojedinih vrsta ET/IET u zraku (pri sobnoj temperaturi od 25° C i normalnom tlaku zraka) i nužne razine osjetljivosti uređaja za njihovu moguću instrumentalnu detekciju i identifikaciju (novijim podacima prema Sk. a., 2007b, 11. te Pellegrino, Holthoff i Farrell, 2015., 307. i 365. korig./dop. a. prema grafikonu OTA, 1991., 48.)[503]

[502] Iznimku čini jedino ravnotežni tlak zasićenih para TATP-a, koji se pri navedenim uvjetima kreće oko 4 Pa, a koncentracija njegovih molekula u zraku se kreće blizu 60 ppm, pa se pare njegove sublimacije (kao i pare kapljevitih EGDN i NG) mogu relativno vrlo lako detektirati (Pellegrino, Holthoff, Farrell, 2015., 307.).
[503] Grafikonom navedene vrijednosti detektabilnih koncentracija ponešto variraju, ovisno o literaturnom izvoru. Pritom još treba imati na umu da utjecaj načina skrivanja (I)ET/(I)EN može smanjiti mjerljivu koncentraciju njene (I)ET i za oko 1000 puta (prema Pellegrino, Holthoff, Farrell, 2015., 307.) ili za 100 do 10.000 puta (prema Sk. a., 2004a, 86.). Zbog toga je praktična *daljinska detekcija* glavnine visokoeksplozivnih (tj. brizantnih, detonantnih) eksploziva aktualno rabljenim metodama/tehnikama praktički nemoguća, pa se zato krenulo u usavršavanje i razvitak novih metoda i tehnika za *izravnu analizu čestica* na ET sumnjivih tvari možebitno

- relativno velika adsorptivnost (fizikalna prionjivost) para i čestica slabo isparljivih ET na površinama dodirujućih ili obližnjih krupnijih čestica neeksplozivnih tvari i na površinama predmeta od inih (neeksplozivnih) vrsta materijala[504] te
- stanovita razina otrovnosti (putem probavnih i dišnih organa, a i kože).[505]

Kako je prije spomenuto, zbog vrlo/posebno niskog ravnotežnog tlaka zasićenih para iznad same površine neke ET, iznad nje može biti molekulskih sastojaka takve ET, njenih nečistoća ili produkata njene razgradnje u rasponu reda veličine od najviše 1000 milijuntih dijelova (*ppm*) do samo nekoliko djelića trilijuntih dijelova (*ppt*) ili samo par kvadrilijuntih dijelova (*ppq*) jediničnog obujma atmosfere iznad površine takve ET, ovisno o vrsti/hlapivosti molekula te ET i njenoj temperaturi/temperaturi njene okoline – vidi sliku 3.

Za detekciju i identifikaciju se mogu uspješno rabiti tehnike molekulske spektroskopije u plinovitoj fazi, osim za one primjere ET posebno niskog tlaka zasićenih para. Osim toga, kako većina pakiranih ET, izuzev dinamita (na osnovi nitroglicerina i/ili EGDN) te TATP-a, oslobađa iznimno male količine para, pouzdana detekcija i identifikacija ovom tehnikom je moguća tek izravnim uzorkovanjem, iznad same površine takvih tvari i vjerojatno postupkom koncentriranja uzoraka (Sk. a., 2004a., 65.).

Kako pojedini eksplozivi sadrže i stanovite proizvodne nečistoće veće isparljivosti (kao što je dinitrotoluen/DNT u sastavu TNT-a), to svojstvo se rabi u njihovoj detekciji, kao u slučaju detekcije plinovitih tragova skrivenih protutenkovskih i protupješačkih nemagnetnih mina. Neki od plastičnih komercijalnih i vojnih eksploziva na osnovi RDX-a, PETN-a, HMX-a i/ili TATB-a sadrže detekcijski dovoljno hlapljive *energetske plastifikatore* i/ili *tajne hlapljive obilježivače* (npr. butantriol trinitrat/BTTN, dietilen glikolnitrat/DEGN, 2,3-dimetil-2,3-dinitrobutan/DMNB ili DMDNB, etilen glikol dinitrat/EGDN mononitrotoluen/MNT). Detekcija isparenja takvih tvari može biti pouzdanim pokazateljem moguće nazočnosti takvih eksploziva (Sk. a. 2004a, 62.; Pellegrino, Holthoff, Farrell, 2015., 152.).

Glavnina prije pobrojanih svojstava klasičnih eksploziva se aktualno, u većem ili manjem opsegu kombinirano te s više ili manje uspjeha, rabi za njihovu preliminarnu fizikalnu, kemijsku i (multisenzorski kombiniranu) instrumentalnu detekciju.

---

nazočnih na površinama kože tijela, odjeće, obuće i inih predmeta koji su mogli biti u izravnom dodiru s ET ili u njenom bliskom okružju.

[504] Zbog toga se vrlo sitne čestice takvih ET vrlo lako mogu nahvatati na materijal pakiranja, odjeće, obuće i na koži tijela izrađivača IEN kao i na materijal prtljage, odjeće i obuće preuzimatelja, prenositelja i/ili postavljača IEN.

[505] Takva izloženost eksplozivima uzrokuje širok spektar bioloških učinaka, kako na cijeli organizam tako i do stanične i podstanične razine. Zbog toga se i ovo svojstvo ET vrlo pozorno istražuje poradi pronalaženja i usavršavanja pogodnih *biomarkera* u svezi fizioloških promjena koje ukazuju na možebitnu izloženost stanovitoj skupini/vrsti ET, tj. radi moguće *posredne detekcije* kronične ili akutne izloženosti neke osobe eksplozivu (zbog možebitne ilegalne proizvodnje, dužeg posjedovanja, kraćeg rukovanja pri izradi IEN ili samo nošenja eksploziva u sklopu nekakve IEN – vidi Sk. a., 2004a, 99-100.).

4.SUSTAVI ZA DETEKCIJU I IDENTIFIKACIJU EKSPLOZIVNIH TVARI I EKSPLOZIVNIH NAPRAVA

Prije spominjani i mnogobrojni ini, sve češći slučajevi terorističkih napada s IEN doveli su do intenziviranja znanstvenih i stručnih istraživanja te do (pokušaja) razvitka nekih novih (lako integrabilnih ili već integriranih) tehnologija pogodnih za *kontaktnu, u bliskom polju* (sa stanovite manje udaljenosti) ili za moguću *daljinsku detekciju* i *identifikaciju*, ne samo takvih vrsta opasnih tvari/naprava, već ujedno i za detekciju i identifikaciju i inih vrsta vrlo opasnih tvari/naprava (posebice KBRN opasnih;[506] vidi Petersen, 2012., 218.), kao i svih onih strogo zabranjenih/kontroliranih tvari i proizvoda namijenjenih „crnom" tržištu. Neke od njih se već sada, s više ili manje uspjeha, rabe i u otkrivanju mjesta ukopanih vojnih mina, tajnih ilegalnih proizvodnih radionica i pogona, skladišta i skrovišta gerilskih, terorističkih i narkozločinačkih organizacija, individualnih ili masovnih grobišta žrtava zločina, novih arheoloških lokaliteta itd., ovisno o njihovim posebnim obilježjima, strukturnim obilježjima njihova prirodnog ili urbanog okružja te lokalnim hidrometeorološkim i geofizičkim prilikama.

Naime, na osnovi prije navedene nekolicine općih značajki ET i golemog mnoštva različitih mogućih inačica tehničke izvedbe i *modusa operandi* (MOS) napadajne zloporabe (I)EN, razvidno je kako još ne postoji ni jedna (barem ne komercijalno dostupna) toliko sofisticirana jedinstvena metoda/tehnika kojom bi se moglo sigurnosno dovoljno brzo i pouzdano otkriti i prepoznati sve moguće vrste (I)ET[507] i konstrukcijske oblike (I)EN,[508] a poglavito ne onih u stadiju vrlo niskog/prizemnog leta nakon lansiranja/ispaljenja ili tijekom osobnog prijenosa, neke vrste dovoljno brzog prijevoza ili (samo)navođenja do moguće mete napada te sa stanovite, za pravodobnu (možebitno automatsku) protunapadajnu/protudiverzijsku intervenciju obrambeno i zaštitno presudno važne, najmanje dovoljne sigurnosne udaljenosti.

Zbog toga se danas rabi, razvija i/ili pokušava što funkcionalnije međusobno povezati ili integrirati tehničke sustave nekolicine/više posve različitih metoda i tehnika pogodnih za dovoljno brzu identifikaciju određenih skupina i pojedinih vrsta (I)ET te za otkrivanje i prepoznavanje vješto skrivenih/prikrivenih masa mogućih eksplozivnih naboja, različitih možebitnih konstrukcijskih sastavnica ili možebitnih oblika izgleda cjelovitih vrsta (I)EN pri njihovu osobnom prijenosu i kopnenom prijevozu, u realnom vremenu i na što je moguće većoj pristupnoj (detekcijskoj) udaljenosti od mjesta rabljenih (multi)senzora.

Ovdje valja još podsjetiti na redarstveno tradicionalno dobro poznatu, preporučanu i rabljenu izvidnu radnju fizičkog sigurnosnog *pregleda* i dokaznu radnju fizičke *pretrage*,[509] ali i na

---

[506] Kemijski, biološki, radiološki ili nuklearno opasne tvari.

[507] Pritom, čak i stjecajem okolnosti možebitno omogućeno pravodobno podrobno ispitivanje stanovitih sigurnosno sumnjivih tvari može biti identifikacijski problematično, ako se pritom zbog nekog razloga ne pretpostavi da se, među inim, možda radi o nekoj ET.

[508] Prouči *moduse operandi* (MOS) prije spominjanih slučajeva njihova uspješnog unosa u zrakoplove i u ine protudiverzijski standardno ili posebno štićene građevine/prostore ili pokretne objekte.

[509] Stručan, iskusan i pozoran *fizički pregled*, a posebice *fizička pretraga*, jamči visoku vjerojatnost otkrivanja i prepoznavanja možebitnog posjedovanja/postojanja nekakve ET/EN, ali mu je mana što može biti zakonski ili postupovno sporno/neugodno invazivan s motrišta pretraživanju podvrgnutih (ženskih, invalidnih, starih) osoba, jer zahtijeva operativno možebitno neprihvatljivo duže/predugo raspoloživo vrijeme za njegovo dovoljno temeljito obavljanje i jer ujedno ugrožava živote svih osoba koje ga obavljaju, ako se možebitno skrivena/postavljena (I)EN pritom namjerno ili nekom radnjom pregleda/pretrage aktivira. S druge strane, mnogi

neke tradicionalno dobro poznate, preporučane i rabljene *jednostavne* (primitivne, ali vrlo djelotvorne) *terenske preliminarne fizikalne pokuse na eksplozivne tvari*, u koje se ubrajaju *pokusi provjere ponašanja* vrlo malog uzorka (oko 1 mg ili 5-10 kristalića) sumnjive tvari na *utjecaj plamena* i *mehaničkog udarca*, kao i provjere njene *relativne gustoće u odnosu na vodu*, u slučaju pronalaska sumnjive uljaste kapljevine (stavljanjem jedne kapi na površinu vode u prozirnoj čaši) [vidi Houghton, 2008., 251-252., 2009., 132., 240. i Kulišić, 2003., 349-350.].

Danas se sve *suvremene metode i tehnike za detekciju* (i *identifikaciju*) eksplozivnih tvari i eksplozivnih naprava grubo razvrstava na sve one:

- namijenjene otkrivanju: (a) *mase i geometrije eksplozivne tvari/naprave* i/ili (b) *tragova* (i *vrste*) *eksplozivne tvari*;
- pogodne ili s (mogućim/daljim) razvojnim potencijalom za detekciju (i identifikaciju) ET/EN: (a) *na dodirnoj* ili *vrlo blizu same površine* moguće ET/EN; (b) *na* stanovitoj *relativno manjoj udaljenosti* od mjesta postavljanja ili trenutačnog zaticanja ET/EN i (c) *na daljinu*/*većoj udaljenosti* od mjesta postavljanja ili trenutačnog zaticanja ET/EN;
- s mogućnošću detekcije (i identifikacije): (a) *nepokretnih* (*fiksnih*) ET/EN i/ili (b) *pokretnih* ET/EN (pri njihovu prijenosu ili pri prijevozu) te
- s mogućnošću: (a) *skoro trenutačne*; (b) *vrlo*/*dovoljno brze* i (c) *relativno spore* (s prevencijskog motrišta prespore) detekcije (i identifikacije) ET/EN.

4.1. Tehnički sustavi za detekciju mase možebitne eksplozivne tvari/naprave

U suvremene, aktualno rabljene i dalje usavršavane ili tek razvijane tehničke sustave za *detekciju mase* možebitne eksplozivne tvari/naprave ubrajaju se svi oni koji funkcioniraju na bilo kojoj od sljedećih pet osnova (Caygill, Davis i Higson, 2012.; Purišić, 1997.; Petersen, 2012.; Sk. a., 2007a, 403.; Sk. a., 2004a, 73.; Sk. a., 2006.):[510]

- na osnovi *analize rendgenskim zrakama* (tipa *kompjutorske tomografije*/CT, *transmisijske*,[a] *dvojne* (*dualne*) *energije*,[a] *povratnog raspršenja*,[a] *fokusiranih rendgenskih zraka*,[b] *pulsirajućih izvora*,[b] *izvora visoke razine toka*[b] i *detektora za daljinsku detekciju*[c]);
- na osnovi *neutronske analize* [tipa *termičke neutronske analize* (*Thermal Neutron Analysis* – TNA), *brze neutronske analize* (*Fast Neutron Analysis*), *pulsirajuće brze*

---

suvremeni tehnički sustavi daljinske detekcije i identifikacije ET/EN omogućuju možebitno nešto nižu razinu vjerojatnosti uspješne detekcije (i identifikacije), ali uglavnom nisu pregledavanim osobama neprihvatljivo tehnički invazivni, troše znatno manje vremena i pružaju znatno bolju zaštitu operaterima sustava dovoljnim sigurnosnim razmakom.

[510] Radi nestandardiziranosti/neujednačenosti dijela rabljenih ili nepostojanja dijela hrvatskih naziva za pojedine novije vrste navedenih tehnika i radi lakšeg korisničkog pretraživanja anglo-američkih stručnih literaturnih izvora (pa i primjene pogodnijeg/stručno pravilnijeg hrvatskog nazivlja za njih), u zagradama su navedeni i njihovi izvorni/uobičajeno rabljeni anglo-američki nazivi i akronimi (autor je ponajviše rabio stručne rječnike Kaštelan-Macan, 2014. i Popović, Tonejc i Mihaljević, 2014.).

Napomene uz nazive dijela pobrojanih detekcijskih sustava:

[a] Tehnologija s mogućnošću primjene za detekciju ET i/ili EN ujedno i sa stanovite manje udaljenosti.

[b] Tehnologija/e u stadiju daljnjeg istraživanja i razvitka radi poboljšanja detekcijske osjetljivosti i selektivnosti te dometa moguće detekcije sa stanovite manje udaljenosti.

[c] Posebne izvedbe detektora u daljem razvitku, pogodne za daljinsku detekciju ET i/ili EN.

neutronske analize (*Pulsed Fast Neutron Analysis* – PFNA), *pulsirajuće brze toplinske neutronske analize* (*Pulsed Fast Thermal Neutron Analysis*), *neutronske analize vremena proleta* (*ToF*) *pridruženih α čestica* (*Associated α Particles – Time-of-Flight Neutron Analysis*), *povratnog raspršenja neutrona* i *neutronske rezonancije*];

- *analize elektromagnetskim oslikavanjem* (pomoću *IC, terahertz, mikrovalnog* ili *radarskog* zračenja)[a] te *posebnim tehnikama* (poput *analize dobivene slike, kombiniranja detektora, iluminatora, osjetljive pasivne detekcije* i *sintetičkih blendi*) *usavršene analize elektromagnetskog oslikavanja* pomoću *IC, terahertz* i *mikrovalnog zračenja*[b];
- *elektromagnetskom analizom* [tipa *nuklearne kvadripolne rezonancije* (*Nuclear Quadruple Resonance* – NQR), *nuklearne magnetske rezonancije* – NMR, ESR i *magnetskim poljem* uz pomoć iznimno osjetljivih magnetometara razvijenih npr. na osnovi *mikroelektromehaničke*/MEMS tehnologije] i
- *analize gama (ɤ) zrakama* (tipa *transmisijske* i *povratnog raspršenja*).[511]

4.2. Tehnički i biološki sustavi za detekciju tragova možebitne eksplozivne tvari

U suvremene, aktualno rabljene i dalje usavršavane ili tek razvijane tehničke ili biološke sustave za *detekciju tragova* možebitne eksplozivne tvari (neke od njih i za *prepoznavanje* njene *vrste*) ubrajaju se svi oni koji funkcioniraju na bilo kojoj od sljedeće tri osnove (Caygill, Davis i Higson, 2012.; Ruffin i Yin, 2013.; Sk. a., 2007a, 403.; Sk. a., 2004a, 73.; Sk. a., 2006.):

- na osnovi *elektroničke/kemijske analize* [tipa: „*elektroničkog nosa*“, tj. *olfaktorne* (na osnovi *površinskog akustičkog vala*/*surface acoustic wave* – SAW, tj. detektora obloženih različitim poluselektivnim polimernim slojevima; *mikroelektromehaničkih sustava*/ *microelectromechancial systems* – MEMS; *mikrokonzolnih senzora*/*microcantilever sensors*; *optike vlakana* i *senzorskih zrnaca*; *polimernog tankog filma*; *nanogrozdova* u obliku *metal-izolator-metal sklopova*/*metal-insulator-metal ensembles* – MIME; *pojačanog prigušenja kromofora u fluorescentnih polimera*/*quenching amplifying fluorescent polymers* – AFP);[c] *raspoređene mreže* senzora detektora tipa „elektroničkog, kemijskog, biološkog ili optičkog nosa“;[b] *plinske kromatografije* sa *spektroskopijom ionske pokretljivosti* (GC+IMS); *spektrometrije ionske pokretljivosti s ionskom klopkom* (*ion trap mobility spectrometry* – ITMS); *plinske kromatografije* s *detektorom za zahvat elektrona* (*Electron Capture Detector* – ECD) – (GC+ECD); *plinske kromatografije* s *detektorom kemijske luminiscencije*; *razdiobnih mikrorezonatora*;[b] *plinske kromatografije* s *površinskim akustičnim valom*; *termo redoksa*; *spektrometrije s emisijom iona s pomoću polja*

[511] Kraći ili opsežniji opisi (mogućih inačica) tehničke izvedbe, počela funkcioniranja, prepoznatih detekcijskih i uporabnih prednosti i nedostataka kod pojedinih ili kod skupina popisom navedenih i ostalih mogućih tehničkih i inih vrsta detekcijskih (i identifikacijskih) sustava dani su popisom literature navedenim radovima: Chizhik, Kupriyanov i Mozzhukhin, 2015.; Daniels, 2010.; Divin et al., 2015.; Fraden, 2016.; Garibbo i Palucci, 2014.; Griffiths i Baker, 2007.; Havens et al., 2016.; Liu, Wang, i Shu, 2011.; Hallowell, 2008.; Kapilevich, Harmer i Bowring, 2015.; Malka, Rosenwaks i Bar, 2014.; Miao et al., 2010.; Pellegrino, Holthoff i Farrell, 2015.; Purišić, 1997.; Senesac i Thundat, 2008.; Sharma, Kutner i D’Souza, 2012.; Sk. a., 2015.; Sk. a., 2014.; Sk. a., 2014a; Sk. a., 2014b; Sk. a., 2014c; Sk. a., 2009.; Sk. a., 2009a; Sk. a., 2008.; Sk. a., 2007a.; Sk. a., 2007b.; Sk. a., 2007c.; Sk. a., 2004.; Sk. a., 2004a; Sk. a., 2004b; Sk. a., 1998.; Tesař i Smyk, 2015.; Thurman, 2006.; Yarovoy, 2009. i Yinon i Zitrin, 1981.

(*Field Ion Spectrometry* – FIS); MEMS;[b] *plinske kromatografije* s *masenom spektrometrijom* – GC+MS; *tekućinske kromatografije visoke djelotvornosti* – HPLC; *kapilarne elektroforeze* – CE];

- na osnovi *optičke analize* [tipa: *transmisijske i refleksijske spektroskopije*; *optoakustičke* (OA)/(*laserske*) *fotoakustičke spektroskopije* (LPAS/PAS);[c] *fototoplinskim oslikavanjem* (*photothermal imaging*);[c] *CRD spektroskopije* (*Cavity Ring Down Spectroscopy* - CRDS); *detekcije svjetlosnog* (tj. pulsirajućeg laserskog) *zračenja i razvrstavanja* (povratnog raspršenog zračenja od uzorka; *Light Detection and Ranging* – LIDAR);[c] *spektroskopije laserom inducirane disocijacije* molekula i stvaranja mikroplazmi (*laser-induced breakdown spectroscopy* – LIBS);[c] *diferencijalne apsorpcijske* LIDAR (*Differential absorption* LIDAR – DIAL);[c] *diferencijalne refleksijske* LIDAR (*Differential reflectance* LIDAR – DIRL);[c] *nelinearne optičke* (tj. međusobnim djelovanjem pobuđujućeg svjetlosnog/laserskog zračenja u plinovitim i čvrstim tvarima);[c] nekom metalnom *površinom potpomognuta Ramanova raspršivanja* (*surface enhanced Raman spectroscopy* – SERS);[b] *koherentnog anti-Stokes Ramanova raspršivanja* – CARS (*Coherent anti-Stokes Raman scattering* – CARS);[b] *senzora Fourierove transformacije IC* (*Fourier Transform infrared – FTIR sensors*);[b] *UV/VIS apsorpcijske metode* uz uporabu CRDS, *Ramanovog raspršivanja* uz uporabu *lokalizirane rezonancije površinskog plazmona* (*localized surface plasmon resonance* – LSPR) i OA spektroskopije;[b] *konjugacijom optičke faze* (*Optical Phase Conjugation*);[b] *koherentne kontrole* posebnih stanja molekula i optimiranja njihove luminiscencije uz pomoć pulsirajućih ultrakratkih laserskih zraka (*Coherent Control*)[b]] i
- na osnovi *biosenzorske analize* (uz pomoć posebno uvježbanih *pasa*,[512] *svinja, pčela, štakora, dupina, morskih lavova* ili uz pomoć pogodnih *antigena antitijela, robotskih insekata*,[b] *biljaka, mikroorganizama*).[513]

4.3. Sustavi za moguće tajno obilježavanje eksplozivnih tvari

U sustave za moguće tajno proizvođačko obilježavanje vojnih i gospodarstvenih (komercijalno dostupnih) eksploziva, poradi olakšavanja njihove detekcije u slučaju otuđenja, nezakonite trgovine ili možebitne zloporabe takvih proizvoda u sklopu IEN, ubrajaju se svi oni namijenjeni: (a) *prijeeksplozijskoj detekciji skrivene ET* ili (b) *poslijeeksplozijskoj* (*posteksplozijskoj*) *identifikaciji vrste i podrijetla zlorabljene ET*.

Kao *tajni obilježivači* (*markeri*, eng. *taggants*), više ili manje pogodni za *prijeeksplozijsku detekciju eksploziva*, predlagane, istraživane, usavršavane i (u određenom dužem ili kraćem razdoblju) pokusno rabljene su sljedeće tvari: (a) *hlapljive kemikalije*, (b) stanoviti *izotopi* kemijski identičnih tvari u sastavu ET ili mu dodani, (c) stanovite *elektromagnetske tvari* i (d) *umjetne biološke tvari* (umjetno stvorene biološke molekule, fragmenti DNK i druge tvari dobivene primjenom inih procesa biotehnologije).

Tajni obilježivači za poslijeeksplozijsku identifikaciju eksploziva i izvora opskrbe se mogu dodati u različitim pogodnim stadijima procesa proizvodnje i distribucije eksploziva i mogu

[512] Njihove komparativne prednosti i nedostatke u odnosu na instrumentalne metode detekcije vidi u: Mooney, 2015.; Petersen, 2013., 242.; Stewart, 2010.; Sk. a. 2007a, 404-406.
[513] Vidi napomene u bilješkama 51 i 52.

na različite načine sadržavati istražno vrlo vrijedne informacije. Za tu su namjenu predlagane, istraživane, usavršavane i (u određenom dužem ili kraćem razdoblju) pokusno rabljene sljedeće tvari ili metode/tehnike: (a) *mikroskopske valjkaste, na vrlo visoke temperature dovoljno otporne polimerne čestice sa slojevima u bojama, koje mogu „preživjeti" uvjete eksplozije* (poput u višegodišnjoj praksi dokazanog obilježivača „HF6" švicarske proizvodnje), (b) *mikroskopska polimerna zrnca različitih veličina i boja, dovoljno otporna na vrlo visoke temperature*, (c) *elementi rijetkih zemalja u sintetskoj matrici pomiješani s fluorescentnim pigmentima i željezom u prahu*, (d) *metoda znakovitog omjera izotopa* i (e) *tehnike imunološke analize*.

Naravno, komercijalno najprihvatljivijima se drže oni *tajni obilježivači* koji su *pogodni za obje namjene* i koji su pritom dovoljno jeftini i sigurni za predviđenu uporabu pojedinih vrsta eksploziva, kao i za okoliš držanja i uporabe (detaljnija obilježja nekih ili većine spomenutih vidi u Kulišić, 1991.; Sk. a., 1998a; Sk. a., 1997.; Sk. a., 2007a, 409-410. i Yinon i Zitrin, 1981., 238-240.).

5. ZAKLJUČAK

Suvremeni razvitak znanosti i tehnologije, stvorio je, nažalost (što se neprestance ponavlja tijekom cijele povijesti ljudske civilizacije), ujedno i mogućnosti i za iznimno opasne zloporabe mnoštva općecivilizacijski iznimno vrijednih dosega i plodova tog razvitka u obliku mnoštva donedavno ili zasad još nepoznatih, novih, iznimno pogibeljnih ili čak civilizacijski dalekosežno pogubnih djelovanja, kako u razdobljima rata, političkih i socijalnih kriznih stanja ili zaoštrenih napetosti tako i u razdobljima (prividnog lokalnog ili regionalnog) mira i stanovite društvene stabilnosti. Među inima, i za još sofisticiranije taktičke inačice i *moduse operandi* (združenog ili povremeno interesno uzajamno podupirućeg) djelovanja međunarodnog, transnacionalnog i/ili regionalno nazočnog i djelujućeg *visokotehnološkog terorizma* i *visokosofisticiranog kriminala*. Takve pogibelji zahtijevaju vrlo pozorne i pravodobne/stalno ažurne stručne raščlambe opasnosti i prosudbe ugroza i rizika kako bi se potom pronašla i primijenila dovoljno djelotvorna rješenja prevencije/sigurnosti, obrane i zaštite za svaku prepoznatu vrstu takvih pogibelji. Ta zadaća zahtijeva, među inim, i barem jednako multidisciplinaran znanstveno i tehnološki visokoučinkoviti pristup rješavanju pitanja novim pogibeljima primjerenog ustroja, međusobne suradnje, koordinacije i taktike djelovanja te primjenu visokosofisticiranih, znatno učinkovitijih tehničkih rješenja i sredstava opreme sustava sigurnosti, obrane i zaštite u sklopu svih sastavnica sustava nacionalne sigurnosti.

Djelatnost sustavnog stalnog praćenja rezultata novih znanstvenih istraživanja i dosega razvitka novih sigurnosno i zaštitno zanimljivih (možebitno lako zlorabivih ili preventivno primjenjivih) tehnologija je *conditio sine qua non* pravodobnosti i učinkovitosti preventivnog djelovanja i reagiranja svakog suvremenog sustava nacionalne sigurnosti, obrane i zaštite.[514]

Radom predočene suvremene (dijelom visokotehnološke ili visokosofisticirane) vrste ili oblici pogibelji od terorističke ili ine organizirane ili individualne zločinačke zloporabe najraznovrsnijih eksplozivnih (ali i inih vrsta općeopasnih ili masovno ubojitih i

[514] Vidi primjerice ciljeve i načine sustavne raščlambe takve vrste i namjene u Jackson i sur., 2007., Sk. a., 2014a, Sk. a., 2010., Sk. a., 2010a i Sk. a., 2005.

uništavajućih) sredstava u napadima na objekte kritične euroatlantske, europske, regionalne, transgranične, nacionalne ili lokalne infrastrukture, na posebno štićene, važne ili društveno ugledne osobe, skupine osoba, pokretne i nepokretne objekte, kao i na mjesta masovnijeg okupljanja i zatjecanja građana, tvori posebno složen izazov za sve sastavnice, kako svjetskog, euroatlantskog i europskog tako i svakog nacionalnog, sustava sigurnosti, obrane i zaštite angažirane na zadaćama *društvene prevencije pojavnosti terorizma* i *oružanom nasilju sklonoga organiziranog kriminala*, *defenzivnog djelovanja* (*antiterorizma* i *obrane od najopasnijih MOS organiziranoga kriminala*) ili (međusobno usklađenog ili združenog) *ofenzivnog protuterorističkog* ili *protukriminalnog djelovanja*.

Mnogobrojni uspješno izvedeni i neki (javno poznati), zamalo uspjeli teroristički napadi inovativnim metodama skrivanja i prijenosa/provoza te (zasada) tek s većinom relativno jednostavnijim tehnikama izvedbe skoro svih sastavnica eksplozivnih naprava, pokazali su sve aktualne slabosti standardno rabljenih sustava obrambene taktike i nadzorne (ponajprije detekcijske) tehnologije te su potaknuli na znatna ulaganja u istraživanje u razvitak novih, pouzdanijih multisenzorskih tehnologija za pravodobno otkrivanje (i identifikaciju mogućih sastavnica) takvih masovno ubojitih i razornih sredstava, kako pri bliskoj kontroli putničkog i robnog prometa tako i na što je moguće većim udaljenostima od lako mogućih meta samoubilačkog[515] i daljinski navođenog i/ili aktiviranog napada. Glede već dokazanih ili vrlo obećavajućih *blizinskih* ili *daljinskih detekcijskih sposobnosti*, poput analize *rendgenskim zrakama tipa povratnog raspršenja*, *elektromagnetskim oslikavanjem* pomoću *terahertz*, *mikrovalne* i *radarske* tehnologije, na osnovi *optičke analize* tipa LIDAR, LIBS i nekih inih, postoji stanovita/ozbiljna zabrinutost (stručne) javnosti glede (lako) mogućeg odgođenog ili dugoročnog štetnog utjecaja zračenja takvih tehničkih sustava za njihovo zdravlje pri kretanju po zonama štićenim takvim tehničkim sustavima ili pri prolazu kroz prostore (a ponajprije kroz kontrolne portale) opremljene s takvim vrstama tehničkih sustava protuterorističkog (protueksplozijskog/protudiverzijskog) nadzora. Zbog toga se istraživanja i usavršavanja učinkovitosti te ispitivanja možebitnih štetnih utjecaja za zdravlje ovih, ali i inih ovim radom spomenutih novijih metoda i tehnika, i dalje vrlo intenzivno nastavljaju.

Pritom se nastoji razviti i usavršiti detekcijski još osjetljivije, na lažne alarme znatno manje osjetljive kompleksne viševrsne multisenzorske sustave skeniranja i većih javnih prostora, poput autobusnih i željezničkih kolodvora, zračnih luka, podzemnih željeznica, športskih arena, gradskih trgova, trgovinskih središta, tržnica itd., poradi ranog otkrivanja, pravodobnog prosljeđivanja upozorenja/sumnji nadležnim službama sigurnosti, videosnimanja i po mogućnosti stalnog videopraćenja puta kretanja i sredstava prijevoza istodobno i većeg broja osoba koje možebitno nose/prenose eksplozivne ili ine opasne tvari ili naprave za potrebe ili s namjerom izvedbe terorističkog napada. Razvitak i mjestimično instaliranje takvih sustava nadzora uzrokuju povremene prosvjede dijela javnosti zabrinute za zakonom zajamčenu zaštitu osobne privatnosti, poglavito u svim onim razdobljima dugotrajnijeg izostanka bilo kakvih terorističkih ili inih oružano nasilnih (razbojničkih) kriminalnih aktivnosti.

---

[515] Za djelotvoran izravan obrambeni odgovor na svaki pokušaj pješačkog samoubilačkog bombaškog napada nužno je raspolagati s brzo reagirajućim, dovoljno osjetljivim tehničkim sustavom za pouzdanu detekcije ET/EN dometa od najmanje preko 10 do oko 100 m kako bi postojali minimalni izgledi za pravodobno uspješno zaustavljanje pokušaja prilaza na takvu napadajnu aktivnost sumnjive osobe, prije njegova pokušaja aktiviranja EN (prema Sk. a., 2006., 18-19.).

LITERATURA

Burns, M.G. (2016). *Logistics and Transportation Security: A Strategic, Tactical, and Operational Guide to Resilience*. Boca Raton (FL): CRC Press.

Caygill, J.S., Davis, F., Higson, S.P.J. (2012). Current trends in explosive detection techniques. *Talanta*, 88, 14-29. (doi:10.1016/j.talanta.2011.11.043).

Chizhik, V.I., Kupriyanov, P.A., Mozzhukhin, G.V. (2015). On Question of Possibilities of NMR in Weak Magnetic Fields for Detection of Illicit Liquids, Ch. 14, U: *Nanotechnology in the Security Systems* (NATO Security through Science, Series – C: Environmental Security), Bonca, J., Kruchinin, S. (Eds.). Dordrecht: Springer, 151.-164.

Cooper, P.W. (1996). *Explosives engineering*. New York (NY): Wiley-VCH, 59.

Crippin, J.B. (2006). *Explosives and Chemical Weapons Identification* (*Forensic Science Techniques Series*). Boca Raton (FL): CRC Press.

CTTSO/TSWG (2007). *Indicators and Warnings on Homemade Explosives*, Technical Support Working Group (TSWG), Training Technology Development Subgroup (CTTSO), Washington (D.C.): Government Printing Office (For Official Use Only).

Daniels, D.J. (2010). *EM Detection of Concealed Targets*. Hoboken (NJ): John Wiley & Sons, Inc.

Demortier, G. (2003). The Nobel Laureates in Physics (1901 - 2001), U: *A Century of Nobel Prize Recipients: Chemistry, Physics, and Medicine*. Leroy, F. (Ed.). New York (NY): Marcel Dekker, Inc., 120.

Divin, Y. et al. (2015). Screening of Liquids with Quasioptical High-T_c Josephson Detectors, Ch. 15, U: *Nanotechnology in the Security Systems* (NATO Security through Science, Series – C: Environmental Security), Bonca, J., Kruchinin, S. (Eds.). Dordrecht: Springer, 165.-179.

Fraden, J. (2016). *Handbook of Modern Sensors: Physics, Designs, and Applications*, 5th Ed., Heidelberg: Springer.

Garibbo, A., Palucci, A. (2014). Photonics for Detection of Chemicals, Drugs and Explosives, Ch. 6, U: *Photonics for Safety and Security*. Cutolo, A., Mignani, A.G., Tajani, A. (Eds.), Hackensack (NJ): World Scientific.

Griffiths, H.D., Baker, C.J. (2007). Radar Imaging For Combating Terrorism, U: *Imaging for Detection and Identification* (NATO Security through Science, Series – B: Physics and Biophysics), Byrnes, J. (Ed.). Dordrecht: Springer, 29.-48.

Havens, T.C. et al. (2016). Computational Intelligence Methods in Forward-Looking Explosive Hazard Detection, U: *Recent Advances in Computational Intelligence in Defense and Security*. Abielmona, R., Falcon, R., Zincir-Heywood, N., Abbass, H.A. (Eds.). Heidelberg: Springer, 13.-44.

JIEDDO COIC MID (2012). *Global IED monthly summary report*, Joint Improvised Explosive Device Defeat Organization (https://publicintelligence.net/jieddo-global-ieds-aug-2012/ (15. siječnja 2016.).

Liu, Y., Wang, W., Shu, W. (2011). Nanomechanical Cantilever Sensors: Theory and Applications, Ch. 3, U: *Nanosensors: Theory and Applications in Industry, Healthcare and Defense*, Lim, T.-C. (Ed.). Boca Raton (FL): CRC Press, 86.-96.

Hallowell, S.F. (2008). Explosives Trace Detection. U: *"Putting First Responders First"* (*Conference PowerPoint Presentation*). Transportation Security Laboratory, U.S. DHS Science and Technology Directorate, January 14, 2008.

Hesterman, J. (2015). *Soft Target Hardening: Protecting People from Attack*. Boca Raton (FL): CRC Press.

Houghton, L.R. (2008). *Emergency Characterization of Unknown Materials*. Boca Raton (FL): CRC Press.
Houghton, R. (2009). *Field Confirmation Testing for Suspicious Substances*. Boca Raton (FL): CRC Press.
Jackson, B.A. et al. (2007). *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*. Santa Monica (CA): RAND Corporation.
Kapilevich, B.Y., Harmer, S.W., Bowring, N.J. (2015). *Non-Imaging Microwave and Millimetre-Wave Sensors for Concealed Object Detection*. Boca Raton (FL): CRC Press.
Kaštelan-Macan, M. (2014). *Enciklopedijski rječnik analitičkoga nazivlja*. Zagreb: Fakultet kemijskog inženjerstva i tehnologije (FKIT) i Mentor, d.o.o.
Klitou, D. (2014). Body Scanners: A Strip Search by Other Means?, Ch. 5, U: *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st* Century (Information Technology & Law Series). Hague: Asser Press/Berlin: Springer-Verlag.
Krešić, Ž. (1998). Sigurnosni (protudiverzijski) pregledi starih, nemoćnih i osoba sa smanjenom pokretljivošću. *Policija i sigurnost*, 7 (4), 297.-301.
Kulišić, D. (2007). Uvod u oružja i moduse operandi suvremenog terorizma (*PowerPoint* prezentacija). *Seminar za stručno usavršavanje djelatnika državnih tijela i službi sigurnosti i zaštite*, Zagreb, 11. – 12. prosinca 2007., sl. 2-4/196.
Kulišić, D. (2003). *Metodika istraživanja požara i eksplozija*. Skripta tadašnjeg istoimenog sveučilišnog i specijalističkog diplomskog kolegija na Visokoj policijskoj školi MUP-a RH, Zagreb (*samoizdat*, uk. 497 str.), 365.-373.
Kulišić, D. (2001). Diskretne indicijalno-dokazne značajke paleži i podmetnutih eksplozija radi stjecanja materijalne koristi, Zbornik radova: *"Istraživački dan VPŠ 2000."*, Policijska akademija, Visoka policijska škola, Zagreb, 2. ožujka 2001., str. 20.-33.
Kulišić, D. (1997). Sabotaže i diverzije – Opasni klasični, glavni suvremeni i, nažalost, još važniji i pogibeljniji budući *modusi operandi* vojnih, civilnih i gospodarstvenih doglasnih službi te terorističkih, gerilskih, pobunjeničkih i kriminalnih ustrojbi, udruga i ekstremnih pojedinaca, *Policija i sigurnost*, 6, 1-2: 57.-131.
Kulišić, D. (1994). *Diverzije i sabotaže: Značajke i neki aspekti učinkovitijeg preveniranja, otkrivanja i rasvjetljavanja na primjeru industrije i transporta*. Skripta tadašnjeg istoimenog sveučilišnog i specijalističkog diplomskog kolegija na Fakultetu kriminalističkih znanosti/Visokoj policijskoj školi MUP-a RH, Zagreb (*samoizdat*, uk. 219. str.).
Kulišić, D. (1993). Eksplozijske i požarne opasnosti od velikih količina amonij-nitrata i nekih njegovih smjesa (III. dio), *Policija i sigurnost*, 2 (1-2), 34.-56.
Kulišić, D. (1992). Eksplozijske i požarne opasnosti od velikih količina amonij-nitrata i nekih njegovih smjesa (II. dio), *Policija i sigurnost*, 1 (5-6), 465.-480.
Kulišić, D. (1992a). Eksplozijske i požarne opasnosti od velikih količina amonij-nitrata i nekih njegovih smjesa (I. dio), *Policija i sigurnost*, 1 (4), 322.-337.
Kulišić, D. (1991). Značenje nutarnjih obilježivača eksploziva za kriminalističku istragu slučajeva eksplozija eksplozivnih naprava, *Priručnik*, 39, 1: 413.-414.
Malka, I., Rosenwaks, S., Bar, I. (2014). Laser-Based Detection of Explosives and Related Compounds, Ch. 12 U: *Detection of Chemical, Biological, Radiological and Nuclear Agents for the Prevention of Terrorism: Mass Spectrometry and Allied Topics* (NATO Security through Science, Series – A: Chemistry and Biology). Banoub, J. (Ed.). Dordrecht: Springer.
Miao, W. et al. (2010). Trace Detection of High Explosives with Nanomaterials, Ch. 7, U: *Trace Analysis with Nanomaterials*. Pierce, D.T., Zhao, J.X. (Eds.). Weinheim: WILEY-VCH Verlag GmbH & Co. KGaA, 161.-190.
Mooney, C. (2015). *Remarkable Military Animals (Ready for Military Action)*. Minneapolis (MI): Abdo Publishing.

MUP RH (2010). Eksplozije, Gl. 8., U: *Priručnik za kriminalističke tehničare*, Zagreb: Centar za forenzična ispitivanja, istraživanja i vještačenja „Ivan Vučetić“, 97.-104.
MUP RH (2005). *Upute za uzorkovanje tragova eksplozivnih tvari za analizu instrumentom «Itemiser»*. Zagreb: Centar za kriminalistička vještačenja MUP-a RH.
NCC (2005). *IED Trigger Recognition Guide*, 2nd Ed., Washington (DC): U.S. National Counterterrorism Center (For Official Use Only).
OTA (1991). *Technology Against Terrorism: The Federal Effort* (*OTA-ISC-481*). U.S. Congress, Office of Technology Assessment (OTA), Washington (DC): U.S. Government Printing Office, 33.-51.
Pellegrino, P.M., Holthoff, E.L., Farrell, M.E. (2015). *Laser-Based Optical Detection of Explosives* (Devices, Circuits, and Systems series). Boca Raton (FL): CRC Press.
Petersen, J.K. (2012). *Handbook of Surveillance Technologies*, 3rd Ed., Boca Raton (FL): CRC Press.
Petersen, J.K. (2013). *Introduction to Surveillance Studies*. Boca Raton (FL): CRC Press.
Popović, S., Tonejc, A., Mihaljević, M. (2014). *Rječnik kristalografije, fizike kondenzirane tvari i fizike materijala*. Zagreb: Institut za hrvatski jezik i jezikoslovlje.
Purišić, A. (1997). *Uređaji i oprema za protueksplozijsku zaštitu*. Zagreb: Policijska akademija MUP-a RH.
Ruffin, P.B., Yin, S. (2013). Nano-Optical Sensors for Explosive Detection, Ch. 22, U: *Optochemical Nanosensors* (Series in Sensors). Cusano, A. et al. (Eds.). Boca Raton (FL): CRC Press, 566.
Senesac, L., Thundat, T.G. (2008). Nanosensors for trace explosive detection. *Materials Today*, 11 (3), 28.-36.
Sharma, P.S., Kutner, W., D’Souza, F. (2012). Molecular Imprinting for Selective Sensing of Explosives, Warfare Agents, and Toxins, Ch. 4, U: *Portable Chemical Sensors: Weapons Against Bioterrorism* (NATO Science for Peace and Security, Series – A: Chemistry and Biology), Nikolelis, D.P. (Ed.). Dordrecht: Springer, 63.-94.
Skupina autora (2015). *Airport Passenger Screening Using Backscatter X-Ray Machines: Compliance with Standards*. Committee on Airport Passenger Screening: Backscatter X-Ray Machines, National Academies of Sciences, Engineering, and Medicine, Washington (D.C.): The National Academies Press.
Skupina autora (2014). *Bioelectronic Nose: Integration of Biotechnology and Nanotechnology*. Park, T.H. (Ed.), Dordrecht: Springer.
Skupina autora (2014a). *Emerging and Readily Available Technologies and National Security - A Framework for Addressing Ethical, Legal, and Societal Issues*. Committee on Ethical and Societal Implications of Advances in Militarily Significant Technologies That Are Rapidly Changing and Increasingly Globally Accessible, NRC, Chameau, J.-L., Ballhaus, W.F., Lin, H.S. (Eds.), Washington (D.C.): The National Academies Press.
Skupina autora (2014b). *Magnetic Resonance Detection of Explosives and Illicit Materials* (NATO Security through Science, Series – B: Physics and Biophysics), Apih, T. et al. (Eds.). Dordrecht: Springer.
Skupina autora (2014c). *Terahertz and Mid Infrared Radiation: Detection of Explosives and CBRN (Using Terahertz)* (NATO Science for Peace and Security Series B - Physics and Biophysics). Pereira, M., Shulika, O. (Eds.). Dordrecht: Springer.
Skupina autora (2013). *Encyclopedia of Terrorism*, Vol. 1-2, Chalk, P. (Ed.). Santa Barbara (Ca): ABC-CLIO.
Skupina autora (2012). *Forensic Investigation of Explosions* (International Forensic Science and Investigation Series), 2nd Ed., Beveridge, A.D. (Ed.). Boca Raton (FL): CRC Press.

Skupina autora (2011). *Prudent Practices in the Laboratory: Handling and Management of Chemical Hazards – An Update*. Committee on Prudent Practices in the Laboratory, National Research Council (NRC), Washington (D.C.): The National Academies Press.
Skupina autora (2010). *Persistent Forecasting of Disruptive Technologies*. Committee on Forecasting Future Disruptive Technologies, NRC, Washington (D.C.): The National Academies Press.
Skupina autora (2010a). *Persistent Forecasting of Disruptive Technologies - Report 2*. Committee on Forecasting Future Disruptive Technologies, NRC, Washington (D.C.): The National Academies Press.
Skupina autora (2009). *Anti-personnel Landmine Detection for Humanitarian Demining: The Current Situation and Future Direction for Japanese Research and Development*, Furuta, K., Ishikawa, J. (Eds.), London: Springer.
Skupina autora (2009a). *Aspects of Explosives Detection*. Marshall, M., Oxley, J.C. (Eds.). Amsterdam: Elsevier.
Skupina autora (2008). *Detection of Liquid Explosives and Flammable Agents in Connection with Terrorism* (NATO Security through Science, Series – B: Physics and Biophysics). Schubert, H., Kuznetsov, A. (Eds.). Dordrecht: Springer.
Skupina autora (2007). *Countering the Threat of Improvised Explosive Devices: Basic Research Opportunities (Abbreviated Version)*. Committee on Defeating Improvised Explosive Devices: Basic Research to Interrupt the IED Delivery Chain, NRC, Washington (D.C.): The National Academies Press.
Skupina autora (2007a). *Counterterrorist Detection Techniques of Explosives*. Yinon, J. (Ed.). Amsterdam: Elsevier.
Skupina autora (2007b). *Detection and Disposal of Improvised Explosives* (NATO Security through Science, Series – B: Physics and Biophysics). Schubert, H., Kuznetsov, A. (Eds.). Dordrecht: Springer.
Skupina autora (2007c). *Terahertz Science and Technology for Military and Security Applications* (Selected Topics in Electronics and Systems - Vol. 46). Woolard, D.L. et al. (Eds.). Hackensack (NJ): World Scientific.
Skupina autora (2006). *Stand-off Detection of Suicide Bombers and Mobile Subjects* (NATO Security through Science, Series – B: Physics and Biophysics). Schubert, H., Rimski-Korsakov, A. (Eds.). Dordrecht: Springer.
Skupina autora (2005). *Avoiding Surprise in an Era of Global Technology Advances*. Committee on Defense Intelligence Agency Technology Forecasts and Reviews, NRC, Washington (D.C.): The National Academies Press.
Skupina autora (2004). *Electronic Noses & Sensors for the Detection of Explosives* (NATO Security through Science, Series II: Mathematics, Physics and Chemistry – Vol. 159). J.W. Gardner, J. Yinon (Eds.), Amsterdam: IOS Press, and Dordrecht: Kluwer Academic Publishers.
Skupina autora (2004a). *Existing and Potential Standoff Explosives Detection Techniques*. Committee on the Review of Existing and Potential Standoff Explosives Detection Techniques, NRC, Washington (D.C.): The National Academies Press.
Skupina autora (2004b). Mine detection, Ch. 12, U: *Ground Penetrating Radar*, 2nd Ed., Daniels, D.J. (Ed.). Herts (UK): The Institution of Electrical Engineers, 501.-624.
Skupina autora (1999). *Improving Surface Transportation Security, a Research and Development Strategy*. National Research Council (NRC), Washington (DC): National Academy Press.
Skupina autora (1998). *Black and Smokeless Powders: Technologies for Finding Bombs and the Bomb Makers*. Committee on Smokeless and Black Powder, National Research Council of

the National Academy of Sciences (NRC), Washington (D.C.): The National Academies Press.
Skupina autora (1998a). *Containing the Threat from Illegal Bombings: An Integrated National Strategy for Marking, Tagging, Rendering Inert, and Licensing Explosives and Their Precursors*. Committee on Marking, Rendering Inert, and Licensing of Explosive Materials, NRC, Washington (D.C.): The National Academies Press.
Skupina autora (1997). *Marking, Rendering Inert, and Licensing of Explosive Materials: Interim Report*. Committee on Marking, Rendering Inert, and Licensing of Explosive Materials, NRC, Washington (D.C.): The National Academies Press.
Stewart, G.B. (2010). *K-9 Police Units* (Lucent's Crime Scene Investigation series). Farmington Hills (MI): Lucent Books/Gale, Cengage Learning.
TC 9-21 (2004). *Soldiers Improvised Explosive Device (IED) Awareness Guide: Iraq and Afghanistan Theaters of Operation* [TC 9-21 (093-89D-01)]. Aberdeen Proving Ground (MD): US Army Ordnance Corps and Redstone Arsenal (AL): EOD Training Department (Unclassified/For Official Use Only).
Tesař, V., Smyk, E. (2015). Infrasonic fluidic oscillator for use in anti-terrorist warfare, U: *Safety and Security Engineering VI*, Brebbia, C.A., Garzia, F., Poljak, D. (Eds.), Southampton: WIT Press, 179.-189.
Thurman, J.T. (2006). *Practical Bomb Scene Investigation* (Practical Aspects of Criminal & Forensic Investigations). Boca Raton (FL): CRC Press.
Yarovoy, A. (2009). Landmine and Unexploded Ordnance Detection and Classification with Ground Penetrating Radar, Ch. 14, U: *Ground Penetrating Radar Theory and Applications*. Jol, H.M. (Ed.), Amsterdam: Elsevier, 445.-478.
Yinon, J., Zitrin, S. (1981). *The Analysis of Explosives* (Pergamon Series in Analytical Chemistry, Vol. 3). Oxford: Pergamon Press.
Suicide Bomb Detector Moves Forward With Sandia Engineer's Help. *Domestic Preparedness Journal* (Government Updates), March 01, 2016.

Damir Kulišić

ON CURRENT POSSIBILITIES AND PROBLEMS IN THE DETECTION AND IDENTIFICATION OF EXPLOSIVE SUBSTANCES/DEVICES

Summary

Counter-sabotage (counter-explosive) security, pre-blast or post-blast detection, identification, criminal investigation and forensic analysis of kinds and origins (used precursors/raw materials for the production) of explosive substances and other components of explosive devices, in the context of numerous criminal bomb attacks on potentially endangered, i.e. attacked (groups of) persons, buildings, public areas and vehicles, have always presented a special tactical and technical challenge, even for the technically well-equipped, educated, trained and very experienced counter-sabotage/counter-explosive officers employed in the security, defence and protection services, and often for teams of forensic examiners conducting expert evaluation of items/traces of such criminal offenses.
On the basis of the contents analysis of available contemporary foreign and domestic professional literature in the field of tactics and techniques for explosive detection, pre-blast or post-blast identification of explosive devices/substances, a concise overview is given of possible kinds, forms and varieties of such devices/substances which are important for safety, investigation and evidence collection, an overview of currently used and well-developed detection techniques of explosive devices/substances, as well as an overview of currently recognised key problems/factors which can disable or decrease the efficiency of counter-explosive security, defence and protection systems, and the efficiency of pre-blast or post-blast identification of kinds and origin of misused explosive substances and components of possible structures of misused explosive devices. This paper is a contribution to the necessary expansion and increase of professional knowledge of all security and protection officers as well as of trainee criminal and forensic investigators, especially in these hard times of terrorist bombing campaigns all over the world and/or in our near and far neighbourhood.

Key words: *chemical explosions in condensed phase, improvised explosive devices, explosive substances, detection and identification of explosive substances/devices, forensics of explosive substances/devices.*

STRUČNI RAD

Darko Dundović[516]

NEISKORIŠTENE MOGUĆNOSTI PRIVATNOG SEKTORA U PODIZANJU RAZINE JAVNE SIGURNOSTI

Sažetak

Brzi razvoj tehnologije omogućio je kompanijama da koriste razne sustave tehničke zaštite u cilju zaštite svojih zaposlenika, preveniranja krađa i drugih štetnih događaja, ali i praćenja poslovnih procesa. Svakodnevno se snima na tisuće prostora i objekata, bilježi prolazak osoba putem identifikacijski kartica, dolazaka alrama, međutim uvid u sve to uglavnom imaju zaposlenici zaštitarskih kompanija ili zaposlenici kompanija koje imaju sustave tehničke zaštite. Policija, ali niti druge sigurnosne službe nemaju direktan pristup (uvid) alarmnim sustavima, sustavima video nadzora, kontrole prolaza i dr. koje pojedine kompanije koriste bilo poradi zakonskih obveza ili poradi svojih potreba. Iako sudovi, policija i neka druga državna tijela imaju pravo zatražiti primjerice snimku video nadzora, direktan uvid u video nadzor u smislu da udaljeno mogu pristupiti nekim ili svima kamerama na nekom prostoru ili objektu nije praksa u Republici Hrvatskoj. Jedan od razloga da je tome tako je i nepostojeća zakonska regulativa, mogući troškovi, ali i nezainteresiranost sigurnosnih službi za ovakvim mogućnostima. Iako je nesporno da bi u slučaju direktnog pristupa i pregleda video nadzora policija mogla imati trenutnu sliku događaja ili prostora, a time i značajno poboljšala javnu sigurnost, osim iskustva sa „javnim kamerama" u gradovima, iskustva sa privatnim sektorom su iznimno skromna.

Ključne riječi*: sustavi tehničke zaštite, kompanije, policija*

1. UVOD

Današnji razvoj društva te sve brutalniji i učestaliji događaji koji su posljedica kriminalnih radnji utječu i na osjećaj sigurnosti pojedinaca pa tako i zaposlenika kompanija. Radi zaštite svojih zaposlenika i kupaca, ali i smanjenja šteta, kompanije postavljaju sustave tehničke zaštite na svoje objekte i prostore. S obzirom na to da je sigurnost zaposlenika i zaštita imovine jedan od osnovnih preduvjeta uspješnoga poslovanja, kompanije nastoje na različite načine zaštititi svoje zaposlenike, imovinu, ali i druge interesne dionike. Kompanije koriste, uz već spomenute sustave tehničke zaštite, tjelesnu zaštitu (zaštitare), određene mehaničke zaštite, usluge detektivskih agencija, propisane sigurnosne procedure i drugo. Sve to značajno ovisi i o djelatnosti kojom se određena kompanija bavi te koliko je velika. Čovjek i njegovo znanje i vještina najveće su bogatstvo svake kompanije, pa je i to jedan od razloga zašto kompanije ulažu u sigurnost svojih zaposlenika.

[516] mr. sc. Darko Dundović, INA, Industrija nafte, d.d.

Podatak da se danas tržište privatne sigurnosti procjenjuje na 85 milijardi američkih dolara, s godišnjom stopom rasta 6-8 posto (Abrahamsen i Williams, 2005) govori sam za sebe. Međutim taj podatak ne prati istodobno i razvoj suradnje između privatnog i javnog sektora zaduženog za javnu sigurnost u Republici Hrvatskoj i za sada taj međuodnos ne možemo nazvati "partnerskim". Cilj rada je prikaz mogućnosti jednog dijela sustava tehničke zaštite koji koristi privatna kompanija i kako te mogućnosti staviti u funkciju podizanja javne sigurnosti.

2. KORPORATIVNA SIGURNOST – OSNOVNE NAPOMENE

Poslovanje kompanije svakodnevno je izloženo različitim utjecajima: financijske krize, sve veći zahtjevi tržišta, promjene radnog zakonodavstva, poreznih pravila, štetni (kriminalni) događaji i drugo. Značajan element uspješnog poslovanja kompanije jest i "sigurnosno okruženje" u kojem kompanija posluje. Na dio tog "sigurnosnog okruženja" kompanija ne može direktno utjecati, međutim mogu se primijeniti razni alati kako bi sigurnosno okruženje u kojem posluje određena kompanija imalo što manje utjecaja i činilo što manje šteta kompaniji. Poradi toga i drugih razloga, dio kompanija razvija i strategiju korporativne sigurnosti. Glavni cilj korporativne sigurnosti u kompaniji trebalo bi biti ostvarenje sigurnosti poslovnog uspjeha kompanije, što se odnosi na:

- smanjenje ili uklanjanje svih rizika i ugrožavanja koji mogu utjecati na poslovne aktivnosti i ostvarenje poslovnog uspjeha
- uspješno poslovno funkcioniranje i u uvjetima kriza
- prevladavanje kriza i nastavak normalnog poslovanja (Ivandić Vidović i sur., 2011).

Isti autori smatraju da se strategija korporativne sigurnosti u kompaniji provodi na funkcionalnoj razini i pripada jednoj od funkcijskih strategija poslovnog sustava (Ivandić Vidović i sur., 2011). Temeljem ovakvih stavova možemo se složiti da sigurnost nije tehničko već strategijsko pitanje, ugroze mogu dolaziti iz vanjske i unutarnje poslovne okoline te je taj koncept usredotočen na materijalno-tehnički i ljudski faktor. Kovachic i Halibozek (2002) navode nešto veći broj funkcija korporativne sigurnosti od kojih ćemo nabrojiti neke:

- administrativna sigurnost (engl. *Administrative Security*) koja se odnosi na procedure i politike
- tjelesna i tehnička sigurnost (engl. *Protetctive Security*) koja se odnosi na zaštitu imovine kompanije
- sigurnost vlasništva i vanjskih partnerstva (engl. *Out-Source/Proprietary*)
- osobna sigurnost (engl. *Personnel Security*) koja se odnosi na zaštitu ljudi i zaštitu na radu
- programi izobrazbe i razvoja svijesti u odnosu na sigurnost (engl. *Security Education Awareness and Training Program*) kojoj je primarna funkcija edukacija zaposlenih
- istrage (engl. *Investigations*) koje se odnose na program zaštite od kriminala
- informacijska sigurnost (engl. *Information Security*)

- sigurnost menadžera (engl. *Executive Security*)
- sigurnost na raznim poslovnim događajima (engl. *Event Security*).

Ivandić Vidović i sur. (2011) u normativni okvir korporativne sigurnosti uključuju uz spomenuto i privatnu zaštitu, zaštitu intelektualnog vlasništva, zaštitu podataka, privatnu istražnu djelatnost, *business intelligence*, sprečavanje pranja novca i financiranja terorizma, obrambene pripreme i poslove koji se odnose na zaštitu na radu i protupožarnu zaštitu (Ivandić Vidović i sur., 2011).

3. TEMELJNI ZAKONSKI I DRUGI AKTI KOJI REGULIRAJU POSLOVE PRIVATNE ZAŠTITE

Temeljni zakon koji regulira područje privatne zaštite je Zakon o privatnoj zaštiti (NN 68/03., 31/10., 139/10.). Ovaj Zakon regulira način obavljanja zaštite osoba i imovine koju ne osigurava država. U njemu se određuju ovlasti i opseg obavljanja tjelesne i tehničke zaštite. S obzirom na sadržaj rada nešto detaljnije ćemo prikazati regulativu koja se odnosi na "tehničku zaštitu". Tehnička zaštita je definirana u Pravilniku o uvjetima i načinu provedbe tehničke zaštite (NN 198/03.). Pravilnik već u članku 1. definira tehničku zaštitu kao "…skup radnji kojima se neposredno ili posredno zaštićuju ljudi i njihova imovina, a provodi se tehničkim sredstvima i napravama te sustavima tehničke zaštite kojima je osnovna namjena sprečavanje protupravnih radnji usmjerenih prema štićenim osobama ili imovini kao što su: protuprovalno djelovanje, protuprepadno djelovanje i protusabotažno djelovanje". Smatramo kako ovakav koncept daje vrlo široku osnovu za projektiranje sigurnosnih mjera i omogućuje primjenu suvremene tehnologije koja se u današnje vrijeme na području sigurnosti razvija impresivnom brzinom. Takve mogućnosti se dodatno povećavaju međusobnim "povezivanjem dvaju ili više sredstava, naprava i uređaja koji zajedno čine funkcionalnu cjelinu" (članak 2. Pravilnika). Pri tome se misli na integriranje protuprovalnih i protuprepadnih sustava s javljačima raznih izvedbi (aktivnim i pasivnim); sustava kojima se obavlja stalni nadzor nad štićenim objektom s jednog mjesta (videonadzorni sustavi); sustava centralnog prijma i signalizacije alarma; centralni dojavni sustav i centralni tehnički nadzor; integralnih sustava zaštite s najmanje jednim nadzornim mjestom unutar štićenog objekta. Iz navedenog je vidljivo da zakonske odredbe predviđaju mogućnost povezivanja svih sustava na jedno mjesto, što olakšava pristup i nadzor svih situacija i alarma, ali otvara i neslućene mogućnosti pristupa svim tim podacima iz "udaljenih lokacija" pa i osobama/institucijama koje nisu dio kompanije. Donošenjem i stupanjem na snagu Zakona o zaštiti novčarskih institucija (NN 56/15.) još su detaljnije uređene odredbe o karakteristikama (kvaliteti) opreme koja se ugrađuje u takvim institucijama. Tako kamere koje imaju funkciju identifikacije moraju imati horizontalnu rezoluciju od minimalno 330 piksela po metru, a brzina snimanja videozapisa mora biti minimalno 2 fps po kameri s minimalnom rezolucijom za "identifikacijske" kamere najmanje 4 CIF-a. (Članak 8., točka 1. i 6. Zakona.) Ovakve odredbe primorale su kompanije da ugrađuju opremu (kada govorimo o sustavima videonadzora) čija kvaliteta snimke omogućuje identifikaciju osoba, ali i bolje praćenje bilo kakvih događaja u tom prostoru. U nastavku je primjer snimke lica različitih funkcionalnosti kamera.

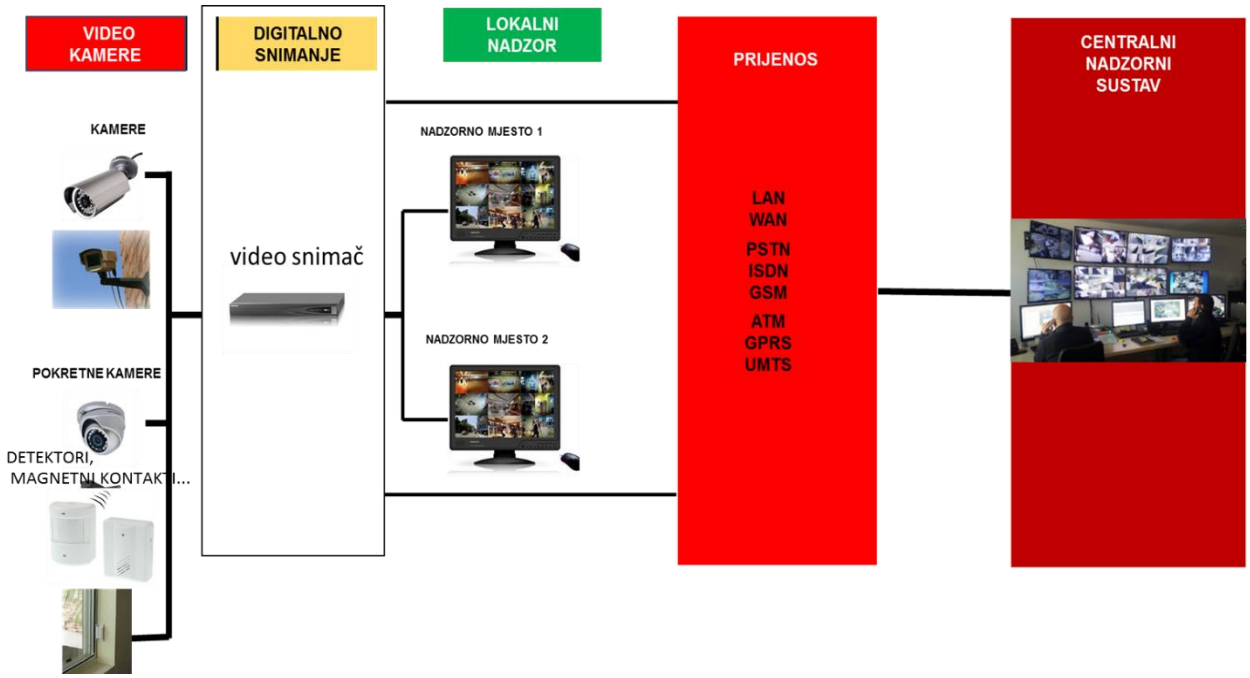
Funkcija kamere		
nadzor/detekcija	prepoznavanje	identifikacija
66 piks/m	135 piks/m	330 piks/m

Slika 1: Prikaz kvalitete snimke kod različitih funkcija kamera

4. SREDIŠNJI NADZORNI SUSTAV KOMPANIJE – FUNKCIONALNOSTI I MOGUĆNOSTI

Kompanije koje korite različite sustave tehničke zaštite, naročito one koje imaju veći broj takvih sustava uglavnom imaju jedno centralno mjesto (bilo u kompaniji bilo da su spojene na neku zaštitarsku kompaniju koja pruža takve usluge) gdje centralno zaprimaju alarme i imaju pristup svim videonadzornim kamerama.

U skladu s člankom 3. Pravilnika o uvjetima i načinu provedbe tehničke zaštite (NN 198/03.), CDS – Centralni dojavni sustav je sustav zaštite koji omogućava dojavu alarmnog signala s javljača štićenih objekata na centralni dojavni prijamnik dojavnog centra radi pružanja intervencije tjelesne zaštite. To je mjesto u koje putem sustava komunikacijskih kanala dolaze dojave sa svih sustava tehničke zaštite štićenih objekata i/ili prostora. Takav dojavni centar ili centar za nadzor ili centralni nadzorni sustav, kako se naziva u nekim kompanijama, obrađuje sve alarme odnosno alarmne situacije na jednom mjestu. Nakon zaprimanja alarmnog signala (bilo zaprimljenog alarma, primjerice za provalu ili razbojništvo ili alarmne situacije s videonadzornog sustava) signal se "obrađuje" te se upućuje interventna ekipa ovlaštene zaštitarske kuće i izvješćuje policija, a ovisno o situaciji i druge nadležne službe. Integracija različitih sustava tehničke zaštite omogućena je softverima razvijenima za tu namjenu. Cijeli sustav je izgrađen tako da alarmni uređaj šalje preko alarmne centrale informaciju o incidentu trenutno, što znači da operater u nadzornom centru odmah raspolaže s informacijom o potencijalnom štetnom događaju na mjestu odakle je došao signal. Osim što su svi alarmi vidljivi trenutno, moguće je obavljati i pregled ranije zaprimljenih i obrađenih alarma. Uz popis alarma u sustavu mogu se vidjeti i detalji o svakom pojedinačnom događaju – alarmu jer zaštitar mora upisati što je poduzeo i utvrdio (npr. upućena interventna ekipa, obaviještena policija, utvrđeno da se radi o provali, razbojništvu...). Pojednostavljeni shematski prikaz ovakvog sustava tehničke zaštite prikazujemo u nastavku.

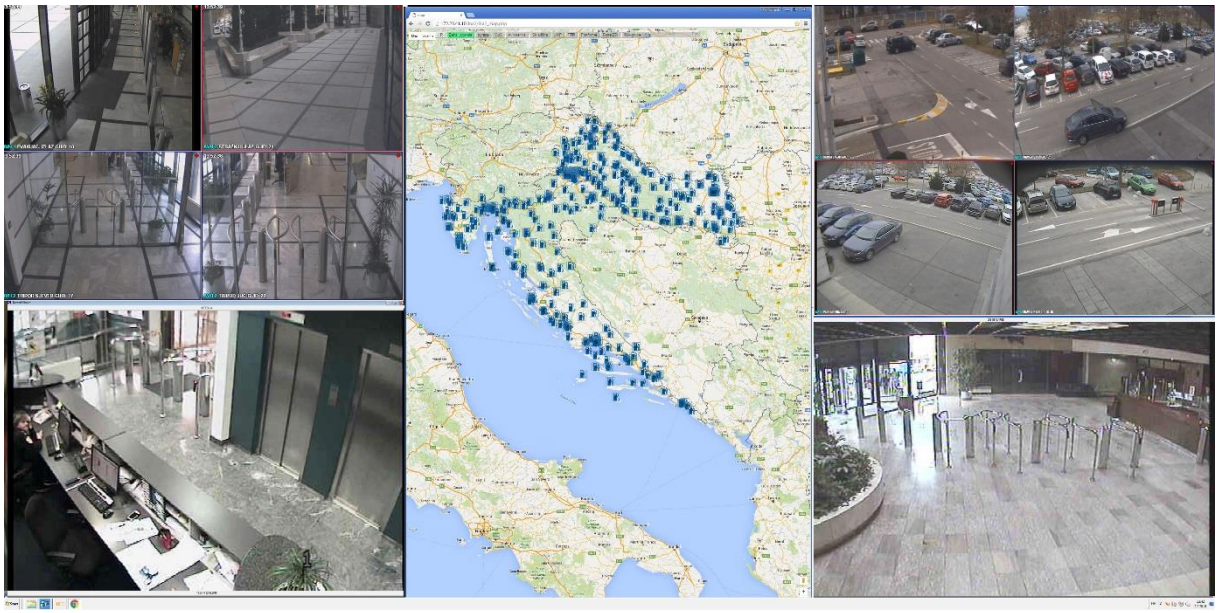


Shema 1: Pojednostavljeni prikaz sustava tehničke zaštite

Nemoguće je definirati sve incidente koje aktiviraju alarme, međutim važno je da svaki takav alarm bude trenutan kako bi reakcija i utvrđivanje zašto je do alarmne situacije došlo bila što brža. Razvoj tehnologije omogućio je da se temeljem alarma odmah povezuju kamere (ili neki drugi sustavi, npr. kontrola prolaza osoba i vozila), tako da operater odmah može vidjeti i sliku s mjesta aktiviranog alarma. Na taj način se pažnja operatera usmjerava na kritičnu situaciju na koju je potrebno reagirati odmah. Ako se radi o pokretnim kamerama i operater ima mogućnost udaljenog upravljanja kamerama, operater može dodatno fokusirati kameru na određeni događaj.

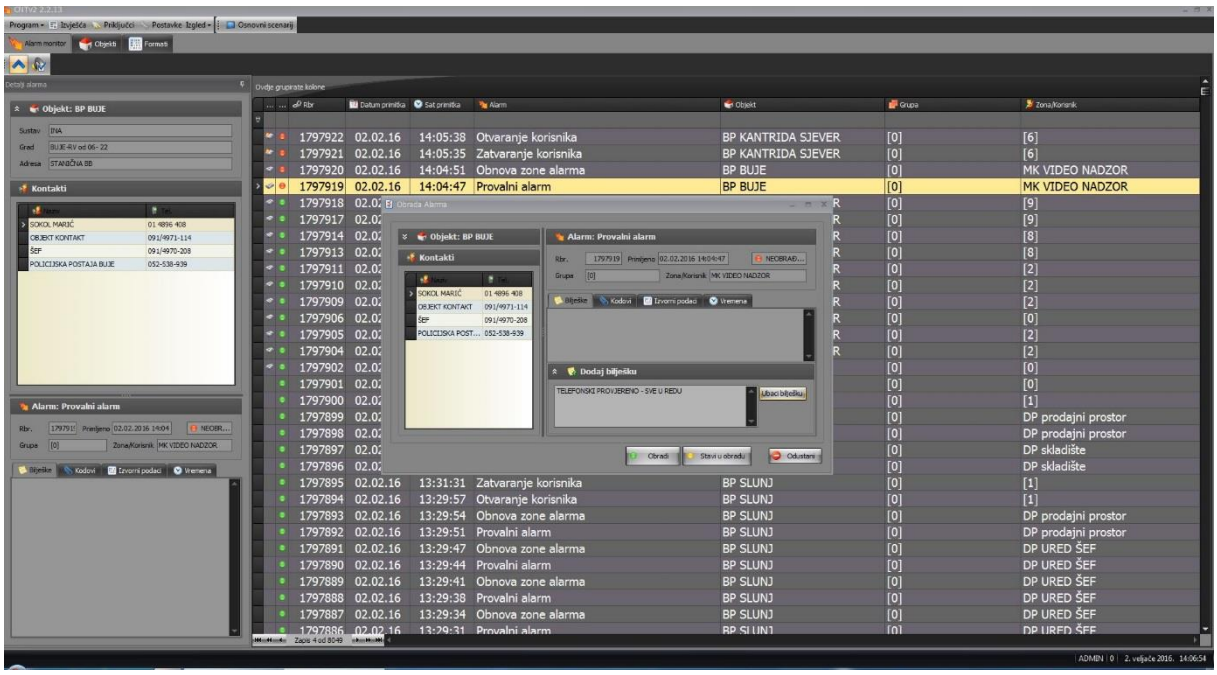
Prije prikaza i obrade cijelog postupka alarmne situacije važno je naglasiti najznačajnije karakteristike jednog takvog sustava: *trenutan prijam alarma, mogućnost udaljenog pristupa sustavu i integracija više sustava*. Upravo ove karakteristike važne su u definiranju mogućnosti korištenja ovakvih sustava tehničke zaštite privatnih kompanija za potrebe javne sigurnosti.

Kako bismo mogli prikazati sve mogućnosti korištenja jednog ovakvog sustava ukratko ćemo opisati postupak i funkcionalnosti koje se prikazuju kod zaprimanja alarma (npr. protuprovale). Slika 2 prikazuje početni zaslon na videozidu nadzornog centra.



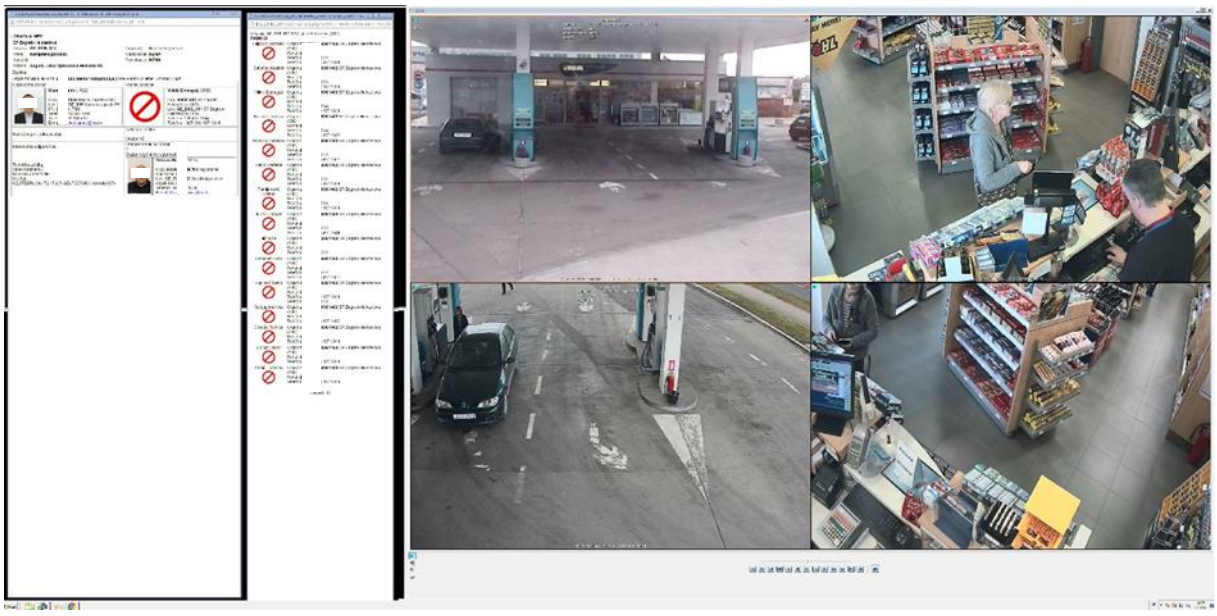
Slika 2: Početni zaslon na videozidu nadzornog centra

Nakon što se u nadzornom centru zaprimi alarm s neke lokacije (alarm je vidljiv na monitoru i daje zvučni signal), operater izvješćuje telefonom interventnu ekipu i policijsku postaju.



Slika 3: Prikaz monitora centralnog dojavnog sustava u trenutku dolaska alarma

Istodobno se na centralnom monitoru (videozidu) prikazuju sve kamere s trenutnom slikom lokacije s koje je zaprimljen alarm (slika 4). Operater osim kamera na monitoru vidi i druge podatke, točnu adresu lokacije, podatke i kontakte odgovornih osoba za tu lokaciju, tlocrt i drugo.



Slika 4: Prikaz videozida nakon prijma alarma

Prilikom pozivanja policije operater javlja točne podatke o adresi s koje je zaprimljen alarm, točnom vremenu zaprimanja alarma te o svemu što je vidljivo na videonadzoru. Ukratko, nakon zaprimanja alarma operater mora nazvati interventnu ekipu, nakon toga *nadležnu policijsku postaju (biranjem broja 192 s fiksnog telefona dobije se operativno dežurstvo najbliže policijske uprave/postaje, a signal alarma dolazi s područja neke druge policijske uprave pa je ponekad potrebno prespajanje)*. Uza sve to operater gleda kamere i pokušava opisati trenutnu situaciju na lokaciji, opisati osobe, odjeću, vozila, kretanje... . Već prilikom uspostave poziva s policijom gubi se dosta vremena u javljanju točne adrese lokacije s koje je došao alarm, a dosadašnja iskustva pokazuju da, primjerice događaji provale u benzinske postaje koje imaju sustave tehničke zaštite traju manje 2-3 minute s počinjenom štetom više od desetaka tisuća kuna, što jasno govori koliko je važno točnu informaciju prenijeti što prije. Posebno je rizično prenošenje opisa stanja temeljem videonadzora koji promatra operater i koji sve prenosi policijskom službeniku. Uz moguću subjektivnost u bilo kojem detalju opisivanja trenutne situacije s videonadzora, postavlja se pitanje može li operater (uz vremenski pritisak) odrediti koji su detalji važni u toj situaciji za policijskog službenika. Iako se za svaki događaj pohranjuje videoverifikacija koja omogućuje naknadni pregled događaja identičan onome koji operater ima u realnom vremenu, s mogućnošću vraćanja u vremenu kako bi se mogao pregledati točno određeni trenutak i u takvom naknadnom pregledu snimke od strane operatera (bez vremenskog pritiska), velika je mogućnost prenošenja nepotpune informacije.

Za potrebe ovog rada dan je samo osnovni prikaz funkcionalnosti i mogućnosti jednog ovakvog nadzornog centra privatne kompanije (konkretan primjer iz INA d.d.) i dio procedura koje su uobičajene u alarmnim situacijama. U spomenuti nadzorni centar spojeno je preko 1 700 kamera s oko dvjestotinjak lokacija te alarmi s preko 230 različitih lokacija. Iako u konkretnom primjeru dio kamera ne pokriva samo "javni prostor" (benzinske postaje, poslovne objekte...) već i prostore (unutar štićenih prostora) gdje se odvijaju poslovni procesi,

ovoliki broj kamera i alarma (a radi se samo o jednoj kompaniji) otvara velike mogućnosti korištenja za podizanje javne sigurnosti.

5. KOMPANIJSKI RESURSI – JAVNA SIGURNOST

Pojam javne sigurnosti možemo promatrati kao skup mjera i aktivnosti koje neka državna tijela (rjeđe i pojedinci, nevladine organizacije ili privatne kompanije) poduzimaju kako bi se zaštitio život, zdravlje i imovina građana nekog područja, ponajprije od kriminala, ali i od drugih događaja: prometne nezgode, požari ili prirodne katastrofe. Javnu sigurnost promatrat ćemo sa stajališta aktivnosti i radnji kojima se prije svega bavi policija kako bi se smanjio kriminalitet na javnim prostorima i objektima, gdje se nalaze sustavi videonadzora privatnih kompanija.

Uz već poznate i djelomično korištene sustave videonadzora na javnim površinama i prostorima koje je postavila i koje djelomično koristi i policija (npr. Gradska uprava Zagreba i Zagrebački holding danas u svom vlasništvu imaju oko 4 000 kamera /Ostojić, 2015/), policija u svojim aktivnostima i dalje ne koristi dovoljno kapacitete ovakvih sustava privatnih kompanija. Ostojić smatra da nepostojanje registra kamera u gradu Zagrebu, kojima bi direktan pristup imala i policija, pokazuje nedovoljnu inicijativu policije i gradskih vlasti, posebno zato što u većim gradovima u drugim zemljama uz registre gradskih i javnih kamera postoje i registri korporativnih kamera (Ostojić, 2015).

Potrebu takve suradnje naglasio je i Pavliček (2010) u svojem izlaganju na IV. konferenciji hrvatskih menadžera sigurnosti iz 2010. godine, gdje navodi da za uspostavu partnerstva javne i privatne sigurnosti treba težiti podizanju razine profesionalizma i stručne osposobljenosti svih sudionika u tom procesu. Naglasak stavlja i na svakodnevnu komunikaciju i suradnju na operativnoj razini jer se jedino na takav način može postići temeljni cilj partnerstva, bolja sigurnost građana i njihove imovine. Iako se u svojem izlaganju uglavnom bavi mogućnošću suradnje policije i privatnog sektora s naglaskom na tjelesnu zaštitu (zaštitari), Pavliček spominje i "tehničku zaštitu" gdje navodi "da sustavi videonadzora postavljeni na javnim površinama mogu značajno utjecati na sigurnost na pojedinim kriminalnim žarištima" (Pavliček, 2010). Svoj doprinos obradi ove teme u Republici Hrvatskoj dali su i Podhraški, Tršinski i Kancir (2007) koji navode da bi uvođenje videonadzora javnih prostora bio veliki napredak u metodologiji rada policije jer bi, s obzirom na sve prisutniji problem nedovoljnog broja policijskih službenika u odnosu na postojeći ustroj i problematiku, omogućio da jedan policijski službenik istodobno nadzire više javnih površina. Iz ovoga se može zaključiti da autori pretpostavljaju da bi policijski službenici obavljali nadzor nad kamerama na "javnom prostoru" što je idealno, ali porast broja takvih kamera u budućnosti bi mogao policijskim službenicima znatno otežati nadzor svih tih kamera. Iako se autori uglavnom bave suradnjom s lokalnom zajednicom i novčarskim institucijama (Zakon o zaštiti novčarskih institucija /NN 56/15./) te zakonskim mogućnostima takve suradnje i korištenja snimaka u kasnijim sudskim postupcima, u svojem radu spominju i mogućnost korištenja (i način korištenja) kamera koje su postavile (ili poradi zakonskih obaveza ili poradi vlastite zaštite) privatne kompanije. Autori smatraju da bi cijeli taj sustav već postojećih videonadzora bio potpuno funkcionalan (sa stajališta policije) samo ako se

međusobno povežu i stave pod jedinstveni nadzor u koji bi uvid imala i policija. Na taj način bi se prema istim autorima povećala efikasnost policijskih službenika, ali i mogućnosti kasnijeg dokazivanja određenih protupravnih ponašanja. Da postoji znatan napredak upravo u direktnom udaljenom pristupu kamerama od strane policije govori i činjenica da policija pristupa direktno prema 354 kamere instalirane na 118 lokacija u Zagrebu, koje je instalirao Grad Zagreb. (Kraljević, Direktno.hr, 10. 2. 2016.) Korisnost ovakvog pristupa potvrđuje i činjenica da je policija do sada izuzela tri tisuće slika ili detalja s ovih kamera.

Kako bismo mogli prikazati sve stvarne prednosti takvog sustava tehničke zaštite koje bi policija imala kada bi bila spojena na njega, koristit ćemo funkcionalnost već ranije opisanog nadzornog centra. Dakle, pretpostavimo da policija ima direktnu vezu na ovakav sigurnosni centar u koji su spojeni svi alarmi i kamere neke kompanije, s mogućnošću uvida u bilo koju kameru.

Nakon što bi do nadzornog centra došao alarm protuprepada (pretpostavimo da se radi o razbojništvu), isti takav signal zaprimila bi i policija u svojem nadzornom centru ili operativnom dežurstvu. S obzirom na to da su jasno propisane zakonske odredbe tko treba i što poduzeti nakon zaprimanja alarma, policija ne bi bila dužna reagirati sve do trenutka dok ne bi dobila obavijest zaštitara da se radi o razbojništvu. Takva procedura je i sada, samo bi u pretpostavljenoj situaciji policija imala alarm nekoliko minuta prije. Istodobno, ako se radi o razbojništvu (prethodno smo opisali da se u nadzornom centru s dolaskom alarmnog signala na centralnom videozidu prikazuju kamere s lokacije), policija bi u svojem nadzornom centru mogla vidjeti sve kamere koje se nalaze na tom objektu a time i osobe (počinitelje?) koje su na tom objektu, karakteristike i boju odjeće, obuće, maskiranost, vozila, reg. oznake, sredstva s kojim se vrši razbojništvo ako se koriste, smjer kojim odlazi počinitelj ako je razbojništvo već počinjeno, jesu li žrtve ozlijeđene i niz drugih podataka.

Raspolaganje s ovakvim podacima gotovo u realnom vremenu neprocjenjivo doprinosi ne samo brzini policijskog postupanja, nego i načinu na koji će policijski službenici postupati u konkretnom slučaju. Na ovaj način bitno se skraćuje vrijeme zaprimanja obavijesti od zaštitara, ali i smanjuje mogućnost pogreške kod dostavljanja podataka temeljem kojih policijski službenik donosi odluku o načinu postupanja. Upućivanje policijskih službenika na mjesto razbojništva gdje ih se može odmah obavijestiti o detaljima počinitelja: ima li ili nema vatreno oružje, opis odjeće koju nosi, vozilo kojim se je udaljio ili im se čak može dostaviti fotografija događaja, u potpunosti mijenja metodiku postupanja policijskih službenika kod dolaska do mjesta razbojništva. Sve ove mogućnosti dostupne su i kada se radi o provali u takve objekte. Direktnim pristupima kamera iz nadzornog centra policije "uživo" bi se mogla promatrati provala i istodobno davati upute policijskim službenicima na terenu. Važno je naglasiti da bi takvim tehničkim rješenjem bilo moguće ne samo gledanje snimke koja bi se pojavljivala u trenutku alarma, odnosno trenutne situacije, već i pregled prijašnjih događaja, pa onda i "skidanje" videozapisa, i sve to bez potrebe angažiranja korporativne sigurnosti kompanije. Danas, ako policija treba neku snimku videozapisa sa sustava videonadzora neke kompanije, dostavlja službeni zahtjev kompaniji (ponekad prethodno odlazi na lokaciju kako bi pregledala snimku i utvrdila točno vrijeme koje treba snimiti) i tada zaposlenici kompanije ili ovlašteni serviseri odlaze na lokaciju ili u nadzornom centru kompanije obavljaju snimanje. U situacijama kada treba sačuvati tajnost zahtjeva policije za snimku, ovakva trenutna

procedura veliki je rizik. Nedvojbeno je da bi ovakvim pretpostavljenim rješenjima policija imala mogućnost brže reakcije kod ovakvih događaja te neograničen pristup pregledu i snimanju videozapisa, ali treba naglasiti da postoje određene tehničke pretpostavke koje bi trebalo zadovoljiti i financijski troškovi. Jedan od preduvjeta je propusnost (engl. *bandwidth*) infrastrukture kroz koju prolazi videosignal, kako od lokacije gdje se nalaze kamere, do nadzornog centra kompanije, tako i od nadzornog centra policije do nadzornog centra kompanije. Većina te infrastrukture u vlasništvu je privatnih kompanija koje naplaćuju korištenje pa dolazimo i do financijskih troškova ovakvih rješenja i pitanja tko će platiti te troškove – policija ili privatna kompanija. S obzirom na brz razvoj tehnologija valja pretpostaviti da će troškovi svakim danom biti sve manji, a mogućnosti sve veće. U ovom radu nećemo se baviti različitim tehničkim rješenjima koja su moguća već je namjera autora samo upozoriti na moguće tehničke i financijske pretpostavke.

Osim spomenutih tehničkih i financijskih pretpostavki puno je važnije zakonsko uređenje ovog područja koje bi trebalo jasno definirati prava i obaveze svih koji bi bili dio ovog procesa, od državnih tijela, prije svega policije, do vlasnika ovakvih sustava, privatnih kompanija. Trenutno ovo područje uređuju već spomenuti Zakon o privatnoj zaštiti (NN 68/03., 31/10., 139/10.), Pravilnik o uvjetima i načinu provedbe tehničke zaštite (NN 198/03.) i Zakon o zaštiti novčarskih institucija (NN 56/15.). Kako je normativno uređeno upravo spajanje policije na sustave tehničke zaštite obveznika ovih zakona pokazuje i sljedeći primjer. U članku 20. Pravilnika o uvjetima i načinu provedbe tehničke zaštite (NN 198/03.) piše: "Sustavi tehničke zaštite *ne smiju* se programirati tako da se signal nastao aktiviranjem sustava tehničke zaštite prenosi direktno na sustav veza Ministarstva unutarnjih poslova." Međutim, Zakon o zaštiti novčarskih institucija (NN 56/15.) u članku 13. stavak (3.) navodi: "Ako postoje tehničke mogućnosti, sustavi video-nadzora iz članka 8. i protuprovalni i protuprepadni sustavi iz članka 12. ovoga Zakona mogu biti spojeni i na tehničke sustave Ministarstva unutarnjih poslova." Moguće obrazloženje ovih odredbi je i to da Zakon o zaštiti novčarskih institucija točno definira na koje se institucije odnosi ova odredba, dok Pravilnik općenito definira uvjete i način provedbe tehničke zaštite, međutim ovakve odredbe su i dalje zbunjujuće. Uz analizu ovih zakonskih odredbi i Pravilnika bilo bi potrebno izvršiti i analizu zakonskih odredbi koje u sebi definiraju ovlasti policije na ovom području, od snimanja na javnim prostorima, izuzimanja snimaka i fotografija za određene potrebe, sve do direktnog spajanja s mogućnošću pregledavanja i snimanja videozapisa koji se nalazi u privatnim kompanijama i njihovim prostorima. Treba spomenuti i Zakon o zaštiti osobnih podataka (NN 103/03., 118/06., 41/08., 130/11., 106/12.) koji također uređuje ovo područje. Protrka (2012) u svojem radu obrađuje upravo tu normativnu uređenost u Republici Hrvatskoj s naglaskom na Ministarstvo unutarnjih poslova kao voditelja najveće zbirke osobnih podataka u Republici Hrvatskoj i kao državno tijelo koje se svakodnevno susreće s izazovima ustrojavanja novih evidencija. S obzirom na složenost ove problematike smatramo da treba provesti dodatna istraživanja u budućim radovima i na području zakonodavstva koje uređuje direktan pristup službenika policije ovakvim sustavima i na području zaštite osobnih podataka.

Desetine tisuća kamera "pokrivaju" razne prostore i objekte, od kamera postavljenih na bankomatima, u trgovačkim centrima, benzinskim postajama, bankama, mjenjačnicama, stotinama drugih objekata. Pretpostavka da policija ima neograničen udaljen pristup svim tim

kamerama koje su u vlasništvu privatnih kompanija, otvara nove neslućene mogućnosti u postupanju policije, a time i podizanju razine javne sigurnosti. Iako ovakva iskustva postoje u drugim zemljama, u radu nismo spominjali takva iskustva niti predlagali takva rješenja. Rješenja iz drugih država mogla bi se koristiti u ostvarivanju preduvjeta u Republici Hrvatskoj koji bi omogućili da policija (ili neka druga državna tijela?) imaju udaljeni pristup svim sustavima tehničke zaštite privatnih kompanija. Bez namjere da definiramo baš sve preduvjete, smatramo najvažnijima donošenje novih ili jasnije uređenje postojećih zakonskih ili podzakonskih akata koji uređuju ovo područje. Pitanje zaštite osobnih podataka odnosno općenito zaštite privatnosti i ljudskih prava bit će poseban izazov. Mogući troškovi i tko će ih snositi također će se pojaviti kao jedno od pitanja. Operacionalizacija ovakvog modela iziskivat će i odgovore na niz "operativnih" pitanja od toga koji policijski službenici će raditi na tim poslovima, gdje se i koliko dugo čuvaju snimke ako se obavlja snimanje videozapisa, tko odlučuje o uništavanju zapisa, procedure postupanja, do toga gdje se nalaze ti centri i tko sve ima pristup u njih. Privatne kompanije su i prije početka rada ovakvih nadzornih centara trebale ispuniti sve zakonske obaveze, propisati sve interne procedure, tj. dati odgovor na ova i slična pitanja. Njihovo iskustvo moglo bi se iskoristiti kod mogućih budućih aktivnosti na ovom području.

6. ZAKLJUČAK

Većina autora navedenih u ovome radu nedvosmisleno predlaže i obrazlaže potrebu suradnje privatnog sektora i policije te lokalne zajednice i policije. Isto tako opisuju se zakonske mogućnosti takve suradnje, sve prednosti takve suradnje ne samo za policiju već i za privatni sektor, građane, javnu sigurnost općenito, međutim prema podacima dostupnim autoru ovog članka ta suradnja nije u potpunosti ostvarena.

Sve navedeno pokazuje kako bi u slučaju da policija ima mogućnost direktnog, udaljenog pristupa svim sustavima tehničke zaštite, prije svega videonadzoru koje imaju privatne kompanije, značajno utjecalo na povećanje razine javne sigurnosti. Smatramo da bi ovakva situacija utjecala djelomično i na dosadašnju metodologiju postupanja policije u pojedinim slučajevima.

Možda će nekima zastrašujuće djelovati mogućnost da policija ima neograničen udaljeni pristup svim kamerama koje koriste privatne kompanije i lokalna zajednica, ali će u većem ili manjem opsegu u vrlo bliskoj budućnosti to biti svakodnevnica, a dio toga događa se već i danas. Cilj ovog rada je temeljem opisanog primjera rada nadzornog centra u privatnoj kompaniji potaknuti stručnu i znanstvenu raspravu i istraživanja o različitim mogućnostima korištenja ovakvih sustava u podizanju javne sigurnosti. Rasprava bi trebala obuhvatiti zakonska, tehnička, financijska i sva druga područja važna za ovu temu.

LITERATURA

Abrahamsen, R., Williams, M. C. (2005). *The Globalization of Private Security.* London, Royal Institute for International Affairs. The World Today, 2005., 5-7.
Ivandić Vidović, D., Karlović, L., Ostojić, A. (2011). *Korporativna sigurnost.* Zagreb, AKD.

Kovacich, L. G., Halibozek, P. E. (2002). *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program.* Burlington, Butterworth-Heinemann.
Kraljević, M., Direktno.hr. http://direktno.hr/en/2014/domovina/38595/Zagreb-nove-nadzorne-kamere-na-jo%C5%A1-23-lokacije-ukupno-118.htm, 10. veljače 2016.
Pavliček, J. (2010). *Partnerstvo javne i privatne sigurnosti*. Konferenciji hrvatskih menadžera sigurnosti. Zagreb, 25. i 26. studenoga 2010.
6. Pothraški, F. Tršinski, S., Kancir, K. (2008). *Prijedlog unapređenja rada policije uvođenjem videonadzora javnih prostora.* Policija i sigurnost, godina 17., broj 3-4, str. 243-253., Zagreb.
Protrka, N. (2013). *Normativna uređenost zaštite osobnih podataka u Republici Hrvatskoj*. Policija i sigurnost, godina 22., broj 4, str. 509-521., Zagreb.
Zagreb između kamera, punjenja proračuna, sigurnosti i privatnosti građana. http://www.svijetsigurnosti.com/blogs/5847-zagreb-izmedu-kamera-punjenja-proracuna-sigurnosti-i-privatnosti-gradana Ostojić, A., 5. veljače 2016.
Zakon o zaštiti novčarskih institucija. Narodne novine 56/15.
Zakon o zaštiti osobnih podataka. Narodne novine 103/03., 118/06., 41/08., 130/11., 106/12. Zagreb.

Darko Dundović

UNUSED POSSIBILITIES OF PRIVATE SECTOR IN RAISING THE LEVEL OF PUBLIC SAFETY

Summary
A rapid development of technology has enabled companies to use different electronic security systems to protect their property and employees, prevent thefts and other damaging events as well as to monitor business processes.
Every day, thousands of facilities and different areas are recorded, entrance / exit of persons are monitored through identification cards and alarms are received. Surveillance of the recorded material is exclusively reserved for security professionals (either contracted security guards or employees of companies that have the technical protection systems). Police or even other security services have no direct access to the alarm systems, video surveillance, access control etc. that some companies use either because of legal obligations or because of their own needs.
Although the courts, police and other state bodies have the right to request such recorded video surveillance materials, remote access to video surveillance by state authorities is not the practice in the Republic of Croatia.
One of the reasons for that is lack of the existing legislation, possible budget problems, but also the indifference of the police and security agencies for such possibilities.
While it is undeniable that in case of direct access and review of video surveillance the police might have a current picture of events or the area, and thus significantly improve public safety, apart from the experience with "public cameras" in the cities, co-operation with the private sector is extremely modest.

Key words: *technical protection systems, companies, police*

PREGLEDNI ZNANSTVENI RAD

Joško Sindik[517]
Lucija Dodigović[518]
Joško Vukosav[519]

PREDATORSKI ČASOPISI: SVE VEĆI PROBLEM ZNANSTVENE ZAJEDNICE

Sažetak

Objavljivanje radova u kvalitetnom znanstvenom časopisu glavni je cilj za svakog znanstvenika, osobito za istraživače u ranoj fazi karijere. Međutim, znanstvenicima i stručnjacima je važno naučiti pažljivo procijeniti i odabrati publikacije u kojima mogu publicirati svoje članke, zadovoljavajući uvjete za postizanje znanstvenih i nastavnih zvanja. Naime, s "eksplozijom" broja novoutemeljenih znanstvenih časopisa zadatak odabira može biti vrlo težak, a pritom osobiti problem stvaraju tzv. predatorski časopisi (PČ). PČ, kao specifični oblik kriminaliteta, ostvaruju zaradu krađom identiteta legitimnih časopisa, krivotvorenjem metrike i baza u kojima se citiraju, uz prikupljanje pristojbe za objavu članaka. Nastoje pridobiti znanstvenike dobro razvijenom mrežom koja uključuje izradu web stranica, intenzivni e-mail marketing i dobar izbor žrtava. Pokušaji razlučivanja legitimnih i nelegitimnih časopisa, kreiranjem liste sumnjivih časopisa (Jeffrey Beallov popis), uz zahtijevanje izdavanja pismene izjave o transparentnosti u izdavaštvu (udruge Open Access Scholarly Publishers /OAS/ i drugih globalnih organizacija), te postroženje kriterija indeksiranja od strane ureda OAS-a. Na žalost, niti jedna od postojećih mjera nije se pokazala posve učinkovitom, pa se autorima savjetuje stalno sustavno provjeravanje postojećih lista PČ zbog njihove sve češće pojave. Naime, rezultati provedene analize Beallove liste predatorskih izdavača, časopisa, metrike i "ukradenih" časopisa (2011-2015), pokazuju drastične razlike u verižnim (prosječna stopa promjene 84-267), a osobito u baznim (138-4883) indeksima (kod usporedbe početnog i finalnog razdoblja).

Ključne riječi: *izdavačka etika, Jeffrey Beallov popis, kontrola kvalitete, krađa identiteta, otvoren pristup.*

1. UVOD

U ovom radu bavimo se specifičnim oblikom digitalnog kriminala, tzv. predatorskim časopisima, te analiziramo njihovu etimologiju nastanka, njihov brojčani rast u vremenskoj perspektivi te načine detekcije ovakvih časopisa.

Važnost publiciranja u rangiranim časopisima

U akademskom svijetu je otvorena razmjena znanstvene komunikacije od velike važnosti i za potvrđivanje znanstvenog statusa i za napredovanje u znanstvenoj karijeri. Razmjena

[517] Joško Sindik, Institut za antropologiju, znanstveni suradnik, e-mail: josko.sindik@inantro.hr
[518] Lucija Dodigović, Institut za antropologiju, Voditelj INDOK službe i knjižnice, lucija.dodigovic@inantro.hr
[519] Joško Vukosav, Visoka policijska škola, dekan, vjosko@fkz.hr

znanstvenih informacija pomaže u razvijanju znanstvene teorije, pobijanju pogrešnih teza i stvaranju novih, ali razvija i bazu za nadogradnju onih saznanja i metodologije, koji mogu poslužiti kao izvrstan temelj za daljnja istraživanja (Grgić, 2004). Svaki znanstvenik ili student, koji je tek počeo svoju znanstvenu karijeru zna da za bilo koji napredak mora istraživati i objavljivati svoja saznanja i rezultate svog istraživačkog rada u što renomiranijim časopisima u određenom znanstvenom polju i području. Međutim, znanstvenici i stručnjaci trebaju naučiti pažljivo procijeniti i odabrati publikacije u kojima mogu publicirati svoje članke i tako zadovoljiti uvjete za postizanje znanstvenih i nastavnih zvanja.

Baze i čimbenici utjecaja kao mjerila znanstvene izvrsnosti

Svakom znanstveniku koji želi objaviti znanstveni članak izuzetno je važna i metrika časopisa u kojemu objavljuje. Jedna od najpoznatijih metrika je *Journal Impact factor* (JIF). Iako i sama nije idealna, u čestoj je uporabi. Internet i razni društveni mediji se koriste raznim mrežnim bazama kao mjeriteljima važnosti nekog časopisa, poput Altmetrije koja mjeri citiranost radova u kratkom periodu vremena čak i na ljudima izvan akademske zajednice (Wehrmeijer, 2014). JIF rangira časopise prema njihovoj citiranosti. Thompson Reuters, kao jedna od poznatijih baza, izračunava ga na preko 10 000 časopisa. Osim njega postoje još i Eigenfactor, SNIP (*Source Normalized model in Paper*), SJR (*Scimago Journal Rank*), Scopus, Google Schoolar Metrics i mnogi drugi (Wehrmeijer, 2014). Odbori i komisije za procjenu izvrsnosti nekog znanstvenika te za potvrdu njegova napredovanja, često gledaju citiranost časopisa u kojem se rad objavljuje kao važniji čimbenik od citiranosti samog rada (Garfield, 1972). Premda podaci o "čitanosti" i citiranosti članka nekog znanstvenika s racionalnog stajališta mogu biti dobar pokazatelj znanstvenog "odjeka", već i intuitivno možemo domisliti barem dva načina kako se ovakvo mjerilo znanstvene izvrsnosti može "izigrati". Prvo, jednostavno je moguće da se dva ili više znanstvenika dogovore da jedni citiraju u svojim člancima članke onih drugih ili da namjerno citiraju članke baš iz određenih časopisa, čime i JIF određenih časopisa i određenih autora na umjetan način raste, kao i njegov znanstveni ugled. Drugo, postoje softwarei koji uploadiraju (stavljaju na internetsku mrežu) određene članke na portale određenih časopisa raspoloživih online (*online first*) na samom kraju ili početku godine ili mjeseca, pa tako uploadirani članci postaju vidljiviji čitateljima, što opet utječe na njihovu bolju citiranost (viši JIF).

Razlozi pojave predatorskih časopisa

Otvoreni pristup je svima omogućio puno brži način objavljivanja, ali i pretraživanje već objavljenih radova te njihovo korištenje za daljnji razvoj znanosti. Uz želju za vlastitim napretkom znanstvenika, znanstvenike i njihova sveučilišta institucije i agencije koje financiraju razna istraživanja potiču ili čak i zahtijevaju javno objavljivanje tih istraživanja. Ako ste imalo zainteresirani za vlastiti razvoj u znanosti, sigurno ste čuli za predatore među časopisima u otvorenom pristupu. To su časopisi koji postoje isključivo u svrhu vlastitog profita, a ne unapređivanja znanosti. Naplaćuju autorima naknadu za objavljivanje pod izlikom da je to trošak obrade članka (Wehrmeijer, 2014).

Pojam predatorski časopis

Predatorskim časopisima mogu se nazvati oni časopisi čije uredništvo koristi otvoreni pristup da bi ostvarilo osobni profit. No naplaćivanje nije jedini pokazatelj predatorskog časopisa jer mnogi renomirani časopisi imaju određenu naknadu za pokrivanje troškova, posebno ako se radi o sufinanciranju ili potpori za istraživanje (Berger i Cirasella, 2015). Neki u prepozicijama objavljivanja imaju i naplatu po stranici ili slici. No predatorski časopisi kao takvi uglavnom postoje samo zbog naplate, a onda tek usputno članke i objave, no najčešće bez recenzije i s lažnom metrikom, premda stalno tvrde suprotno (Beall, 2009). Za otkrivanje ove vrste časopisa pobrinuo se akademski bibliotekar Jeffrey Beall sa Sveučilišta Colorado, Denver, koji je na svojem blogu nazvanom *Scholarly Open Access* objavio listu predatorskih časopisa i izdavača, koja iz godine u godinu raste sve brže (SOA, 2015; Beall's List, 2016). Jednom je ova lista bila objavljena čak u *The New York Timesu* (Kolata, 2013). Beall je svakako doprinio povećanju svijesti o postojanju predatorskih časopisa u otvorenom pristupu, no na žalost nije baš pokazao sklonost spram izdavača u manje razvijenim i ekonomski lošije stojećim zemljama, pa se na njegovom popisu može naći i priličan broj časopisa koji zapravo nisu predatori (Berger i Cirasella, 2015).

Detekcija predatorskog časopisa

Neovisno o potencijalnim pogreškama, Beall je nedvojbeno upozorio znanstvenu zajednicu i sve ostale zainteresirane za ovu problematiku o glavnim pokazateljima i upozoravateljima predatorskih časopisa. Vrlo često su to časopisi sa sumnjivom recenzijom, ili je čak i nemaju (katkad je već naočigled vidljivo da je objavljeni članak zapravo vrlo loše napisan i u formalnom i u sadržajnom pogledu). Recenzija nije transparentna kao u otvorenom pristupu, a često izdavači pri sveučilištima koji zapravo ne postoje, bar ne na toj adresi, nisu indeksirani u indeksnim bazama, niti imaju JIF (Beall, 2009). Premda postoje časopisi niske indeksiranosti koji nisu predatorski časopisi, s pravom nas se upozorava na oprez prilikom suradnje s časopisima koji prihvaćaju radove znanstvenika i istraživača s popularnim e-mail adresama na Gmail ili Yahoo domenama. Također, njegova nas lista upozorava na časopise veoma širokog spektra i opsega koji nude izuzetno brzo vrijeme objave rada, jer tada znamo da u danim časopisima vjerojatno i nema prave recenzije (Beall, 2009).

Adresar časopisa u otvorenom pristupu (DOAJ) zbog postojeće Beallove *Crne liste* (Berger i Cirasella, 2015; Beall's List, 2016), koja svakim danom sve više raste, uklonio je čak 114 časopisa te pooštrio svoje kriterije za upis u DOAJ. Nakon ožujka 2014. od svakog je novog časopisa zatražio ispunjenje svih uvjeta za upis. Stoga dajemo kratak opis DOAJ uvjeta. Na osnovnoj razini časopis bi trebao biti ponajprije znanstvenog karaktera, sa svojim sadržajem odmah dostupnim, mora osigurati kontrolu kvalitete rada kroz urednika, uredništvo i recenziju, mora imati ISSN (*International Standard Serial Number*) broj te u potpunosti transparentno poslovanje, u slučaju kad postoji neka naplata prilikom obrade rada u postupku objavljivanja (Code of Conduct, 2015). Ako časopis zadovolji sve uvjete dobije od DOAJ-a pečat. Ako ne zadovolji sve uvjete, DOAJ javlja ISSN centru zabranu dodjeljivanja jedinstvenog ISSN broja (ISSN, 2014). Kad časopis bude prihvaćen u udrugu znanstvenih časopisa u otvorenom pristupu (*Open Access Scholarly Publishers Association*, tj. OASPA)

mora prihvatiti i određen kodeks i pravila ponašanja koji onemogućuju bilo kakav oblik predatorskog ponašanja ili ga se izbacuje (Wehrmeijer, 2014).

Glavni kriteriji za utvrđivanje predatorskih izdavača časopisa u otvorenom pristupu su: urednik i urednički odbor (nema urednika i uredničkog odbora, nema izdavača, dupliciraju se urednički odbori u dva ili više časopisa itd.); upravljanje poslovanjem (isti izdavač ima veliki broj časopisa s istim sučeljem, sadržaj se pojavljuje i nestaje, nema transparentnosti itd.); loša praksa standarda (kopiraju se upute za autore iz drugih časopisa, vrlo široka znanstvena područja koja su obuhvaćena tematikom, nema jasnih adresa za kontakte itd.), integritet (naziv časopisa nema veze s tematikom koju pokriva, časopis šalje *spam* zahtjeve za recenziju znanstvenicima nestručnim za određeno područje itd.). Detaljniji prikaz upravo za kriterije integriteta dan je u tablici 1.

Tablica 1: Vodič za evaluaciju integriteta časopisa (Odom Foren, 2015)

Pitanje	Što se traži	Upozorenja
Tko je glavni urednik časopisa?	Osoba s reputacijom u svom polju rada	Nema nikakvog dokaza o postojanju glavnog urednika
	Direktan kontakt podatak o uredniku jasno je vidljiv	Ne postoji kontakt podatak o uredniku
Kakva je procedura objave unutar časopisa kojom se osigurava kvaliteta?	Jasno vidljiva izjava o načinu recenzije svakog rada prije objave u časopisu	Obećanje brzog pregleda rada i objave (kvalitetan pregled zahtijeva vremena)
	Navedena imena svih članova uredništva ili recenzenata	Tajanstvenost osoba koje rade pregled rada
Ima li časopis već sigurnu praksu poslovanja i izdavaštva?	Časopis je član COPEa	Izdavač ili časopis se nalazi na Beallovoj listi Scholarly OA
	Časopis se nalazi na listi INANE/NA&E časopisa	Ime časopisa ili neka druga informacija jako je slična nekom drugom časopisu
	Informacija o procesu naplate autorima jasno je vidljiva	Časopis ili urednik potražuje radove s pretjerano komplimentirajućim mailovima
	Ako časopis navodi svoj Impact Factor, on je jednak i u *Journal Citation Report* (WoS)	

Svaki časopis ima svoju kvalitetu koju mjerimo kvalitativnim i kvantitativnim metodama. U kvalitativne spada prikupljanje mišljenja (ankete), reputacija urednika i odbora, postotak odbijenih radova, recenzijski postupak i analiza sadržaja, dok u kvantitativne metode spada broj prikupljenih citata, zbirke knjižnica, čitanost, meta-analize i metrika vanjskog vrednovanja (Caretta i Mattarocci, 2009). Upravo tu kvalitetu naši PČ prikazuju lažnom

metrikom. Osim toga prepoznaje ih se i po "otetim" nazivima poznatih časopisa (*hijacked journals*). Hakeri zaposjednu domene kojima je istekao rok ili konstruiraju lažne, vrlo slične i uvjerljive web stranice sa sličnim nazivima te hakiraju sam časopis i preusmjere njegov promet na lažnu web stranicu. Korisnici takvih stranica mogu otkriti svoje lozinke ili svoje bankovne podatke, mogu uplatiti članarine, knjige ili čak pristojbe za obradu i objavljivanje svojih članka (Bohannon, 2013).

Cilj istraživanja koje je provedeno bio je utvrditi verižne i bazne indekse koji će reflektirati obilježja razvoja (povećanja) broja predatorskih izdavača, časopisa, otetih časopisa i lažne metrike, u vremenu od 2011. do rujna 2015. godine.

2. METODE

Statistička analiza vremenskih nizova sastoji se od njihova grafičkog prikazivanja i primjena različitih brojčanih postupaka radi uočavanja obilježja razvoja pojave u vremenu. Indeksi vremenskog niza relativni su brojevi koji iskazuju odnos stanja jedne pojave ili skupine pojava u različitim razdobljima ili vremenskim točkama. Ako se pomoću njih prati razvoj jedne pojave u vremenu tada je riječ o individualnim indeksima, dok skupni indeksi prate razvoj skupine pojava. Individualni indeksi dijele se na: verižne indekse i bazne indekse. Verižni indeksi su relativni brojevi (u %) koji pokazuju promjene stanja pojave u uzastopnim razdobljima, odnosno pokazuju za koliko se posto vrijednost pojave u jednom razdoblju promijenila u odnosu na prethodno razdoblje. Bazni indeksi pokazuju relativne promjene pojave u tekućem razdoblju u odnosu na neko odabrano bazno razdoblje (Marković, 2008). U ovom istraživanju, uz bazne i verižne indekse izračunate su i stope promjena te prosječne stope promjena.

3. REZULTATI

U tablici 2 dan je pregled povećanja broja predatorskih izdavača, časopisa, lažne metrike te otetih časopisa u razdoblju od 2011. do 2015. godine (Hebrang Grgić, 2004).

Tablica 2: Pregled povećanja broja predatorskih izdavača, časopisa, lažne metrike te otetih časopisa u razdoblju od 2011. do 2015. godine

Godina	Izdavača (V, SP)	Časopisa (V, SP)	Metrika (V, SP)	Otetih časopisa (V, SP)
2011	18	-	-	-
2012	23 (128, 28)	-	-	-
2013	225 (900, 800)	126	-	-
2014	477 (212, 112)	303 (240, 140)	-	-
2015/01	693 (145, 45)	507 (167, 67)	26	30
2015/09	879 (127, 27)	787 (155, 55)	36 (138, 38)	80 (267, 167)

PSP	118	84	138	267
B	4883	625	138	267

Legenda: V – verižni indeksi; SP – stopa promjene; PSP – prosječna stopa promjene; B – bazni indeksi

Premda je porast broja predatorskih izdavača i časopisa više nego očigledan, što se očituje i u baznim i u verižnim indeksima (dok su i razdoblja praćenja nejednaka, barem za 2015. godinu, gdje su analizirani podaci iz siječnja i rujna), verižni indeksi i pripadne stope promjene pokazuju da je porast broja predatorskih izdavača bio najveći za 2013. godinu. Porast broja predatorskih časopisa bio je najveći u 2014. godini. Podaci o lažnoj metrici te o otetim časopisima dani su samo za 2015. godinu, ali već podatak o značajnom prirastu baznih i verižnih indeksa te pripadnih stopa promjene već u razdoblju od samo 9 mjeseci 2015. godine, upućuje na razmjerno visok porast broja ovih forma predatorskih aktivnosti.

4. RASPRAVA

Glavni nalaz istraživanja je činjenica da se broj predatorskih izdavača i časopisa značajno povećao u analiziranom razdoblju, što se reflektira u baznim i verižnim indeksima. Također, prilično je visoka stopa porasta otetih časopisa i lažne metrike, već u kratkom razdoblju od devet mjeseci 2015. godine. Premda su rezultati pokazali kako je napretkom tehnologije i širenjem ovog oblika kriminala drastično porastao broj lažnih izdavača i časopisa tijekom 2013. godine (izdavači) odnosno 2014. godine (časopisi), izgleda da je prisutan sve manji porast ovih oblika kriminala tijekom 2015. godine zbog sve veće svijesti javnosti i znanstvene zajednice o problemu koji ih je počeo okruživati. Znanstvenici su postali sve oprezniji te sve više provjeravaju čak i one poznate izdavače i urednike (Caretta i Mattarocci, 2009). Premda opisana problematika predatorskih časopisa zapravo i nije neka novost jer oduvijek postoje časopisi s relativnom slabom recenzijom, nedavna "eksplozija" boja predatorskih oblika kriminala i njihova vrlo ubrzana pojava, upućuje na važnost ovog problema.

Prednost ovog istraživanja je u kvantitativnom doprinosu egzaktnijeg mjerenja prirasta broja predatorskih izdavača, časopisa, lažne metrike te otetih časopisa u promatranom razdoblju, gdje je uz očiglednu činjenicu porasta ovih oblika kriminala, očito i postupno mijenjanje dominantnih oblika ove vrste kriminala. Primjerice, očito je da dolazi do smanjenja naprosto eksponencijalnog prirasta broja predatorskih izdavača i časopisa, ali izgleda da falsificiranje metrike časopisa te otimanje njihovih domena uzima sve više maha. ***Nedostatak*** istraživanja je nepostojanje podataka o analiziranim pojavama iz ranijih vremenskih razdoblja, pa je zadatak ***budućih istraživača*** praćenje ove pojave idućih godina, ali i razlikovanje zastupljenosti ovakvog oblika kriminala u pojedinim državama.

Sa stajališta ***praktične primjene*** u prvom redu knjižničari moraju razumjeti obilježja i metode "grabežljivih" izdavača. Potom knjižničari moraju znati pomoći istraživačima i čitateljima da prepoznaju niske kvalitete časopisa te im pokazati načine kako da ne postanu žrtve nečije težnje za ovim oblikom zarade. S knjižničnog aspekta važno se znati suprotstaviti zabludama i lažnim uzbunama (koje katkad u svim časopisima mogu vidjeti predatorske),

koje stavljaju u neugodan položaj prihvaćanje otvorenog pristupa znanstvenim i drugim časopisima. Suvremena znanstvena zajednica zalaže se za otvoreni pristup znanstvenih članaka korisnicima. Naime, zbog povećane dostupnosti radovi u otvorenom pristupu više se citiraju, pa se na taj način povećava i njihov čimbenik utjecaja (*Impact Factor*). Međutim, otvoreni pristup pritom i ubrzava znanstveni ciklus rada jer potiče na daljnja istraživanja. Istovremeno, pokazalo se da otvoreni pristup ima i svojih mana, jer često biva upitno tko su recenzenti znanstvenog rada u otvorenom pristupu. Kad se rad zaprimi u uredništvo, nakon što glavni urednik sa suradnicima provjeri osnovne podatke, rad se šalje na recenziju, koju bi trebali obavljati stručnjaci koji bi trebali biti nepristrani. No jesu li zaista i kako bismo to mogli znati (Dujmušić, 2013), posebno u situacijama kad se od autora traži da predloži potencijalne recenzente? Međutim, otvoreni pristup uza sve nedostatke ipak omogućuje unaprjeđenje znanstvene komunikacije i potiče daljnji razvoj znanosti. U širem smislu knjižničari imaju važnu ulogu sudionika u marginaliziranju potencijalnih predatorskih časopisa i promoviranju sigurnih opcija. Stoga knjižničari imaju važnu ulogu u tumačenju razlika između kvalitete i ugleda nekog časopisa te činjenice da časopisi u otvorenom pristupu mogu imati naknadu za obradu i objavu rada, kao i da svi predatorski časopisi nemaju nužno naplatu.

5. ZAKLJUČCI

Rezultati istraživanja potvrđuju činjenicu da se broj predatorskih izdavača i časopisa značajno povećao u analiziranom razdoblju, dok je prilično visoka stopa porasta otetih časopisa i lažne metrike. Preciznije, rezultati provedene analize Beallove liste predatorskih izdavača, časopisa, metrike i "ukradenih" časopisa (2011.-2015.), pokazuju drastične razlike u verižnim (prosječna stopa promjene 84-267), a osobito u baznim (138-4883) indeksima, ako se uspoređuje početno i finalno razdoblje. Pokušaji razlučivanja legitimnih i nelegitimnih (predatorskih) časopisa, kreiranjem liste sumnjivih časopisa (Beallov popis), uz zahtijevanje izdavanja pismene izjave o transparentnosti u izdavaštvu te postroženje kriterija indeksiranja od strane ureda OAS-a, nisu posve uspješni. Stoga se autorima savjetuje stalno sustavno provjeravanje postojećih lista predatorskih časopisa zbog njihove sve češće pojave, uz savjetovanje s knjižničarima.

LITERATURA

Beall, J. (2009). Bentham Open. *The Charleston Advisor 11*, 1, 29–32.

Beall's List: Potential, possible, or probable predatory scholarly open-access publishers (2016). *Scholarly Open Access*, http://scholarlyoa.com/publishers/. Također pogledaj http://scholarlyoa.com/individual-journals/. (Pristupljeno 15. siječnja 2016.)

Berger, M. i Cirasella, J. (2015). Beyond Beall's List: Better understanding predatory publishers. *College & Research Libraries News*, 76, 132-135.

Bohannon, J. (2013). Who's Afraid of Peer Review? *Science 342*, 6154, 60–65.

Caretta, A. i Mattarocci, G. (2009). Evaluating scientific journals: properties, limits and conditions of effectiveness of classification methodologies. *Journal of Economics and Economic Education Research, 10*, 2. http://www.freepatentsonline.com/article/Journal-Economics-Economic-Education-Research/219011027.html (pristupljeno 15. siječnja 2016.)

Code of Conduct (2016). *Open Access Scholarly Publishers Association*, http://oaspa.org/membership/code-of-conduct/. (pristupljeno 5. siječnja, 2016.)

Dujmušić, I. (2013). Lažni znanstveni rad objavilo 157 časopisa. *Matrix World*, http://matrixworldhr.com/2013/11/01/lazni-znanstveni-rad-objavilo-157-casopisa/. (Pristupljeno 2. veljače 2016.)

Garfield, E. (1972). Citation analysis as a tool in journal evaluation. *Science 178*, 471–479.

ISSN (2014). Guidelines for Requesting an ISSN through the ISSN International Centre Website. *International Serial Standard Number International Centre*, www.issn.org/wp-content/uploads/2013/09/ISSNguidelinesENG_03032014.pdf. (Pristupljeno 3. ožujka, 2014.)

Hebrang Grgić, I. (2004). Kontrola kvalitete znanstvenih članaka objavljenih u elektroničkoj sredini. *Vjesnik bibliotekara Hrvatske, 47*, 1-2, 78-86.

Kolata, G. (2013) Scientific Articles Accepted (Personal Checks, Too). *The New York Times*, April 7, www.nytimes.com/2013/04/08/health/for-scientists-an-exploding-world-of-pseudo-academia.html. (Pristupljeno 3. veljače, 2016.)

Marković, S. (2008). *Statistika - priručnik.* Rijeka: Sveučilište u Rijeci, Fakultet za turistički i hotelski menadžment u Opatiji.

Odom Foren, J. (2015). Predatory Publishers: What the Nursing Community Needs to Know. *Journal of PeriAnesthesia Nursing, 30*, 2, 87-90.

Wehrmeijer, M. (2014). Exposing the Predators: methods to Stop Predatory Journals. *Leiden University*, https://openaccess.leidenuniv.nl/handle/1887/28943. (Pristupljeno 3. veljače 2016.)

Joško Sindik
Lucija Dodigović
Joško Vukosav

PREDATORY JOURNALS: AN INCREASING PROBLEM OF THE SCIENTIFIC COMMUNITY

Summary

Publishing in a high-quality peer reviewed journal remains a prime goal for academics, especially for early-career researchers. However, it is more important than ever that scholars carefully evaluate and select the publications in which they wish to disseminate their work, that meets the requirements for their scientific and educational titles. Specifically, the "explosion" in the number of newly created scientific journals, the task of choosing, can be difficult, and the ones that create a special problem are the so-called predatory journals (PJ). PJ, as a specific form of crime, make a profit by stealing the identity of legitimate magazines falsifying the metrics and citation bases, but still collecting the authorship fee. They are trying to recruit scientists with a well-developed network, including web development, intensive e-mail marketing and a good choice of victims. Attempts of differentiating legitimate and illegitimate magazines, the creation of lists of suspected journals (Jeffrey Beall's list), along with requesting a written statement about transparency in publishing (Association of Open Access Scholarly Publishers (OAS) and other global organizations), and stricter criteria of indexing by the OAS office. Unfortunately, none of the existing measures has proven as overall effective. Hence, the authors are advised to keep checking systematically existing lists of PJ, because of their growing frequency of occurrences. The results of the analysis of Beall's list of predatory publishers, journals, metrics and "hijacked" journals (2011-2015), shows drastic differences in the chain (average rate of change of 84 to 267), and in particular in the base (138-4883) indices (code comparing the initial and final period).

Key words: *publishing ethics, Jeffrey Beall's list, quality control, identity theft, open access.*

NACIONALNA, URBANA I RAČUNALNA SIGURNOST, ZAŠTITA I SIGURNOST PODATAKA/ NATIONAL, URBAN AND COMPUTER SECURITY AND DATA PROTECTION

STRUČNI RAD

Tihomir Šujster[520]

FINANCIRANJE IZ KRIMINALNOG MILJEA, OPASNOST ZA UČINKOVITOST NACIONALNE SIGURNOSTI

Sažetak

Na međunarodnoj razini sustavno jača borba protiv korupcije i finaniranja iz kriminalnog miljea jer takvo financiranje izravno razara temelje demokracije i osnovne vrijednosti sustava. Kada je u funkcioniranje sustava izravno uključen organizirani kriminal, vrlo je teško, a najčešće i nemoguće razvijati demokratske institucije i osiguravati normalni gospodarski razvoj, dok je nacionalna sigurnost teško ugrožena. U sustavu sprječavanja pranja novca i financiranja terorizma koji se primjenjuje u Republici Hrvatskoj, središnje mjesto zauzima Zakon o sprječavanju pranja novca i financiranja terorizma koji je u primjeni od 01. siječnja 2009. godine. Navedenim zakonom i aktima donesenim na temelju njega Hrvatska je preuzela sve relevantne smjernice i konvencije međunarodnih tijela i organizacija koje imaju za cilj učinkovitu borbu protiv ulaganja novca stečenog kaznenim djelom u legalne financijske poslove. Kriminalni milje je jednim djelom ugledao svoju šansu u globalizaciji tržišta i tijekova novca, dok s druge strane moderne tehnologije omogućavaju plasman novca na drugačiji način poslovanja, te se klasičan način pranja novca zamjenjuje transakcijama kojima je teško ući u trag. Međunarodni sporazumi su omogućili da se ipak može ući u trag jer je danas skoro sve umreženo na globalnoj razini. Raznovrsnost metoda i tehnika djelovanja koje uključuju transakcije novca kroz financijski i nefinancijski sektor u fazi stavljanja novca u banke ili druge institucije daje prioritet te ističe značaj prevencije pranja novca, ulaganja iz kriminalnog miljea u financiranje terorizma i drugih kriminalnih radnji u zaštiti nacionalne sigurnosti.

Ključne riječi: *financiranje, kriminalni milje, nacionalna sigurnost, terorizam.*

1. UVOD

Početkom 21. stoljeća problem financiranja iz kriminalnog miljea je sve raširenij i vrlo unosan posao koji kontrolira političke pritiske, a time i političke odluke pojedinih država. Europska unija daje prioritet privremenom oduzimanju i konačnom oduzimanju prihoda stečenog kaznenim djelom zbog jačanja europske sigurnosti o pranju novca, traganju, korupciji i financiranju terorizma, kao i drugim konvencijama vezanim za organizirani kriminal i terorizam, te ulaže ogromne resurse s ciljem smanjivanja nacionalnih, međunarodnih i regionalnih kriminalnih radnji u vezi pranja novca, korupcije i financiranja terorizma. Tako pojedine države udružene u razne asocijacije mogu donositi i predlagati

[520] Mr. sc. Tihomir Šujster, predavač, Visoka policijska škola, MUP RH, instruktor policijskih vještina, e-mail: tsujster@fkz.hr

inicijative koje su dalekosežne za kvalitetu života građana u tim državama, regijama i asocijacijama čiji su članovi. Pod kvalitetom se podrazumijeva nacionalno - ekonomski i nacionalno - sigurnosni aspekt građana pojedine države. Pranje novca i financiranje terorizma je primarna zadaća kriminalnog miljea ukoliko je došlo do političko – kriminalne sprege kojom se kontroliraju resursi države iz koje otječe ogromno bogatstvo na račun političkih pojedinaca i kriminalnih skupina. Novim tehnologijama tijek novca se kreće drugačije od starog načina pranja novca jer je ujedinjenje tržišta otvorilo mogućnost brzog prebacivanja novca i teško mu je ući u trag. Opasnost po nacionalnu sigurnost pojedine države je održivost financijskog sustava, no, i održivost kriminalnog miljea je financijska dobit, te dolazi do prijepora ukoliko jedna strana dobiva - druga sigurno gubi pa se postavlja pitanje je li moguće doći do kompromisa između tih strana. Događaj koji je promijenio odnos financiranja iz kriminalnog miljea koji je usmjeren prema financiranju terorizma je teroristički napad koji se dogodio 11. rujna 2001. godine u SAD-u. U cilju sprječavanja financiranja terorizma pojačava se suradnja svih nadležnih tijela, razvijaju se međunarodni pravni instrumenti, te se usklađuju mjere i radnje sprječavanja pranja novca, korupcije, širenje terorizma i njegovog financiranja. Osjećaj posvemašnje nesigurnosti je posljedica terorizma, što je pospješila globalizacija koja je krenula iz SAD – a u cilju kretanja kapitala i tehnologija, te su organizirane kriminalne skupine počele uvoditi i koristiti nove tehnologije financiranja da im se teže uđe u trag. Sprječavanje terorista u financiranju svojih aktivnosti vodi prema značajnom nadzoru bankarskih institucija i umrežavanju istih na globalnoj razini, što je učinkovit instrument za borbu protiv pranja novca, korupcije i financiranja iz kriminalnog miljea te drugih aktivnosti poput financiranja predizbornih političkih kampanja. U radu se navode politički i korupcijski slučajevi u svijetu financiranja iz kriminalnog miljea kojima su se financirale i političke elite. Nerijetko iza toga stoje i terorističke skupine kojima odgovara stanje u pojedinim državama. Takav slijed događaja stvara ugrozu nacionalne sigurnosti koje odgovara kriminalnim skupinama, korumpiranim političarima i teroristima koji su zavedeni nacionalističkim, vjerskim i ideološkim idejama, a krajnji cilj je bogaćenje političara i kriminalaca. U ovom kontekstu djeluju i multinacionalne kompanije koje nisu predmetom ovog rada.

2. Financiranje iz kriminalnog miljea

Kada je u funkcioniranje političkih sustava izravno uključen organizirani kriminal, vrlo je teško, a najčešće i nemoguće razvijati demokratske institucije i osiguravati normalni gospodarski razvoj. No, ključna stvar koja se pokazuje u odnosu države prema organiziranom kriminalu je spremnost države da se s njime otvoreno obračuna. U nizu zemalja Latinske Amerike takva spremnost zapravo ne postoji, za razliku primjer Italije u kojoj su poslije ubojstva suca Falconea, demokratske snage, koristeći raspoložive državne instrumente, krenule u borbu s organiziranim kriminalom. Problem s kojim se susrela Italija nije bio uopće zanemariv jer se kriminal upleo u sve sfere političkog života. Shvatilo se da prijeti opasnost da mafija preuzme upravljanje državom. Notorno je da bitka s mafijom nije dovršena, no, ipak, tri premijera su bila osuđena na zatvorske kazne (pri čemu su neki i pobjegli iz zemlje), a i bivši premijer Silvio Berlusconi stalno je pod prijetnjom istrage u vezi financiranja njegove političke karijere iz kriminalnog miljea (Šujster, 2007:56).

Postoji vrlo velik interes kriminalnog miljea da se uključi u političko odlučivanje i procese u Istočnoj Europi. Razlog tome je činjenica što je kompletno bogatstvo države izloženo otimačini na brojne načine koja je na djelu u bivšim socijalističkim zemljama, uključujući privatizaciju, pretvorbe i sanacije. Najlakši način prisvajanja je da se pomoću loših zakona dođe legalno do resursa, poduzeća i slično, a za to je potrebito kontrolirati politiku. Nakon što su se domogli kapitala takve skupine, financirajući političke stranke i pojedince koji se žele baviti politikom, određene skupine mogu izravno utjecati i na donošenje zakona. Ako je novac iz kriminalnog miljea doveo do pobjedničke opcije na izborima, te povezao vlast s nezakonitim poslovima, njihovi poslovi se mogu realizirati mitom, odnosno širenjem korupcije. Skupine organiziranog kriminala će na taj način upravljati lobijima koji dijele ugovore i plaćaju državne službenike.[521] „Bogatstvo, beskrupuloznost i međunarodne veze mnogobrojnih grupa organiziranog kriminala govore o poteškoćama njihovog kontroliranja u bilo kojoj zemlji. Postoji opasnost da kriminalne aktivnosti, umjesto da budu uklonjene, postanu tako isprepletene s politikom da će ih biti teško razlikovati“ (Rose-Ackerman, 2002:25-27).

Postoji, dakle, velika opasnost da financiranje preko kriminalnog miljea postane u toj mjeri vezano uz sferu politike da mogućnost otklanjanja korupcije i kriminala iz političkog sustava postane zapravo neostvariva. Ono što u tom slučaju ostaje kao posljedica je izopačeni sustav koji besprijekorno funkcionira, dok istodobno demokratski sustav polako postaje virtualnim svijetom koji ne postoji u stvarnosti.

3. Antikorupcijske inicijative međunarodne zajednice

Međunarodna zajednica prepoznala je na vrijeme korupciju kao ključan problem i stavlja korupciju u prioritetan položaj s obzirom na ostale probleme koji su također značajni i koje korupcija može još više uvećati. Razdoblje poslije tzv. hladnog rata omogućilo je novi pristup u nekim zemljama koje su imale korumpirane režime, te ih se više ne podržava radi očuvanja nacionalne sigurnosti. Ignoriranje problema utjecaja raširenosti korupcije i organiziranog kriminala u bivšem Istočnom bloku, kao i sličnih problema u drugim dijelovima svijeta dovodi i „uvozi“ korupciju i u razvijene demokracije (Rose-Ackerman, 2002:28).

Popis osnovnih oblika međunarodnog uplitanja pri tome slijedi pet temeljnih načela:

Kada su u pitanju fondovi međunarodnih organizacija, bilo da se radi o zajmovima ili subvencijama, ove će organizacije imati interesa za učinkovito iskorištavanje njihovih resursa.

Ako zemlja želi reformu, agencije za pružanje pomoći mogu direktno podržati nastojanja borbe protiv korupcije kao što je reforma državne službe i sustava upravljanja proračunom i financijama. Ako je gospodarska i financijska kriza pogoršana institucionalnom strukturom koja je sklona korupciji, međunarodna pomoć može biti uvjetovana reformom čak i kada država ne želi promjene (Šujster, 2007:83).

[521] Na jugu Italije istraživanja pokazuju da se preko polovine malih i srednjih poduzeća povuklo iz javnih poslova nakon pritisaka organiziranih grupa ili njihovih političkih saveznika. „Još uvijek korumpiran“, *The Economist*, 5. veljače 1994.

Međunarodna nastojanja mogu se usredotočiti na smanjenje želja multinacionalnih kompanija za plaćanjem mita i na njihovo zauzimanje za reformatorska nastojanja. U nekim zemljama u razvoju multinacionalni ulagači veći su i moćniji od države s kojom posluju, a kada to nije slučaj, multinacionalne kompanije često imaju znatan utjecaj u državi.[522]

Da bi kontrolirali tijek protuzakonitih fondova, međunarodni programi mogu kontrolirati korupciju praćenjem transfera tajnih fondova preko granice gdje im se umreženošću novih tehnologija može ući u trag. Svoju ulogu imaju i drugi tipovi suradnje u borbi protiv organiziranog kriminaliteta kao što je suzbijanje pranja novca povezanog s financiranjem iz kriminalnog miljea u kontroli međunarodnih terorističkih aktivnosti.

Smanjenje korupcije i financiranja iz kriminalnog miljea potiče osnivanje novih međunarodnih institucija. Da bi mogle dobro funkcionirati, brojne reforme zahtijevaju suradnju izvan državnih granica i stvaranje novih tijela za reviziju i donošenje odluka.

Međunarodni interes za kontrolu financiranja iz kriminalnog miljea je na najvišem stupnju od kada su terorizam i financiranje terorizma u žarištu zanimanja jer postoji rizik nastajanja novih oblika financiranja terorizma i načina ostvarivanja privatnih koristi kao rezultat dobro smišljenih zakulisnih reformi načinjenih radi unapređivanja gospodarstva ili demokratizacije političkih prilika. Za takav način pristupa financiranja iz kriminalnog miljea koji razara društvo idealne su tranzicijske zemlje poput Sirije koja sada prolazi dramatičnu tranziciju kao diktatorski režim koji nije inovirao unutarnji sustav vrijednosti.

4. Kontrola korupcije u međunarodnim razvojnim projektima

U razvojnim projektima međunarodne zajednice nestanak oko pedeset milijarda dolara u deset godina u Rusiji od kredita i pomoći Svjetske banke, te oko dvanaest milijarda dolara u Maleziji, dakle i u vrijeme blokovske politike i čvrste željezne zavjese, istočni blok je davao projekte pomoći koje nije mogao kontrolirati, što samo po sebi pokazuje koliko je korupcija opasna. Korupcija i bogaćenje na kriminalan način, pranjem novca te financiranjem iz kriminalnog miljea pojedinih subjekata na političkoj sceni može znatno smanjiti broj dobrih projekata i usporiti ili čak zaustaviti reforme i napredak države što ima posljedicu nesigurnosti za građane u smislu nacionalne sigurnosti (Šujster, 2007:84).

Nastojanje nekih država da se opiru kontroliranju korupcije jer vjeruju da podmićivanje u zemljama u razvoju koristi njihovom domaćem poslovanju teško može biti argumentirano jer se onda korupcija vraća u njihove zemlje, a javnost u razvijenim zemljama spram korupcije ima stav da je korupcija neprihvatljiva, te je zakonski regulirana kao kazneno djelo.

Neki analitičari tvrde da kontrola korupcije ne bi trebala biti povezana s međunarodnom trgovinom i zajmovnom politikom. Oni uvjeravaju da međunarodna tijela ne bi trebala povezivati financiranje terorizma i pomoć u razvoju, ali financiranje iz kriminalnih miljea je kroničan problem te utječe na konkurentnost globalne ekonomije i učinkovitost ulagačkih i razvojnih projekata širom svijeta što se vidi i kroz cijenu nafte, naime, tzv. Islamska država izvozi naftu i tako se financira.

[522] Financiranjem političkih stranaka i kupovanjem njihovih zastupnika (op. a).

Organizacije za kreditiranje i pružanje pomoći moraju uvidjeti političku i organizacijsku dinamiku koja otežava kontrolu korupcije i financiranje iz kriminalnog miljea te da politička opcija koja je na vlasti u pojedinoj državi ima neka dugovanja prema svojim glavnim financijerima. Ako oni sami ne provode kontrolu trošenja sredstava i ne pristupaju revizijski, novac odlazi pojedincima ili nenamjenski.[523] Dakle oni koji bi se trebali boriti i razvojnim projektima pomagati demokratske vrijednosti, zahvaćeni su korupcijom jer su prihvatili devijantno ponašanje zemalja u razvoju (Kotkin, Sajó, 2002). Uglavnom, kupovanje nafte od terorističkih organizacija predstavlja kriminalno ponašanje privatnih kompanija koje u prešutnom dogovoru s državom dijele profit, a dugoročno ruše svoju nacionalnu sigurnost.

5. Kontrola korupcije u međunarodnom poslovanju

Antikorupcijska politika međunarodne zajednice provodi se jednim dijelom kroz međunarodne institucije poput Međunarodnog monetarnog fonda, Svjetske banke, razvojnih programa Ujedinjenih naroda (UNDP), bilateralne agencije za pružanje pomoći, te razne regionalne razvojne banke. Te institucije imaju zadatak da osiguravaju integritet njihovih projekata, za podržavanje dubokih strukturnih reformi u zemljama u razvoju i tranzicijskim zemljama.[524]

Agencija za međunarodni razvoj i UNDP stalno daju tehničku potporu reformama država, šire svoje projekte da bi u njih uključili i problem korupcije. MMF je prepoznao da korumpirane i tajne veze između vlade, privatnih poduzeća, bankarskog i financijskog sektora pridonosi pogoršanju krize u državi (Rose-Ackerman, 2002: 29).

Međunarodni projekti prvenstveno imaju za cilj reformama napraviti promjene u zakonodavstvu koje bi smanjile korupcijske poticaje u pojedinim sektorima i osigurale poboljšanje u cjelovitosti nadziranja i provođenja zakona te reformirale državne službe i jačale kontrolu. Posebni sektori su mete reformatorskih napora, te MMF i Svjetska banka ciljaju na porezne i carinske sustave.[525] Nije problem samo smanjenje korupcije u postojećim institucijama, već i prevencija u pojavljivanju korupcije u novim institucijama. Evidentno je da poslije rata ili turbulentnih događaja u pojedinim državama gdje nije bilo ratnih sukoba dolaze međunarodne institucije koje pokušavaju dovesti do zakonitog reda u financijskom poslovanju što je općenito prihvaćeno u međunarodnoj zajednici. Pomoću novih tehnologija (umreženost i centraliziranje svih računa) prate se novčana sredstva i pomoć, sprječava se odlazak novca u *„crne rupe“* te legaliziranje novca u poduzetničke poslove.

Postoji niz inicijativa da se spriječi korupcija u međunarodnom poslovanju s korumpiranim vlastima, pa je tako i Organizacija za ekonomsku suradnju i razvoj (OECD) potpisala

---

[523] Svjetska banka je primjerice ispitivala ponašanje svojih zaposlenika i izolirala nekoliko primjera korupcije. „Interna istraga korupcije u Svjetskoj banci“, *Financial Times*, 17. srpanj 1998., „Svjetska banka zapošljava revizore za ispitivanje njezinog trošenja, spomenuta moguća podmićivanja i pronevjere“, *Washington Post,* 16. srpanj 1998. g.

[524] Poput projekta „FIAS“ u Hrvatskoj pod naslovom: „Administrativne prepreke stranim ulaganjima“, Međunarodne financijske korporacije (IFC) i Svjetska banka, siječanj 2001.

[525] Kao i Svjetska banka, Azijska banka za razvoj također je krenula s antikorupcijskom politikom. „Azijska banka razotkriva strogu politiku korupcije“, *Financial Times,* 9. srpanj 1998.

međunarodnu konvenciju protiv podmićivanja stranih javnih službenika u međunarodnim poslovnim transakcijama 17. prosinca 1997. godine u Parizu zajedno s 29 vlada, a od potpisnika se zahtijeva da stave izvan zakona podmićivanje inozemnih stranih službenika. Naime, u mnogim se zemljama mito, plaćeno radi stjecanja inozemnih poslova, može odbijati od poreza (manjkavost u zakonu koja potiče na podmićivanje).[526] Mnogi analitičari se slažu u tome da dokument OECD-a ima veliki nedostatak, a to je izuzeće plaćanja političkim strankama i stranačkim dužnosnicima. Stručnjaci su prepoznali problem, jedino nedostaje političke volje da se on i zakonski pokuša riješiti jer kupovinom stranaka i pojedinaca kupuje se i korumpira cijeli sustav od financijera političkih čimbenika kojima oni zauzvrat, osim novcem, pogoduju i političkom situacijom u zemlji, stoga nacionalna sigurnost trpi nesagledivu ugrozu (Šujster, 2007:86).

6. Sprječavanje pranja novca i ostalih kriminalnih aktivnosti

Organizirani kriminal je veliki protivnik antikorupcijskih nastojanja na nacionalnoj i međunarodnoj razini. Korumpirana vlast treba organizirani kriminal zbog pranja novca izvan nacionalnih granica, a organizirani kriminal treba korumpiranu vlast također za pranje novca kroz nezakonita poduzeća koja plaćaju mito korumpiranoj vlasti i tako se sve odvija u korupcijskom krugu. Ove radnje imaju veliki korupcijski utjecaj na funkcioniranje sustava u državi.

Provođenje zakona i kontrola granica mora predstavljati prepreku u sprječavanju djelovanja tvrtki koje „uvoze“ korupciju, te smanjiti utjecaj kriminala na politiku pojedine države. Političari koji primaju mito pokušati će osigurati ulaganje kapitala u nezakonitim poduzećima bilo gdje na svijetu. Inače, "pranje novca" je radnja koja taj novac treba prikazati kao da je stečen na zakonit način. Tehnika pranja novca koja se najčešće koristi jest prebacivanje sredstava u zemlje gdje je dozvoljeno prikrivanje identiteta klijenta. Put novca se širi dalje prema međunarodnim bankama koje imaju pristup svjetskom tržištu.

Kako bi se sve to odvijalo sa što manje problema, podmićuju se službenici u raznim zemljama te je korupcija, zajedno s kriminalom, proces koji je dobio globalnu dimenziju.[527] Danas se korupcija shvaća kao problem prvog stupnja i prije svega se problematiziraju prekogranična podmićivanja. Većina zemalja nema propise koji se odnose na progon podmićivanja službenika drugih država. Primjerice, ukoliko Nijemac daje mito francuskom službeniku, on je prema francuskom pravu kažnjiv. U Njemačkoj ga se, međutim, ne može progoniti jer prema njemačkom pravu konkretni pojedinac nije počinio kazneno djelo.

Ova temeljna koncepcija postoji u gotovo svim državama u sličnom obliku. Samo države koje manje strogo razlikuju službenike i namještenike mogu eventualno, prema propisima, obuhvatiti osim svojih i druge službenike. To se uglavnom čini teoretskom mogućnosti.

[526] SAD zabranjuju davanje mita kao porezne olakšice, a nekoliko drugih zemalja u postupku je izmjene svojih propisa u skladu s navedenom preporukom.

[527] Na seminaru koji je održan u Hrvatskoj, u Ministarstvu unutarnjih poslova, predstavnici Europola (Europska policija) na pitanje autora ovog rada je li organizirani kriminal iz Hrvatske integriran u Europu, odgovorili su potvrdno. Isto tako složili su se s time da sve dotle dok Hrvatska policija ne bude integrirana u Europol, kriminalci će biti u prednosti, jer njih ne vežu nikakvi uvjeti za pristup u Europsko kriminalno područje.

Svakako je dvojbeno trebaju li se i mogu li se donošenjem odluke o ukidanju razlikovanja između podmićivanja državnih službenika i namještenika obuhvatiti i inozemni državni službenici kao namještenici. U stvarnosti to znači da u navedenom slučaju podmićivanje francuskog službenika za Nijemca ne može imati za posljedicu kaznenopravno sankcioniranje dok se on zadržava u Njemačkoj. Prema njemačkom pravu davatelj mita nije počinio kazneno djelo (Šujster, 2007:87).

Od *afere Lockheed* (američka zrakoplovna industrija potkupljivala je političare u Europi i Japanu) u SAD - u imaju specijalne odredbe u svezi podmićivanja stranih državnih službenika. Oni danas na međunarodnom planu predstavljaju uzor pa različite države i međunarodne organizacije razmatraju uvođenje takvih odredbi (Šujster, 2007:86-87). Ipak, treba napomenuti da su ovi propisi ograničenog dosega.

Kazneno definiranje u svezi s podmićivanjem i korupcijom variraju od zemlje do zemlje. U nekim su državama predviđene vrlo teške kazne, a u Kini čak i smrtna kazna. Ograničenje ili nepostojeća mogućnost sankcioniranja podmićivanja namještenika ili nepostojanje normi u svezi s jednostavnim podmićivanjem su, nažalost, vrlo često prisutne manjkavosti pravnog sustava u velikom broju država.[528]

Neovisno o upornosti i nastojanjima nacionalnih i međunarodnih instanci da kontroliraju taj fenomen, pranje novca postaje sve veći problem jer se stvaraju tzv. financijske oaze, a i neka gospodarska tržišta u razvoju su podložna i koriste se za pranje novca. Veliki je problem pranja novca što otkrivena transakcija nosi negativne sankcije, a ne pridonosi povećanju ulaganja u kapitalom siromašne zemlje poput obustava započetih investicijskih projekata. Kontrola i sprečavanje pranja novca neće imati rezultata ukoliko mjere nisu povezane i koordinirane s nastojanjima poboljšanja djelovanja i odgovornosti onih koji obnašaju vlast.

Međunarodna nastojanja kontroliranja nezakonitog poslovanja po važnosti su na drugom mjestu. Ako je korupcija povezana s organiziranim kriminalom, problem međunarodnih organizacija za pružanje pomoći je veći i kompleksniji. U slučaju da je država prožeta kriminalom, organizacije izvana ne mogu učiniti mnogo, osim čekati i nadati se boljoj situaciji.[529] Dakle država bi trebala učiniti napore za smanjenje pretjeranih zarada dostupnih poduzetnicima kriminalcima u zakonitim poslovanjima.[530] Jedno je rješenje podupiranje ulaska zakonitih poduzeća s velikim kapitalom koja će se uz pomoć države i provođenja zakona moći natjecati s mafijaškim poduzećima (Rose-Ackerman, 2002:56).

Ukoliko je vlast korumpirana, a najčešće se to događa u izbornim kampanjama zbog uzimanja sredstava od raznih financijera, onda su ova nastojanja 'sizifovske' naravi. Ta nastojanja mogu biti i prividna jer ograničavanje pranja novca i kontroliranje nezakonitog poslovanja očito zahtijevaju međunarodnu suradnju, te sama po sebi neće imati puno utjecaja na razinu korupcije ako pozadinski utjecaji ne proizlaze iz nezakonitih poslovnih aktivnosti, već iz koristi kontroliranja države.

---

[528] Najvažnije međunarodno tijelo uključeno u trenutna kontroliranja pranja novca je Odred za financijsko djelovanje osnovan 1989. godine, koji ima predstavnike iz OECD-a, Hong Konga, Singapura, Zaljevskih država i Vijeća Europe.

[529] Glavni motiv je primanje i usmjerivanje strane pomoći. *V.* Kotkin, Sajo (2002)

[530] Svjetska banka je priznala 2005. da ne zna gdje je otišlo 50 milijardi dolara koje je dano Rusiji u tranzicijskom procesu.

Ako se unutarnji politički čimbenici i zdrave snage demokracije dogovore i naprave konsenzus za borbu protiv korupcije, država bi trebala odgoditi privatizaciju jer je državno poduzeće lakše nadzirati nego privatno.[531]

Borba protiv korupcije će biti jalova ako su državne političke i birokratske institucije slabe i ako tržište nije uređeno sukladno ponudi i potražnji, stoga nikakva međunarodna pomoć za razvoj neće dati pozitivne rezultate.

Ukoliko država s ozbiljnim korupcijskim problemom ne uvidi i prepozna problem i ne počne ga rješavati na način koji nema karakter 'lova na vještice', nikakvih promjena nabolje neće biti. Nažalost, antikorupcijska kampanja i borba protiv korupcije često nisu u interesu onih koji su na vlasti jer su na vlast došli zahvaljujući financijerima protiv kojih bi se trebali boriti (sumnjivo predizborno financiranje).

Jednostavnih rješenja za suzbijanje korupcije u političkim financijama jednostavno nema, niti je moguće propisati bilo kakav univerzalni popis mjera koje bi mogle učinkovito smanjiti razinu korupcije u financiranju politike u svakoj pojedinoj zemlji. Ono o čemu se možda može govoriti odnosi se isključivo na temeljna načela u oblikovanju takve politike, a ona se, smatra Hodess (2004:16-17) mogu svesti na sljedeće: utvrđivanje učinkovitog okvira za sprečavanje sukoba interesa kako bi se onemogućilo da izabrani dužnosnici osiguravaju probitke za svoja vlastite poslovne pozicije ili za pozicije onih koji su ih podržali u predizbornoj kampanji; osiguravanje transparentnosti u financiranju politike javnim objavljivanjem i davanje na uvid podataka o izvorima financiranja nečije političke aktivnosti neovisnoj agenciji; takva vrsta podataka mora pri tome biti izložena javnosti po unaprijed poznatoj proceduri; djelotvornost u provođenju regulatornih mjera i reviziji političkih financija; raznolikost izvora financiranja i postavljanje gornjih limita mogućih prihoda i rashoda; raznolikost izvora financiranja politike doprinosi manjem oslanjanju političkih stranaka na, primjerice, korporativni novac i može potaknuti manje donatore da doprinose strankama, kao što je to slučaj u Kanadi gdje deseci i stotine tisuća malih donatora u stvari demokratiziraju proces financiranja politike; jednak i pravedan pristup masovnim medijima, posebice nacionalnim televizijskim kanalima, pokazuje se redovito kao jedan od važnih elemenata antikorupcijske strategije. Mediji, osim toga, preko različitih nastojanja vezanih uz istraživačko novinarstvo mogu ukazivati na koruptivne oblike u financiranju predizbornih kampanja, odnosno, vršiti pritisak na stranke i kandidate da javno objave svoje izvore financiranja; sudjelovanje civilnog društva u oblikovanju regulatornog okvira financiranja stranaka i izbora. U nizu zemalja je upravo na temelju takvog sudjelovanja organizacija civilnog društva značajno unaprijeđen zakonski okvir koji se bavi financiranjem politike da ne bi dolazio novac iz sumnjivih izvora, pogotovo kriminalnog miljea.

7. Migracije i protok novca sumnjivog porijekla

Svjedoci smo migracijske krize koja je zahvatila 2015. godine Europsku uniju u dosada nezapamćenim brojkama migranata. Republika Hrvatska je koridor prema zapadu stotinama

[531] „U državama koje tako postupe, korumpirana vlast osmisli projekte javnih radova“ (Rose-Ackerrman, 2002: 219).

tisuća emigranata prema „*boljem i sigurnijem životu* “. Na prijetnju organiziranog kriminala uvelike utječu hrvatski prometni, gospodarski i geografski položaj, nedovoljno konsolidirane države s juga i istoka Europe te pritisak na Balkansku rutu zbog ratnih zbivanja na Bliskom istoku i sjevernoj Africi. Nastavljena je pojava korištenja hrvatskog teritorija kao boravišta pripadnicima regionalnog organiziranog kriminala, bilo da je riječ o skrivanju od suprotstavljenih kriminalnih skupina ili izbjegavanju kaznenog progona u svojim državama te planiranju daljnjih kriminalnih radnji. Takva će situacija i dalje biti prijetnja stanju sigurnosti u Republici Hrvatskoj zbog financijskih ulaganja na području Republike Hrvatske s ciljem prikrivanja izvora sumnjivog novca. Republika Hrvatska je, također, država koja se nalazi na europskim pravcima prijevoza kokaina iz Južne Amerike u Europu, a i pojačano je financijsko polaganje novaca kroz banke koje su većinom u stranom vlasništvu. Poznato je da je kokain, uz otmice, glavni prihod raznih kriminalnih i terorističkih skupina u Južnoj Americi. Nacionalnu ugrozu predstavlja i nestabilna sigurnosna situacija na području Bliskog istoka, Afrike i Ukrajine te se time povećava krijumčarenje oružja i vojne opreme. Pripadnici kriminalnog miljea iz Republike Hrvatske i regije u tome su prepoznali zaradu i krenuli s ilegalnom trgovinom oružja. Opasnost je vrlo velika s obzirom da oružje nerijetko završava u rukama različitih terorističkih organizacija. Europska središnja banka će, navodno, povući novčanice od petsto eura jer te novčanice koriste teroristi za financiranje svojih aktivnosti („Jutarnji list“ 3. veljače 2016. godine). Plaćaju gotovinom i stoga je problematično otkrivanje takvih transakcija. Neke zemlje su uvele plaćanje od strane migranata pa i uzimanja nakita za proveden boravak u njihovoj zemlji dok ne dobiju azil. Amerikanci su uništili skladište dolara u Siriji proisteklo iz prodaje nafte i kulturnih artefakata tzv. Islamske države. No, postavlja se pitanje koliko je takvog novca distribuirano uz pomoć migranata u Europsku uniju i ostale zemlje i hoće li biti iskorišten za financiranje terorističkih aktivnosti.

8. Zaključak

U Republici Hrvatskoj kaznena djela pranja novca i financiranja terorizma definirana je *Zakonom o sprječavanju pranja novca i financiranja terorizma* od 01. siječnja 2009. godine. Navedenim zakonom i podzakonskim aktima donesenim na temelju njega naša je zemlja preuzela sve relevantne smjernice i konvencije međunarodnih tijela i organizacija koje imaju za cilj učinkovitu borbu protiv plasiranja „prljavog“ novca, odnosno novca stečenog kaznenim djelom u legalne financijske tokove. Pojam pranja novca zapravo podrazumijeva niz aktivnosti u bankovnom, novčarskom ili drugom gospodarskom poslovanju kojima je cilj prikrivanje pravoga izvora novca, odnosno imovine ili prava priskrbljenih novcem koji je stečen na nezakonit način, kaznenim djelom. Općenito, pod pojmom pranja novca podrazumijeva se svaki postupak usmjeren na prikrivanje nezakonito stečenog prihoda na način da se taj prihod u financijskom sustavu prikaže ili da se stvori dojam da se radi o zakonitoj zaradi. Problem sprječavanja financiranja iz kriminalnog miljea može se riješiti jedino globalnom akcijom međunarodne zajednice zbog današnjih brzih transakcija novca u financijske oaze omogućenih visokotehnološkim dostignućima. U tom smislu neke su države, na pritisak međunarodne zajednice, konačno dale na uvid određene sporne račune kako bi se doznalo porijeklo novca i time otežalo financiranje kriminalnih aktivnosti i terorizma. Ove

kriminalne organizacije mogu se uvelike onesposobiti ako im se ukine (samo)financiranje za planiranje i realizaciju kriminalnih i terorističkih aktivnosti.

LITERATURA

Hodess, Robin (2004). *Introduction to Political Corruption*. U: Global Corruption Report 2004., 11-18.
Kotkin, Stephen, Sajo, Andras (ur.) (2002). *Political Corruption in Transition: A Skeptic's Handbook.* Budimpešta: Central European University Press.
Noack, Paul (1995). *Politička dimenzija korupcije: Ili - Kakvu štetu može korupcija nanijeti demokratskom sustavu*. Predavanje održano 28. ožujka 1995. god. u Policijskoj akademiji Munster.
Rose-Ackerman, Susan (2002). *Korupcija i vlada: uzroci, posljedice i reforma*. Zagreb: Progres.
Šujster, Tihomir (2007). *Korupcija i financiranje političkih stranaka*, Magistarski rad. Fakultet političkih znanosti.
Tatalović, S. (1996). Upravljanje u političkim sustavima i sustavima obrane. Zagreb: DEFIMI.
Uberhofen, Michael (1997). Kazneno suzbijanje korupcije: Pravno usporedno istraživanje Instituta za inozemno i međunarodno kazneno pravo Max-Planck. Kriminalistik, 11, 712-716.
Walecki, Marcin (2004). *Political Money and Corruption*. U: Transparency International Global Corruption Report, 19-32.
Ward, Gene (2004). *The Role of Disclosure in Combatting Corruption in Political Finance*. U: Transparency International Global Corruption Report., 38-49, http://www.transparency.org/publications/gcr

Pravni propisi

Zakon o financiranju izborne promidžbe za izbor predsjednika Republike, Narodne novine, 105/2004
Zakon o sprječavanju pranja novca i financiranja terorizma, Narodne novine, 87/08, 25/12

Tihomir Šujster

UNDERWORLD FINANCING, A THREAT TO THE EFFICIENCY OF NATIONAL SECURITY

Summary

The fight against corruption has strengthened at the international level in particular against financing out of criminal sources, as such financing directly destroys the foundations of democracy and the system of basic values. When organizied crime is directly involved the functioning of the system it is very difficult and often impossible to develop democratic institutions and ensure the normal economic development, while the national security system is severely compromised. The prevention of money laundering and terrorist financing as it is applied in the Republic of Croatia is based on the Prevention of Money Laundering and Terrorist Financing Act which has been in force since January 1, 2009. This Act and its bylaws transpose all relevant guidelines and conventions of international bodies and organizations, aimed at effectively preventing investments from criminal activities into legal financial transactions. The criminal scene was partly boosted by the globalization of markets and financial transactions while modern technologies enable easy placement of money so that classic money laundering ways are replaced by transactions that are difficult to trace. International agreements have made tracing of money transactions possible as nearly everything is networked on a global level. The diversity of methods and techniques involving money transactions through the financial and the non-financial sector prioritizes and highlights the importance of prevention of money laundering, terrorist financing out of criminal sources and other criminal activities for the protection of national security.

Key words: *finance, crime, national security, terrorism.*

PREGLEDNI ZNANSTVENI RAD

Matija Frčko[532]
Davor Solomun[533]

UNUTARNJA SIGURNOST EUROPSKE UNIJE U SUVREMENIM UVJETIMA MIGRACIJSKE KRIZE

Sažetak

U radu se analizira suradnja na području unutarnje sigurnosti Europske unije i ocjenjuje prilagođenost njene sigurnosne politike i operativne prakse novim izazovima i prijetnjama. EU kao sigurnosna integracija podrazumijeva partnerski i solidaran odnos zemalja članica, te predanost zajedničkim institucijama u kreiranju provedivih sigurnosnih politika temeljenih na zajedničkim vrijednostima, uz uvažavanje specifičnosti država članica. U uvjetima suvremenih prijetnji i ugroza sigurnosti, trenutna migracijska kriza na mediteranskoj i tzv. zapadno-balkanskoj ruti, pokazala se kao potencijalni katalizator ionako sve izraženije terorističke prijetnje ali i porasta netolerancije i ksenofobije u Europi. Pri tom, stvara se plodno tlo za transnacionalni organizirani kriminal zbog čega se aktualizira pitanje i važnost jačanja sigurnosti na vanjskim granicama Unije. Sigurne vanjske granice preduvjet su i jamstvo očuvanja Unije kao prostora slobode i sigurnosti, a ovise o tješnjoj međudržavnoj i međuinstitucionalnoj suradnji, specijalizaciji službenika tijela za provođenje zakona te o uvođenju novih tehnologija. Elementi sigurnosnih odluka te njihova primjenjivost i učinkovitost u operativnim djelovanjima tijela za provedbu zakona u funkciji zaštite i sigurnosti granica, odnosno unutarnje sigurnosti Unije, predstavljaju izazove u ovome radu.

Ključne riječi: *Europska unija, unutarnja sigurnost, vanjske granice, migracije, operativna suradnja*

1. UVOD

Europska unija kao politička i ekonomska međuvladina i nadnacionalna zajednica europskih država još od početaka prvih europskih integracija stavlja sigurnost i mehanizme ostvarivanja sigurnosti u središte svojih političkih interesa i aktivnosti. Jedan od glavnih preduvjeta, ali i koristi uspješnog političkog integriranja europskih država jest otvaranje unutrašnjih granica radi nesmetanog protoka ljudi, robe i kapitala. Otvaranje granica te tehnološki i ekonomski napredak značili su, osim sve većih sloboda, porast prijetnje od kako prekograničnog, tako i novih vrsta kriminaliteta zbog slabljenja nadzora uslijed ukidanja kontrola na unutrašnjim granicama i posljedično povećane mobilnosti organiziranih kriminalnih skupina koje su tehnološko i organizacijski evoluirale usporedo s novim integracijama. Stoga se javila potreba za zajedničkim, usklađenim odgovorom na nove sigurnosne izazove i prijetnje. Suradnjom

[532] Matija Frčko, bacc. crim., pol. inspektor, Služba za međunarodnu policijsku suradnju, MUP RH e-mail: mfrcko@gmail.com
[533] mr. sc. Davor Solomun, viši predavač, Visoka policijska škola, voditelj Centra za policijska istraživanja, e-mail: dsolomun@fkz.hr

država članica prvo u izvaninstitucionalnom okviru, a potom i pod okriljem europskih institucija pokušalo se suprotstaviti prekograničnom kriminalitetu, terorizmu i drugim najtežim ugrozama. Sve tješnjim integriranjem nastala je konačno i Europska unija. Izgradnjom sve većeg međusobnog povjerenja stvoreni su institucionalni okviri i mogućnosti za osnivanje supranacionalnih tijela za provedbu zakona. Kruna takve suradnje bilo je donošenje strategija s područja unutarnje sigurnosti. Europska unija je postala i sigurnosna integracija.

Analizom strateških dokumenata iz područja unutarnje sigurnosti ne prepoznaje se službena definicija unutarnje sigurnosti Europske unije. Kod država članica ne nailazi se na prigovor takvoj praksi. Jedan od razloga je svakako taj što se radi o sve širem i složenijem, vrlo dinamičnom području aktivnosti[534] s velikim brojem dionika podložnom stalnoj reevaluaciji, dopunama, promjenama prioriteta i u krajnjem slučaju promjenama strateškog smjera. Odgovornost za unutarnju sigurnost na vlastitom teritoriju još uvijek primarno počiva na samim državama, no za njeno postizanje na razini Europske unije nužna je međudržavna i međuinstitucionalna suradnja. Generatori unutarnje nesigurnosti ne potječu nužno samo s prostora unutar Europske unije, već mogu nastati (i nastaju) blizu ili daleko izvan njenih granica. Zbog suvremenih katalizatora nesigurnosti poput krize u Ukrajini, arapskog proljeća, rata u Siriji Iraku te nestabilnosti u Subsaharskoj Africi, kod promišljanja o strategijama unutarnje sigurnosti jednaka pozornost se posvećuje njezinoj vanjskoj i unutarnjoj dimenziji, odnosno njihovoj sinergiji u kreiranju sigurnosnih politika. U najširem kontekstu unutarnja sigurnost Europske unije definira se kao međusobna suradnja nadležnih tijela i drugih relevantnih društvenih faktora u svrhu očuvanja mira unutar granica Unije te zaštite ljudi i vrijednosti slobode i demokracije kako bi svi mogli živjeti svakodnevnim životima bez straha.

Uz klasične statističke pokazatelje stanja unutarnje sigurnosti kao što su broj pojava i događaja koji utječu na sigurnost, njihova rasprostranjenost, posljedice izražene u obliku broja smrtno stradalih i ozlijeđenih osoba te nastale materijalne štete, itd., vrlo je bitan subjektivni osjećaj sigurnosti pojedinca i njegovo povjerenje u sigurnosni sustav. Suvremeno shvaćanje sigurnosti u Europskoj uniji slijedi humanocentrični koncept „ljudske sigurnosti“[535] u kojem je referentni objekt sigurnosti vertikalno proširen s države na pojedinca. Pojačana dinamika društvenih odnosa povezana s društvenim razvojem sa sobom donosi i realno veći broj pojava i događaja koji utječu na sigurnost i sam kvantitativan prikaz zasigurno ne može dati cjelovitu sliku stanja. Zato se kod procjene stanja unutarnje sigurnosti i rangiranja najvećih ugroza,

---

[534] Primjerice, Parlamentarni odbor za Europsku uniju Gornjeg doma Parlamenta Ujedinjenog Kraljevstva u poglavlju br. 2. svojeg Izvješća od 17. svibnja 2011. godine u kojem se raspravlja o akcijskom planu za provedbu Strategije unutarnje sigurnosti Europske unije – *„Pet koraka prema sigurnijoj Europi“*, smatra kako definiranje unutarnje sigurnosti Europske unije nije nužno sve dok istaknuti prioriteti potpadaju pod „razumno gledanje na unutarnju sigurnost“. Izvor: www.parliament.uk, The EU Internal Security Strategy - European Union Committee, http://www.publications.parliament.uk/pa/ld201012/ldselect/ldeucom/149/14905.htm (preuzeto 14. veljače 2016.)

[535] Koncept ljudske sigurnosti nastao je 1994. godine u sklopu Razvojnog programa Ujedinjenih naroda. Izvor: HUMAN SECURITY IN THEORY AND PRACTICE, An Overview of the Human Security Concept and the United Nations Trust Fund for Human Security http://www.un.org/humansecurity/sites/www.un.org.humansecurity/files/human_security_in_theory_and_practice_english.pdf (preuzeto 4. veljače 2016.)

pozornost obraća i na rezultate anketnih ispitivanja provedenih nad građanima Europske unije.

Uključenost drugih relevantnih društvenih faktora u postizanje unutarnje sigurnosti Europske unije upućuje na multisektoralnost i sveobuhvatnost pristupa u rješavanju nesigurnosti. Odgovornost za postizanje sigurnosti je proširena od nacionalne države prema međunarodnim organizacijama, regionalnim i lokalnim razinama, nevladinim organizacijama, javnom mnijenju, medijima pa i pojedincima. Multisektorsko shvaćanje sigurnosti kao sastavni dio koncepta ljudske sigurnosti, osim klasičnih elemenata sigurnosti obuhvaća prijetnje s područja ekonomske sigurnosti, sigurnosti prehrane, zdravstvene sigurnosti, sigurnosti okoliša, osobne sigurnosti, sigurnosti zajednice i političke sigurnosti (Solomun, 2013.). Koncept prepoznaje međuovisnost prijetnji s navedenih područja i poziva na holistički pristup rješavanju nesigurnosti.

Uvažavanje konteksta nastanka otvara prostor iznalaženju prilagođenih rješenja za pojedine prijetnje. Također omogućava preventivni pristup kroz institucionalno pružanje zaštite komplementarno s jačanjem sposobnosti zajednica i pojedinaca u razvijanju njihovog punog potencijala i njihovim uključivanjem u zajedničke napore za postizanje sigurnosti.

Suvremena institucionalna zaštita naglašava važnost brige o ljudskim potencijalima. Ona se odnosi na razvoj i upravljanje ljudskim potencijalima kroz specijalizaciju i cjeloživotno učenje na svim razinama odgovornosti te implementaciju novih tehnologija.

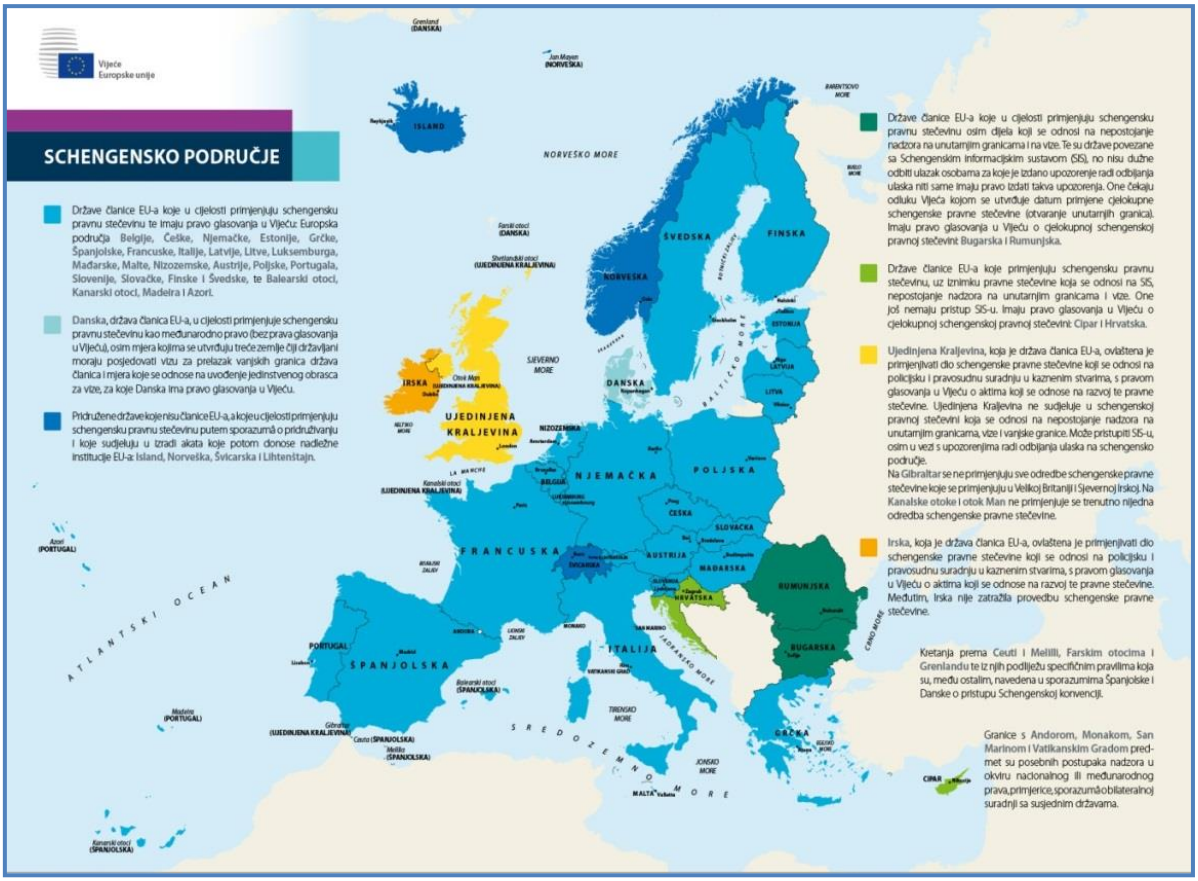
Skrb i upravljanje ljudskim potencijalima jedna je od najvažnijih funkcija suvremenog menadžmenta, a ljudski kapital i u privatnom poduzetništvu i u državnoj i javnoj upravi jednako je vrijedan i temelji se na istim zakonitostima. (Solomun, 2015, 241 prema Noe i sur., 2006.)

Migracijska kriza koja trenutno pogađa Europsku uniju pokrenula je čitav niz sigurnosnih pitanja i stavila na test koncept njene unutarnje sigurnosti, posebno u dijelu zaštite vanjskih granica i poštivanju ljudskih prava. U političkom i sigurnosnom smislu ona svakako predstavlja veliki izazov, no i priliku za preispitivanje i jačanje postojećeg sustava. U radu se metodom opisnog istraživanja i analizom ključnih strateških dokumenata, znanstvenih i stručnih radova te javnih izvora, pokušava ocijeniti učinkovitost sustava unutarnje sigurnosti Europske unije. Prikladnost i fleksibilnost sustava u operativnom suočavanju s migracijskom krizom analizira se kroz nekoliko aspekata: rješavanja uzroka nesigurnosti, zaštite života i zdravlja izbjeglica i migranata na migracijskim rutama, sigurnosti vanjskih granica te spremnosti država članica na pružanje zaštite tražiteljima azila te sprječavanje sekuritizacije migranata i krize.

2. KREIRANJE SIGURNOSNIH POLITIKA U EUROPSKOJ UNIJI

Europska unija u cilju zaštite zdravlja, života i imovine svojih stanovnika razvija niz zajedničkih sigurnosnih politika na poljima kao što su sigurnost i obrana, unutarnja sigurnost, sigurnost hrane, sigurnost zračnog, pomorskog i cestovnog prometa i transporta, energentska sigurnost i dr. Politika unutarnje sigurnosti Europske unije odnosi se na suradnju na području pravosuđa i unutarnjih poslova.

Suradnja na području pravosuđa i unutarnjih poslova u Europskoj uniji može se analizirati kroz dva razdoblja. Prvo razdoblje počinje nastankom Europske zajednice 1951, godine i trajalo je sve do osnivanja Europske unije 1993. godine. Karakterizirala ga je izvaninstitucionalna suradnja s funkcionalističkim pristupom uspostave međunarodnih tijela sa striktno ograničenom odgovornošću te sa zadacima na onim područjima gdje su se mogli definirati zajednički ciljevi suradnje (Horjan i Šuperina, 2012, 78). Za to razdoblje je između ostalog značajno osnivanje Schengenske skupine 1985. godine s ciljem analize učinaka ukidanja unutarnjih granica unutar pet zemalja članica Europske zajednice sukladno Schengenskom sporazumu (Ivanda, 2001, 49). Mjere smanjene kontrole na unutarnjim granicama su se počele primjenjivati već 15.6.1985. godine, dok je granična kontrola na unutarnjim granicama u potpunosti ukinuta 26.3.1995. godine. Sporazum su do sada implementirale: Belgija, Francuska, Njemačka, Luksemburg, Nizozemska, Portugal, Španjolska, Italija, Austrija, Grčka, Danska, Finska, Island, Norveška, Švedska, Češka, Estonija, Mađarska, Latvija, Litva, Malta, Poljska, Slovačka, Slovenija i Lihtenštajn. Švicarska je ukinula samo kontrolu putnika, no ne i carinarnice. Državljani Andore, Monaka, San Marina i Vatikana, kao i teritorija Grenlanda i Farskih otoka mogu se slobodno kretati po državama potpisnicama Schengenskog sporazuma. Bugarska, Cipar, Hrvatska i Rumunjska su kandidati za ulazak u Schengenski prostor (vidi sliku 1.)



Slika 1. - Schengensko područje (Europsko vijeće, Vijeće Europske unije, 8.2.2016., URL)

Razdoblje institucionalne suradnje započelo je 1993. godine.Ugovorom iz Maastrichta, (1993) – koji se naziva još i Ugovor u Europskoj uniji Europska zajednica je iz gospodarske prešla u

političku integraciju – Europsku uniju. Ugovor je temeljio Europsku uniju na tri stupa: Stupu Europske zajednice, Stupu zajedničke vanjske i sigurnosne politike te Stupu pravosuđa i unutarnjih poslova uz neke izmjene do 2009. godine kada je stupanjem na snagu Lisabonskog ugovora Stup prestao postojati te je apsorbiran u ujedinjene strukture Europske unije i postao Prostor slobode, sigurnosti i pravde.[536] Sukladno Glavi V Lisabonskog ugovora[537] u politike pravosuđa i unutarnjih poslova uvršteni su: azil, migracije, granična kontrola, pravosudna suradnja u kaznenim stvarima, pravosudna suradnja u građanskim stvarima, organizirani kriminal, suradnja u području suzbijanja nezakonite trgovine opojnim drogama, terorizam i policijska suradnja. (Rošić, 2012; prema Đurđević, 2009) Ovim ugovorom je Europska unija dobila nadnacionalne zakonodavne ovlasti u području kaznenog prava i kaznenog postupka što u praksi znači da se u zakonodavnom postupku u navedenim područjima politika mogu donositi sve vrste obvezujućih akata: uredbe, smjernice i odluke. Uredbe imaju izravan, obvezujući učinak u svim državama članicama, smjernice definiraju ciljeve koje je potrebno primijeniti u državama članicama, dok odluke imaju izravan, obvezujući učinak, a na državama samim je da odrede način njihove provedbe u nacionalnom pravnom poretku (Rošić, 2012).

Europsko vijeće[538] daje Uniji opće političke smjernice i prioritete kojom prilikom nema zakonodavnu ulogu. Zbog svog sastava i moći, ali i po svojoj ulozi predstavlja najvažnije političko tijelo Europske unije (Dragović i Mikac, 2012, 27).

Europska komisija[539] je jedina institucija Europske unije koja predlaže zakonodavstvo o čijem donošenju odlučuju Europski parlament i Vijeće Europske unije[540] te kojim se štite interesi Europske unije i njezinih građana u pogledu pitanja koja se ne mogu učinkovito riješiti na nacionalnoj razini. Predsjednik određuje političko usmjerenje Komisije, što povjerenicima omogućuje da zajedno donesu odluke o strateškim ciljevima i izrade godišnji program rada. Odluke se donose na temelju načela kolektivne odgovornosti, konsenzusom, no mogu se održati i glasovanja. Nacrti zakonodavnih prijedloga se dostavljaju Vijeću Europske unije i Europskom parlamentu za sljedeću fazu zakonodavnog postupka Europske unije.

---

[536] Police and Judicial Co-operation in Criminal Matters https://en.wikipedia.org/wiki/Police_and_Judicial_Co-operation_in_Criminal_Matters (preuzeto 16.rujna 2015.)

[537] Pod punim nazivom Ugovor iz Lisabona o izmjenama i dopunama Ugovora o Europskoj uniji i Ugovora o osnivanju Europske zajednice. Potpisan je u Lisabonu 13. prosinca 2007. Na snagu je stupio 1. prosinca 2009. godine., Izvor: Republika Hrvatska, MVEP, Ugovor iz Lisabona http://www.mvep.hr/custompages/static/hrv/files/EUugovori/12007L_Ugovor_iz_Lisabona_hrv.pdf (preuzeto 17. rujna. 2015.)

[538] Članovi Vijeća su šefovi država ili vlada iz svih zemalja Europske unije, predsjednik Europske komisije i Visoki predstavnik Europske unije za vanjske poslove i sigurnosnu politiku. To je tijelo koje na najvišoj razini u Europskoj uniji kreira politike zbog čega se njegovi sastanci, koji se obično održavaju četiri puta godišnje i kojima predsjedava stalni predsjedavajući, često nazivaju „sastanci na vrhu".

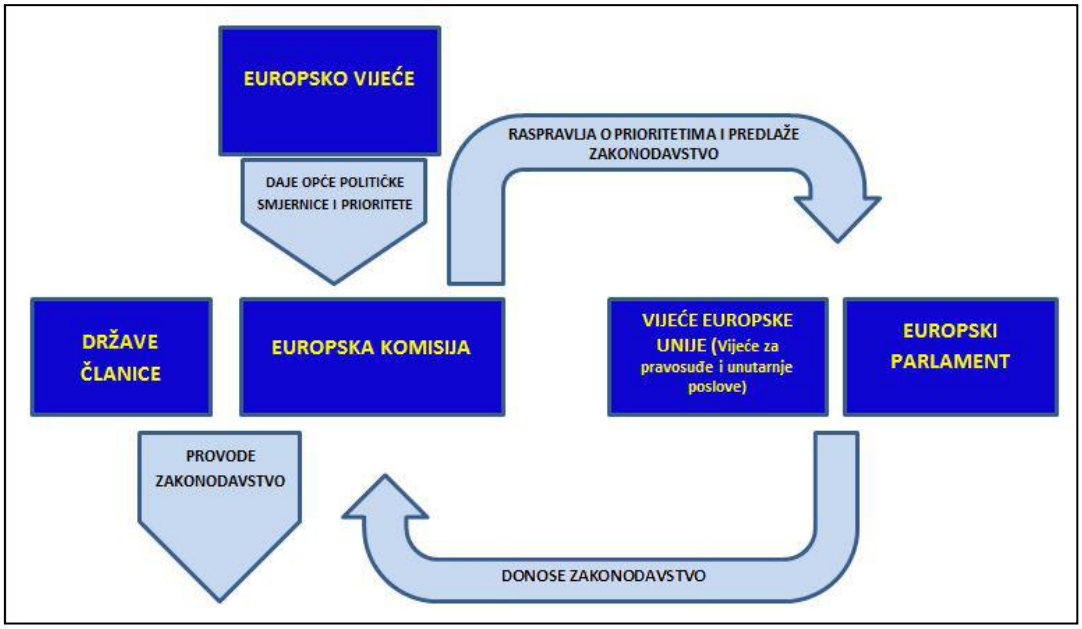
[539] Europe Direct Nova Gradiška: Kako funkcionira Europska unija, str. 5, http://eudirect.ipng.hr/_Data/Files/150713132340302.pdf (preuzeto 17. rujna 2015)

[540] Članovi Vijeća su nacionalni ministri iz svih država članica Europske unije, ovisno o području politike o kojem se raspravlja. Sve države članice se izmjenjuju u obnašanju šestomjesečne dužnosti predsjedavanja Vijećem. U Vijeću se sastaju nacionalni ministri iz svih država članica radi rasprave o zakonodavstvu, njegove izmjene i donošenja te koordinacije politika. Ministri su ovlašteni obvezati svoje vlade da djeluju u skladu s dogovorima sa sjednica. Potrebno ga je razlikovati od već ranije spomenutog Europskog vijeća, kao i od Vijeća Europe koje je međunarodna orgnizacija izvan institucionalnog okvira Europske unije.

Vijeće za pravosuđe i unutarnje poslove[541] djeluje u sklopu Vijeća Europske unije i obično se sastaje svaka tri mjeseca. Vijeće razvija suradnju i zajedničke politike o različitim prekograničnim pitanjima s ciljem izgradnje prostora pravde, sigurnosti i pravde diljem Europske unije. Sastoji se od ministara pravosuđa i unutarnjih poslova iz svih država članica Europske unije. Ministri pravosuđa bave se pravosudnom suradnjom u građanskom i kaznenom pravu, a ministri unutarnjih poslova među ostalim su nadležni za upravljanje granicama i policijsku suradnju. Vijeće za pravosuđe i unutarnje poslove također je odgovorno za civilnu zaštitu. Danska, Ujedinjena Kraljevina i Irska ne sudjeluju u potpunosti u provedbi određenih mjera u području pravosuđa i unutarnjih poslova ili sudjeluju pod određenim uvjetima.

U područjima povezanim sa schengenskom pravnom stečevinom rasprave se odvijaju u formatu mješovitih odbora koji se sastoji se od država članica Europske unije plus četiri zemlje izvan Europske unije koje su dio Schengenskog sporazuma (Island, Lihtenštajn, Norveška i Švicarska). U slučaju zakonodavnih mjera, nakon rasprave u mješovitom odboru donošenje se odvija u Vijeću za pravosuđe i unutarnje poslove, s time da Velika Britanija i Irska ne glasaju.

Vijeće donosi zakonodavstvo, u većini slučajeva zajedno s Europskim parlamentom. Odgovorno je za politike azila i imigracije, pravosudnu suradnju u građanskim i kaznenim stvarima, civilnu zaštitu te za suzbijanje teškog i organiziranog kriminala i terorizma. Ono se također bavi pitanjima koja se odnose na europsko bez granično schengensko područje. Također je nadležno za olakšavanje i jačanje koordinacije aktivnosti država članica u području unutarnje sigurnosti. U tu svrhu rješava pitanja zaštite vanjskih granica i nastoji osnažiti policijsku i carinsku suradnju. Zakonodavstvo provode države članice i Europska komisija.



Slika 2. – Kreiranje politika unutarnje sigurnosti Europskoj uniji (autorska slika).

[541] Vijeće za pravosuđe i unutarnje poslove, www.consilium.europa.eu/hr/council-eu/configurations/jha/ (preuzeto 15. rujna 2015.)

Važan korak prema zajedničkoj strategiji unutarnje sigurnosti Europske unije bio je Stockholmski program donijet 2009. godine za razdoblje 2010.-2014. Njime je Europsko vijeće nastojalo operacionalizirati odredbe Lisabonskog sporazuma (Bilandžić, 2012, 59). Glavni prioritet „Stockholmskog programa – otvorena i sigurna Europa, koja služi građanima, i koja ih štiti“ je izgradnja otvorene i sigurne Europe koja služi i štiti građane.

„Program posebno poziva države članice da podupiru i poboljšavaju preventivne mjere za sprječavanje kriminaliteta. Ističe se ključno multidisciplinarno sudjelovanje i vladinih i nevlainih organizacija, tijela i agencija, a također i suradnja s privatnim sektorom.“ (Horjan i Šuperina, 2012, 81; prema Anželj, 2011, 9)

Strategiju unutarnje sigurnosti Europske unije usvojilo je Vijeće Europske unije na susretu održanom 25.-26. veljače 2010. godine, a potvrdilo Europsko vijeće dva tjedna kasnije. (Bilandžić, 2012:59) Strategijom se po prvi puta uspostavlja koncept unutarnje sigurnosti koji uključuje brojne službe, resore u državama članicama i institucijama. Radi se o uspostavi Europskog sigurnosnog modela.

Izazovi s kojima se model suočava su: zaštita prava i sloboda građana, poboljšanje suradnje i solidarnosti država članica, poklanjanje pažnje rješavanju uzroka nesigurnosti, a ne samo posljedicama, stavljanje prioriteta na prevenciju i anticipaciju budućih događaja vezano za sigurnosne izazove i prijetnje, uključivanje svih sektora (politički, gospodarski, socijalni, itd.) u aktivnosti zaštite javnosti/civila, komuniciranje sigurnosne politike prema građanima te, priznavanje međuovisnosti unutarnje i vanjske sigurnosti u ustanovljenju pristupa „globalne sigurnosti“ u trećim zemljama (Bilandžić, 2012).

Europska komisija je u studenom 2010. godine donijela akcijski plan za provedbu Strategije unutarnje sigurnosti Europske unije – *„Pet koraka prema sigurnijoj Europi“.* Plan između ostaloga sadrži pet strateških ciljeva za ostvarenje unutarnje sigurnosti Europske unije. Polazi od dva temeljna stajališta: prvo da se uloga Europske unije na području unutarnje sigurnosti temelji na definiranju zajedničkih politika, uspostavi zakonodavstva te na praktičnoj suradnji u policijsko-pravosudnim poslovima, upravljanju nadzorom granica i upravljanju kriznim situacijama, dok drugo stajalište ističe kako se unutarnja sigurnost ne može promatrati izolirano. Stoga je posebno važno uspostaviti koherentnost i komplementarnost između unutarnjih i vanjskih dimenzija sigurnosti.

Strateški ciljevi su: uništenje međunarodnih kriminalnih mreža, prevencija terorizma s naglaskom na sprječavanju radikalizacije i novačenja članova terorističkih organizacija, povećanje stupnja sigurnosti građana i poslovanja u kibernetičkom prostoru, jačanje sigurnosti kroz upravljanje nadzorom vanjskih granica Europske unije te, povećanje otpornosti na krize i katastrofe.

Akcijskim planom su određena i tijela te agencije Europske unije koje su, uz države članice, odgovorne za operativnu provedbu strategije unutarnje sigurnosti Europske unije: Europska komisija, Europska policijska akademija – CEPOL, Europska agencija za mrežnu i informacijsku sigurnost – ENISA, Centar za analizu i pomorske operacije – droge – MAOC-N, Koordinacijski centar za zapljenu droge – na Mediteranu – CECLAD-M, Europski ured za podršku azilu – EASO, Visoki predstavnik Europske unije za vanjske poslove i sigurnosnu

politiku, Europski policijski ured – EUROPOL, Jedinica Europske unije za pravosudnu suradnju – EUROJUST i Europska agencija za upravljanje operativnom suradnjom na vanjskim granicama – FRONTEX. Ovo je, dakle, institucionalni okvir djelovanja Unije na planu unutarnje sigurnosti.

Završno izvješće o provedbi Strategije unutarnje sigurnosti Europske unije 2010.-2014[542] ocjenjuje kako je u okviru svih pet strateških ciljeva ostvaren značajan napredak.

Važan korak predstavlja Europski program za sigurnost,[543] kojeg je Komisija donijela 28. 4. 2015., kojim je utvrdila strategiju Unije za rješavanje sigurnosnih prijetnji tijekom razdoblja 2015. - 2020. Ističe se da je Europski program sigurnosti zajednički program Unije i država članica. Programom se želi potaknuti bolja razmjena informacija, povećati operativna suradnja i uzajamno povjerenje te osigurati da se na unutarnjim i vanjskim dimenzijama sigurnosti radi zajedno.

3. OBILJEŽJA MIGRACIJSKE KRIZE 2015./2016. GODINE – UZROCI I TIJEK

Prema procjenama UNHCR-a i IOM-a[544] u 2015. godini do 21. prosinca u Europu je od progona, sukoba i siromaštva prebjeglo milijun osoba. Statistike UNHCR-a govore da je otprilike 972 500 osoba prešlo Sredozemno more (do 21.1.2016. godine ta se brojka popela na preko 1 080 000 osoba).[545] Uz to, IOM procjenjuje da je više od 34.000 osoba prešlo iz Turske u Bugarsku i Grčku kopnenim putem.[546] Prema podacima UNHCR-a najviše osoba dolazi iz Sirije, Afganistana i Iraka (vidi sliku 3.), dakle iz područja zahvaćenih ratnim sukobima. Činjenica je to koja upućuje na zaključak kako je trenutna migracijska kriza izbjeglička kriza. Jedan manji dio osoba uključenih u migracijske tokove su migranti – osobe koje napuštaju svoje države iz drugih (ekonomskih, obrazovnih, obiteljskih) motiva. Iz tog se razloga, umjesto u javnosti uvriježenog termina „migrantska“, u ovom radu koristi sveobuhvatniji izraz „migracijska“ kriza. Dakako, kriza je prije svega humanitarna i kao takva je promatrana u sigurnosnom kontekstu.

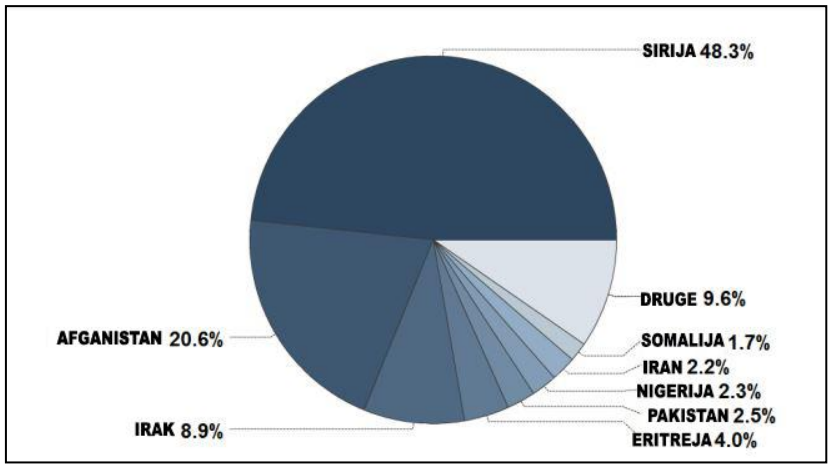
[542] Završno izvješće o provedbi Strategije unutarnje sigurnosti EU-a 2010. – 2014. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2014)0365_/com_com(2014)0365_hr.pdf (preuzeto 15. rujna 2015.)

[543] Europski program za sigurnost http://data.consilium.europa.eu/doc/document/ST-8293-2015-INIT/hr/pdf (preuzeto 22. rujna 2015.)

[544] UNHCR – UN-ova Agencija za izbjeglice, IOM – Međunarodna organizacija za migracije

[545] UNHCR, Mixed Migration Flows in the Mediterranean and Beyond, http://data.unhcr.org/mediterranean/regional.php, (preuzeto 15. veljače 2016.)

[546] UNHCR u Republici Hrvatskoj, Zajednička izjava za medije UNHCR-a i IOM-a Milijun izbjeglica i migranata u bijegu prema Europi u 2015. godini, http://www.unhcr.hr/component/content/article/165-unhcr/news-and-views/news/277-zajednicka-izjava-za-medije-unhcr-a-i-iom-a-milijun-izbjeglica-i-migranata-u-bijegu-prema-europi-u-2015-godini

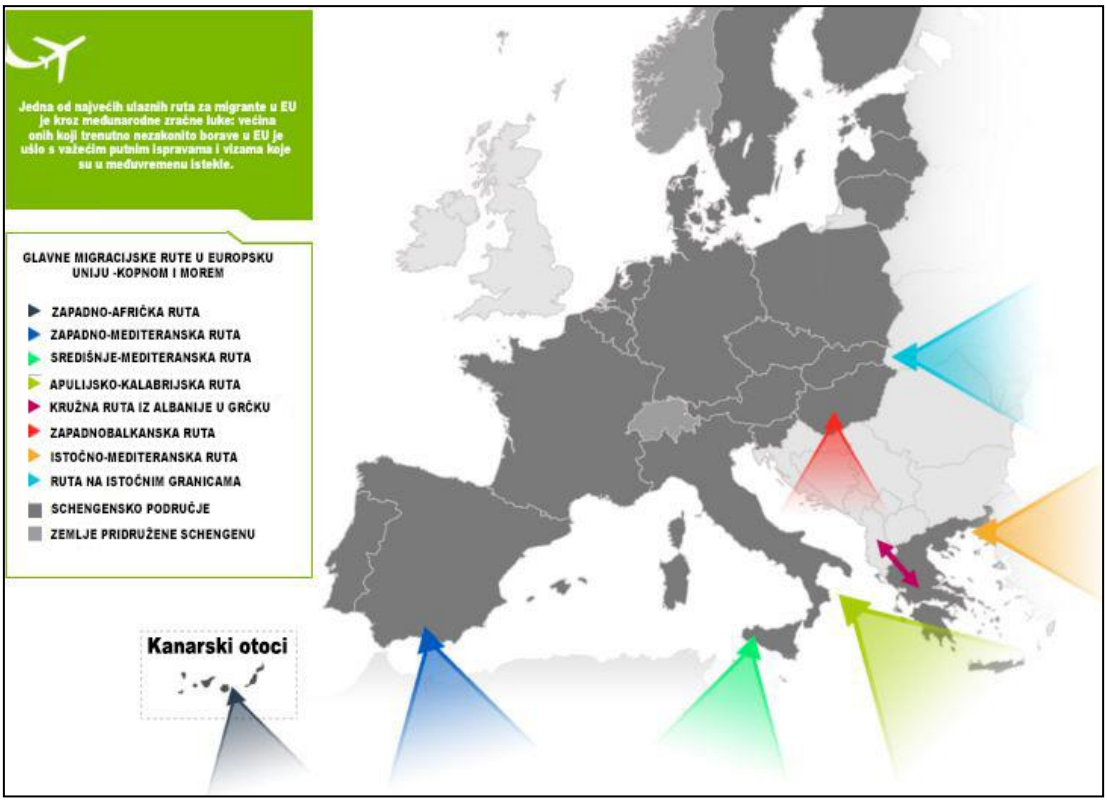


Slika 3. - Migranti i izbjeglice kumulativno pristigli u Europu - po nacionalnostima (UNHCR, Mixed migration flows in the Mediterranean and beyond, 15. veljače 2016., url)

U odnosu na 2014. u 2015. godini broj izbjeglica i migranata koji su nezakonito ušli u Europsku uniju morem i kopnom povećao se s 283.532 na preko već spomenutih 1.080.000.[547] Pitanje koje se nameće je zašto je do tako drastičnog povećanja priljeva ljudi došlo tek u 2015. godini? Prema pisanju The Washingnton Posta[548] za to postoji čak osam razloga. Prvi i najvažniji je rat u Siriji. Ljudi bježe i od ratnih sukoba u Iraku, Afganistanu, Somaliji i Nigeru. Drugo, nakon što je makedonska vlada u lipnju 2015. godine odobrila 72 satnu privremenu vizu za sve izbjeglice i migrante kako bi mogli koristiti legalna sredstva prijevoza kroz Makedoniju, čime je željela smanjiti pritisak sa svojih službi, istočnomediteranska (egejska) ruta je postala mnogo poželjnija. Ruta iz Turske u Grčku je daleko kraća i time manje opasna od do tada preferabilnije srednjemediteranske rute iz Libije u Italiju (vidi sliku 4.).

[547] FRONTEX, Annual Risk Analysis, http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2015.pdf#page=59 (preuzeto 15. veljače 2016.)

[548] The Washington Post, 8 reasons Europe's refugee crisis is happening now, autorice Liz Sly, od 18. rujna 2015., https://www.washingtonpost.com/news/worldviews/wp/2015/09/18/8-reasons-why-europes-refugee-crisis-is-happening-now/ (preuzeto 15. veljače 2016.)

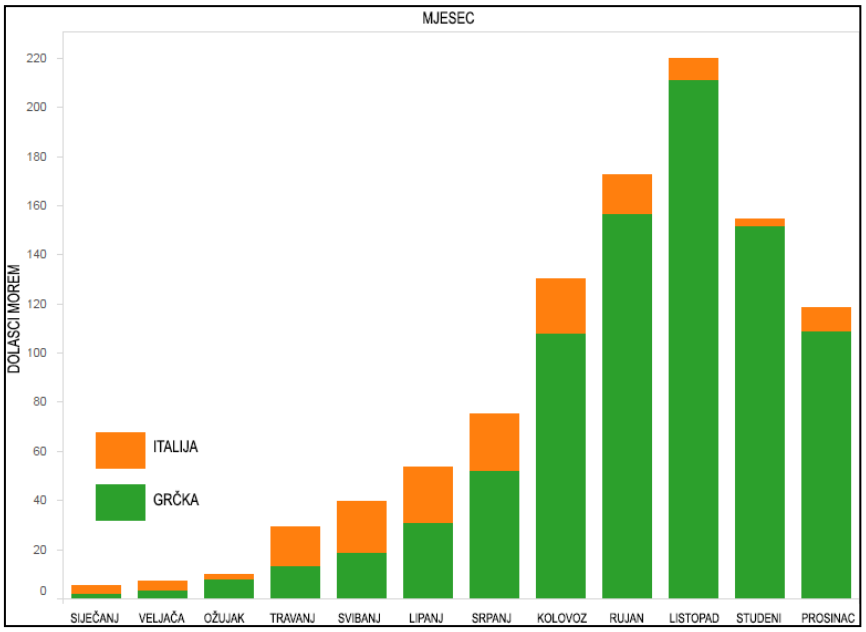


Slika 4. - Glavne migracijske rute u Europsku uniju - kopnom i morem (Frontex, Migratory routes map, 15. veljače 2016., url)

Plovidba od Turske do Grčke traje oko sat vremena, a može trajati i samo 20 minuta. Cijena koju izbjeglice i migranti plaćaju krijumčarima pala je s pet do šest na dvije do tri tisuće dolara. Povoljne meteorološke prilike također su utjecale na veliki priljev ljudi. Objava njemačke kancelarke Angele Merkel da će Njemačka pružiti privremeni boravak svim izbjeglicama koje stignu u Njemačku ohrabrila je mnoge na putovanje. Iračani su se pridružili egzodusu u većem broju. Namjera vlade Bashara al-Assada da mobilizira rezerviste nagnala je mnoge muškarce mlađe od 30 godina (one koji su u zadnjih 10 godina završili obavezni vojni rok) na bijeg u Europu. S druge strane sirijska vlada je olakšala ishođenje putovnica, kako u Siriji tako i u diplomatskim predstavništvima u inozemstvu, a vojnu obvezu je moguće izbjeći i plaćanjem naknade od 300 dolara. Velik broj muškaraca dolazi iz područja pod nadzorom sirijske vlade. Time su potvrđene sumnje mnogih[549] da sirijski režim namjerno potiče izbjeglički val u susjedne zemlje i Europu kako bi ispraznio zemlju od potencijalnih protivnika. Posljednje, prije masovnog priljeva ljudi u Europu, četiri milijuna[550] Sirijaca je već izbjeglo iz Sirije, pretežno u Tursku, Jordan i Libanon. U tim zemljama nisu imali pravo na rad, a većina njihove djece nije se školovala. Mnogi od izbjeglica koji su krenuli prema Europi, a već su živjeli kao izbjeglice u spomenutim državama, izjavili su kako im je obrazovanje njihove djece bio glavni razlog zašto su krenuli na put.

[549] Članak prenosi izjavu Emilea Hokayema, višeg suradnika Međunarodnog instituta za sigurnosne studije u Londonu:"Humanitarna katastrofa kojoj svjedočimo je posljedica Assadove strategije preživljavanja. Assad je odlučio prebaciti teret bavljenja onima koji su protiv njega na druge"

[550] Prema posljednjim procjenama UNHCR-a 4 715 695, Izvor: UNHCR, Syria Regional Refugee Response Inter-agency Information Sharing Portal, http://data.unhcr.org/syrianrefugees/regional.php# (preuzeto 16. veljače 2016.)



Slika 5. – Dolasci izbjeglica i migranata morem u Grčku i Italiju od siječnja do prosinca 2015. Prema podacima UNHCR-a (Wikipedia, European Migrant Crisis, 16. veljače 2016., url)

Sukladno Dublinskoj uredbi[551] tražitelj azila mora zatražiti azil u državi u kojoj je prvo stupio na tlo Europske unije i ako je prešao preko državne granice u drugu državu nakon što je daktiloskopiran, može biti vraćen u prethodnu državu. Pritisak izbjegličkog vala u 2015. godini rezultirao je neregistriranjem velike većine izbjeglica i migranata koji su iz Grčke i Italije nastavili svoj put prema zemljama Zapadne Europe. To je prisililo pojedine države na suspenziju Dublinske uredbe. Mađarska je prestala prihvaćati natrag izbjeglice koje su podnijele zahtjev za azil u Mađarskoj i poslije prešle u druge države.[552] Njemačka je odlučila sama procesuirati zahtjeve sirijskih izbjeglica. Češka je odlučila dozvoliti izbjeglicama da zatraže azil u Češkoj ili da nastave svoje putovanje prema zemljama zapadne Europe.[553] Mađarska je kako bi zaustavila nekontrolirani priljev ljudi koji ilegalno ulaze u zemlju, od lipnja 2015. godine izgradila više od 210 kilometara žičane ograde duž granice sa Srbijom i Hrvatskom. Slovenija je učinila isto na granici s Hrvatskom.[554] Austrija je također postavila nekoliko kilometara ograde na granici sa Slovenijom. Nekoliko zemalja (Danska, Norveška, Njemačka, Švedska, Austrija, Francuska) je uvelo privremene granične kontrole unutar schengenskog područja. Funkcioniranje zajedničkog sustava azila i bez graničnog schengenskog područja je dovedeno u pitanje.

[551] Službeni list Europske unije, Uredba (EU) br. 604/2013 Europskog Parlamenta i Vijeća, http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32013R0604&from=EN (preuzeto 20. veljače 2016.)
[552] Reuters, Defying EU, Hungary suspends rules on asylum seekers, http://uk.reuters.com/article/uk-europe-migrants-austria-hungary-idUKKBN0P31ZB20150623 (preuzeto 20. veljače 2016.)
[553] Prague Post, Change in Czech refugee policy, http://www.praguepost.com/eu-news/49584-change-in-czech-refugee-policy (preuzeto 20. veljače 2016.)
[554] Iako pravom Europske unije nije izričito zabranjeno postaviti ogradu na mjestu koje je i dalje vanjska schengenska granica, Europska komisija u svojem Osmom polugodišnjem izvješću o funkcioniranju schengenskog područja napominje da takva izgradnja nije u skladu s ciljem budućeg pristupanja Hrvatske schengenskom prostoru.

Prema procjeni Agencije za ekonomsko planiranje Francuske vlade, France Stratégie, ponovnim uvođenjem kontrola na državnim granicama unutar Schengenskog prostora Europska unija bi izgubila oko 100 milijardi eura. Dugoročno gledano, trgovinska razmjena bi pala za 10 do 20%. Procjena ne uključuje pad mobilnosti na tržištu rada i pad stranih investicija.[555]

4. POLITIČKO-SIGURNOSNI MEHANIZIMI EUROPSKE UNIJE ZA SUOČAVANJE S MIGRACIJSKOM KRIZOM

Europska komisija je dana 13.5.2015. godine predstavila Europski migracijski program[556] u kojem se iznose hitne mjere koje će se poduzeti u cilju rješavanja krizne situacije u Sredozemlju, kao i koraci koji će se poduzeti idućih godina radi boljeg upravljanja svim aspektima migracija. Program se temelji na četiri stupa boljeg upravljanja migracijama: Smanjivanje motivacije za nezakonitu migraciju**,** Upravljanje granicama – spašavanje života i osiguravanje vanjskih granica, Dužnost Europe da pruži zaštitu: čvrsta zajednička politika azila te Nova politika o zakonitim migracijama.

Europsko vijeće je 23.4.2015. godine, donijelo Izjavu kojom su se države članice obvezale na poduzimanje hitnih mjera u cilju spašavanja života i intenziviranja nastojanja Europske unije u području migracija. Dana 29.4.2015. godine uslijedila je Rezolucija Europskog parlamenta. U sklopu programa naknadno su donijeta i tri provedbena paketa. Dana 10.2.2016. godine Europska komisija je donijela Priopćenje prema Europskom parlamentu i Vijeću Europske unije o stanju stvari u provedbi prioritetnih mjera u sklopu Europskog migracijskog programa.[557]

4.1.Smanjivanje motivacije za nezakonitu migraciju

Hitne mjere koje program predviđa u ovom stupu su rad na mogućoj operaciji zajedničke sigurnosne i obrambene politike u Sredozemlju u cilju razbijanja mreža trgovaca ljudima i suzbijanja krijumčarenja ljudima u skladu s međunarodnim pravom. Slijedom toga je Odlukom Vijeća Europske Unije od dana 22.6.2015. godine pokrenuta vojna operacija Europske unije EUNAFOR MED[558] u južnom srednjem Mediteranu.

Prema Priopćenju Europske komisije diplomatski napori za rješavanje kriza poput Sirijske i Libijske i u borbi protiv Daesha[559] usmjereni su na uzroke migracijskih tokova i na stvaranje stabilnog okruženja u koje se izbjeglice mogu vratiti. Navodi se da ti napori moraju biti

---

[555] Business Insider UK, The European economy will take a €100 billion hit if it re-establishes permanent border controls, http://uk.businessinsider.com/france-strategie-schengen-area-gdp-significantly-affected-by-eu-immigration-border-controls-2016-2 (preuzeto 20. veljače 2016.)

[556] Europska komisija - Priopćenje za tisak, Bolje upravljanje svim aspektima migracija: Europski migracijski program, http://europa.eu/rapid/press-release_IP-15-4956_hr.htm (preuzeto 18. veljače 2016)

[557] European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the State of Play of Implementation of the Priority Actions under the European Agenda on Migration, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-migration/proposal-implementation-package/docs/managing_the_refugee_crisis_state_of_play_20160210_en.pdf (preuzeto 16. veljače 2016.)

[558] European union External Action, EUNAVFOR MED operation SOPHIA, http://eeas.europa.eu/csdp/missions-and-operations/eunavfor-med/index_en.htm (preuzeto 20. veljače 2016.)

[559] Daesh – tzv. „Islamska država“

globalni. U slučaju Libije, Europska unija pruža političku, financijsku i logističku potporu naporima Ujedinjenih naroda u okončavanju političke i sigurnosne krize.

Europska unija je igrala i igra ključnu ulogu u osnivanju i radu Međunarodne grupe za podršku Siriji.[560]

Unija je u 2015. godini iz svojeg proračuna izdvojila više od 400 milijuna eura za humanitarnu pomoć Siriji i susjednim zemljama koje su prihvatile izbjeglice (Libanon, Tursku, Jordan i Irak). To je dio ukupne pomoći Europske unije od preko 5 milijardi eura za humanitarnu pomoć, razvoj i stabilizaciju.

Regionalni fond Europske unije za odgovor na Sirijsku krizu je do sada prikupio 654 milijuna eura pomoći od Europske unije i država članica. On osigurava pomoć za 1.5 milijuna sirijskih izbjeglica u Libanonu, Turskoj, Jordanu i Iraku pružajući obrazovanje i zaštitu djece, bolji pristup zdravstvenoj zaštiti, poboljšane uvjete opskrbe vodom i poboljšanu infrakstruturu otpadnih voda, kao i podršku gospodarskim prilikama i socijalnoj uključenosti.

Na samitu u Valetti, u studenom 2015., europski i afrički šefovi država i vlada susreli su se s ciljem jačanja suradnje na području migracija između zemalja porijekla, tranzita i odredišta. Naglašena je potreba zaustavljanja ilegalne migracije prema Europi i njeno usmjeravanje u razvojnu suradnju. Europska unija je osnovala Zakladu za hitne slučajeve u Africi vrijednu blizu 1.9 milijardi eura.

Zajednički akcijski plan Europske unije i Turske je veliki korak naprijed u suradnji u pružanju pomoći Sirijcima pod privremenom zaštitom u Turskoj. Europska unija i države članice će pojačati suradnju s Turskom i znatno povečati svoj politički i financijski angažman. Glavni doprinos Europske unije koji odražava duh dijeljenja odgovornosti je novi objekt za izbjeglice u Turskoj postavljen od strane Komisije 24.11.2015. godine koji će koštati 3 milijarde eura u 2016. i 2017. godini.

4.2.Upravljanje granicama – spašavanje života i osiguranje vanjskih granica

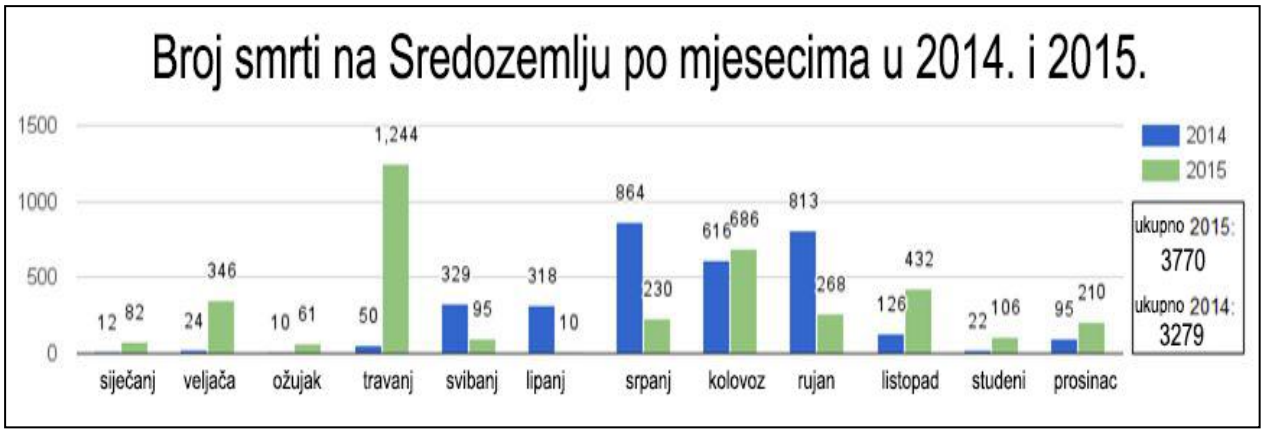
U ovom stupu kao hitne mjere se navode: utrostručavanje kapaciteta i sredstava za zajedničke operacije Frontexa Triton i Poseidon i dosad prva mobilizacija sustava za izvanredne situacije iz članka 78. Stavka 3. Ugovora o funkcioniranju europske unije[561] kako bi se pomoglo državama članicama koje se suočavaju s iznenadnim priljevom migranata. U 2014. Na sredozemlju je u kalvarijama brodova zabilježeno 3279 smrti izbjeglica i migranata, a ta brojka se popela na 3770 u 2015. godini. (vidi sliku 6.) U 2016. godini su do 16. Veljače od 82.636 dolazaka, zabilježene 403 smrtno stradale ili nestale osobe.[562]

---

[560] International Syria Support Group (ISSG) sastoji se od 20 učesnika: Arapske lige, Kine, Egipta, Europske unije, Francuske, Njemačke, Irana, Iraka, Italije, Jordana, Libanona, Omana, Katara, Rusije, Saudijske Arabije, Turske, Ujedinjenih Arapskih Emirata, Velike Britanije , Ujedinjenih naroda i Sjedinjenih Američkih Država

[561] U slučaju da se jedna ili više država članica naže u kriznoj situaciji zbog iznenadnog priljeva državljana trećih zemalja, Vijeće, na prijedlog Komisije, može usvojiti privremene mjere u korist dotične države članice ili dotičnih država članica. Vijeće odlučuje nakon savjetovanja s Europskim parlamentom.

[562] UNHCR, Refugees/Migrants Emergency Response – Mediterranean, http://data.unhcr.org/mediterranean/regional.php (preuzeto 16. veljače 2016.)



Slika 6. - Broj smrti izbjeglica i migranata na Sredozemlju po mjesecima u 2014. i 2015. godini. (Missing Migrants Project, 16. veljače 2016., url)

Spašavanje na moru je bio prvi prioritet Europske unije. Tijekom 2015. godine Frontexovim Združenim operacijama Triton i Poseidon spašeno je preko 250.000 ljudi.

Operacija Triton je pomorska operacija osiguranja granice koju provodi Frontex i koja je pod talijanskom kontrolom započela 1.11.2014. godine. Operacija je poduzeta nakon što je Italija završila operaciju Mare Nostrum koja je postala preskupa za jednu državu i nakon što druge države članice nisu ponudile traženu pomoć. U operaciji dobrovoljno sudjeluje 26 drugih europskih država (i članica i nečlanica Europske unije među kojima i Republika Hrvatska). Nakon Izjave Europskog vijeća od 23.4.2015. financijska sredstva za operaciju su utrostručena.

Združena operacija Poseidon započela je još 2006. godine nakon što je Grčka od Frontexa zatražila nadzor svoje pomorske i kopnene granice s Turskom na Mediteranu i Egejskom moru. Operacija je bila podijeljena u dva dijela: pomorsku te kopnenu. Postala je trajna 2011. godine i 2015. godine je zamijenjena operacijom Poseidon Rapid Intervention također pod nadzorom Frontexa, sada s većim budžetom i većim brojem plovila i službenika koji pomažu kod identifikacije i daktiloskopiranja izbjeglica i migranata, zajedno s prevoditeljima i stručnjacima za krivotvorene dokumente.[563]

U trećem provedbenom paketu od dana 15.12.2015. godine Europska komisija predlaže uspostavljanje Europske granične i obalne straže kako bi se osiguralo čvrsto i zajedničko upravljanje vanjskim granicama. Europska granična i obalna straža[564] povezat će Europsku agenciju za graničnu i obalnu stražu, koja je nastala iz Frontexa, s tijelima država članica nadležnima za upravljanje granicama, koja će se nastaviti baviti svakodnevnim upravljanjem vanjskim granicama. Osnovat će se centar za praćenje i analizu rizika radi praćenja migracijskih tokova prema Europskoj uniji i unutar nje te radi provođenja analize rizika i obveznih procjena osjetljivosti za utvrđivanje i uklanjanje slabih točaka. Časnici za

[563] Frontex, Frontex launches rapid operational assistance in Greece, http://frontex.europa.eu/news/frontex-launches-rapid-operational-assistance-in-greece-u3rqPy (preuzeto 19. veljače 2016.)

[564] Europska komisija - Priopćenje za tisak, Europska granična i obalna straža za zaštitu europskih vanjskih granica, http://europa.eu/rapid/press-release_IP-15-6327_hr.htm (preuzeto 20. veljače 2016.)

vezu uputit će se u države članice kako bi bili na terenu na mjestima gdje su granice ugrožene. Agencija će moći procjenjivati operativne kapacitete, tehničku opremu i resurse država članica za suočavanje s izazovima na njihovim vanjskim granicama i tražiti od država članica da poduzmu mjere za rješavanje situacije unutar zadanih rokova u slučaju ugroženosti. Države članice mogu tražiti zajedničke operacije i brze granične intervencije te raspoređivanje timova Europske granične i obalne straže u tu svrhu. Komisija će moći donijeti provedbenu odluku kojom se utvrđuje da je zbog situacije na određenom dijelu vanjskih granica potrebno hitno djelovanje na europskoj razini.Time će se omogućiti Agenciji da se uključi i rasporedi timove Europske granične i obalne straže kako bi osigurala djelovanje na terenu kad država članica ne može ili ne želi poduzeti potrebne mjere.

Donijet je i prijedlog uredbe o uspostavi Agencije Zajednice za kontrolu ribarstva (EFCA). EFCA je trenutno zadužena za sudjelovanje u borbi protiv nezakonitog, nereguliranog i neprijavljenog ribolova. Njezino iskustvo na međunarodnoj razini ključno je za kapacitet europske obalne straže i nadzor granica s obzirom na to da je nezakoniti, neregulirani i neprijavljeni ribolov često povezan s drugim kaznenim aktivnostima na moru. Nedavno su EFCA i Turska razmijenile inspektore na Sredozemnom moru, a EFCA redovito organizira i seminare za osposobljavanje na kojima se okupljaju inspektori Europske unije i zemalja izvan nje. EFCA će moći bolje poduprijeti razmjenu podataka koje je prikupila i koje uključuju sustave za praćenje plovila (VMS) i elektroničke sustave za prijenos podataka (ERS). Uredbom je obuhvaćeno pružanje usluga nadzora i komunikacije na temelju najsuvremenije tehnologije, uključujući svemirsku i zemaljsku infrastrukturu te senzore ugrađene na bilo koju vrstu platforme. To će Agenciji omogućiti institucionaliziranje suradnje nacionalnih, europskih i međunarodnih partnera.

Predlaže se uspostava Europske agencije za pomorsku sigurnost. Cilj je ove poboljšati međusektorsku suradnju Europske granične i obalne straže, Europske agencije za pomorsku sigurnost, Europske agencije za kontrolu ribarstva i nadležnih institucijama u državama članicama.

Komisija predlaže da se uvedu i sustavne provjere u odgovarajućim bazama podataka svih osoba koje ulaze ili izlaze iz schengenskog prostora, tj. ciljanu prilagodbu Zakonika o schengenskim granicama kako bi se uvele obvezne sustavne provjere građana Europske unije na vanjskim kopnenim, morskim i zračnim granicama. Pojava stranih terorističkih boraca i dalje predstavlja velik razlog za zabrinutost. Broj državljana Europske unije koji putuju u Siriju i Irak kako bi poduprli terorističke skupine stalno raste. Procjenjuje se da je do sada 5 000 građana Europske unije otišlo u područja sukoba i najvjerojatnije se pridružilo snagama ISIS-a. Komisija je u lipnju 2015. utvrdila prvi skup zajedničkih pokazatelja rizika za strane terorističke borce, a njima će se koristiti službenici graničnog nadzora prilikom provođenja kontrola. Taj se popis temelji na trendovima u putovanjima, modelima i posebnim značajkama koje se pripisuju tim osobama. Sastavljanju popisa doprinosile su države članice, Europska služba za vanjsko djelovanje, Europol i Frontex.[565] Uvođenjem sustava Eurosur stvoren je dobar model za daljnji razvoj i sva civilna i vojna tijela odgovorna za nadzor

[565] Europska komisija, Komunikacija Komisije Europskom parlamentu i Vijeću, Osmo polugodišnje izvješće o funkcioniranju schengenskog područja 1. svibnja - 10. prosinca 2015., https://ec.europa.eu/transparency/regdoc/rep/1/2015/HR/1-2015-675-HR-F1-1.PDF (preuzeto 20. veljače 2016.)

pomorskih granica trebala bi se njime služiti. Obvezne provjere uvest će se s pomoću baza podataka kao što su schengenski informacijski sustav, Interpolova baza podataka o ukradenim i izgubljenim ispravama te odgovarajući nacionalni sustavi kako bi se provjerilo da osobe koje ulaze u Uniju nisu prijetnja javnom redu i unutarnjoj sigurnosti. U prijedlogu se naglašava i potreba da se provjeravaju biometrijski identifikatori u putovnicama građana Europske unije u slučaju sumnje u vjerodostojnost putovnice ili legitimitet vlasnika. Učinkovitije upravljanje granicama podrazumijeva i bolju uporabu mogućnosti koje nude informatički sustavi i tehnologije. Europska unija ima tri velika informatička sustava koji se koriste za postupak obrade zahtjeva za azil (Eurodac), za postupak obrade zahtjeva za izdavanje vize (Vizni informacijski sustav) i za razmjenu informacija o osobama ili predmetima za koje je nadležno tijelo izdalo upozorenje (Schengenski informacijski sustav). Provjere će sada biti obvezne i pri izlasku iz Europske unije. Europska komisija je u veljači 2013. predložila paket „Smart Borders" te provela odgovarajući pilot projekt koji će se iskoristiti za studiju izvedivosti. Zaključak je da je prijedlog dobar i provediv. Početkom 2016. Komisija namjerava revidirati zakonodavni prijedlog o pametnim granicama te će ga u ožujku 2016. predstaviti državama članicama. Cilj je poboljšati upravljanje granicama i pridonijeti borbi protiv ilegalne migracije te olakšati prelazak granica putnicima koji se unaprijed registriraju te čestim putnicima. Komisija će u 2016. utvrditi standard Unije za upravljanje granicama kako bi se obuhvatili svi aspekti upravljanja vanjskim granicama Unije. Napori će se uložiti i u poticanje sigurnijih granica, ali i jačanje kapaciteta zemalja Sjeverne Afrike za intervencije i spašavanje migranata u opasnosti.

Također je predložena uspostava Europske putne isprave za povrat državljana trećih država u nezakonitom boravku. Cilj je uspostaviti Europsku putnu ispravu za povratak državljana trećih država koji ne ispunjavaju uvjete za ostanak te osigurati jednoobraznu ispravu naprednih tehničkih i sigurnosnih karakteristika.

Europska komisija je u prvom i drugom provedbenom paketu predložila, a Vijeće se složilo s uspostavljanjem programa premještanja ukupno 160.000 osoba iz Italije i Grčke. Države članice primit će 6.000 eura za svaku premještenu osobu u njihovo državno područje.

4.3.Pružanje zaštite izbjeglicama i migrantima: čvrsta zajednička politika azila

Europski migracijski program inzistira na cjelovitoj i dosljednoj provedbi zajedničkog Europskog sustava azila. Navodi se da svaki zahtjev za azil mora biti obrađen te da je jedna od slabosti koja se ispostavila u dosadašnjoj politici bila nedostatak uzajamnog povjerenja među državama članicama. To je imalo izravan utjecaj na tražitelje azila koji su pokušavali dobiti azil tako što su tražili najpovoljnije uvjete u sustavu, ali i na javno mnijenje Europske unije gdje je vladao osjećaj da je sustav potpuno nepošten. Europski potporni ured za azil (EASO) će na razini Unije pružati potporu državama članicama osnivanjem posebne mreže nacionalnih dublinskih jedinica. Komisija će u 2016. godini napraviti evaluaciju Dublinskog sustava i pritom se koristiti i iskustvima stečenima u okviru mehanizama premještanja i preseljenja. Zahvaljujući tome lakše će se utvrditi postoji li potreba za revizijom pravnih parametara Dublina kako bi se postigla pravednija raspodjela podnositelja zahtjeva za azil.

Program je donio novi koncept „žarišnih točaka“, tzv. Hotspot u sklopu kojega će uz koordinaciju Europske komisije EASO, Frontex, Europol i Eurojust zajednički raditi na terenu u najizloženijim državama članicama u cilju brzog identificiranja i registriranja izbjeglica i migranata, njihovog daktiloskopiranja i koordiniranja povratka. Prema priopćenjima Europske komisije[566] Grčkoj je do 15.12.2015. godine ustrojeno pet žarišnih točaka opremljenih s 46 EURODAC uređaja za uzimanje otisaka prstiju i angažiranih 304 službenika Frontexa i 7 službenika EASO-a. Iskazana je potreba za još 30 EURODAC uređaja, 213 službenika Frontexa i 131 službenikom EASO-a. U Italiji je ustrojeno 6 žarišnih točaka s ukupno 8 EURODAC uređaja, 52 službenika Frontexa i 2 službenika EASO-a (još 17 na drugim lokacijama u Italiji), a iskazana je potreba za još 248 službenika Frontexa i 243 službenika EASO-a.

4.4.Nova politika o zakonitim migracijama

Očekuje se da će promjene u pogledu vještina koje se traže u Europskoj uniji u razdoblju od 2012. do 2025. pokazati nagli porast udjela radnih mjesta za visokokvalificirane radnike (za 23 %). U ključnim sektorima, kao što su znanost, tehnologija, inženjerstvo i zdravstvo, već je vidljiv manjak radne snage. Procjenjuje se da čak ni uz odlučno kratkoročno i dugoročno ulaganje napora Europska unija neće moći u potpunosti odgovoriti na potrebe tržišta rada. Stanovništvo Europske unije postaje sve starije, a gospodarstvo sve ovisnije o radnim mjestima za visokokvalificirane radnike. Ako ne bude migracije, radno sposobno stanovništvo Europske unije će se u sljedećem desetljeću smanjiti za 17,5 milijuna. Ovaj problem je prepoznat i u Završnom izvješće o provedbi Strategije unutarnje sigurnosti Europske unije 2010.-2014 kao jedan od budućih izazova. U dvije godine od stupanja na snagu Direktive o plavoj karti izdano je samo 16. 000 plavih karti, a od tog je ukupnog broja 13.000 izdala jedna država članica. Komisija će uspostaviti platformu za dijalog kako bi prikupila mišljenja poslodavaca, sindikata i drugih socijalnih partnera te ostvarila najveće moguće koristi od migracija za europsko gospodarstvo i same migrante. U sklopu modernizacije vizne politike Komisija je 2014. godine predložila reviziju Zakonika o vizama te uvođenje nove vrste viza: vize za privremeni boravak. Time bi Europska unija stekla fleksibilnije alate vizne politike kojima će se nastojati postići najveći mogući pozitivni gospodarski učinak od privlačenja većeg broja turističkih dolazaka te dolazaka radi osobnih ili poslovnih razloga uz smanjenje rizika od nezakonite migracije i sigurnosnih rizika.

Stav je kako uspješnost migracijske politike ovisi o učinkovitim integracijskim politikama.Ona je u primarnoj nadležnosti država članica. Europska unija može podupirati mjere nacionalnih vlada, tijela lokalne vlasti i civilnog društva koji sudjeluju u procesu poboljšanja integracije i jačanja uzajamnog povjerenja. Sredstva iz više europskih fondova su namijenjena za poboljšanje društvene uključenosti, što uključuje mjere za integraciju migranata uz osobiti naglasak na one koji traže azil, izbjeglice te djecu. Fondovi mogu podupirati ciljane inicijative za unapređenje jezičnih i profesionalnih vještina, promicanje

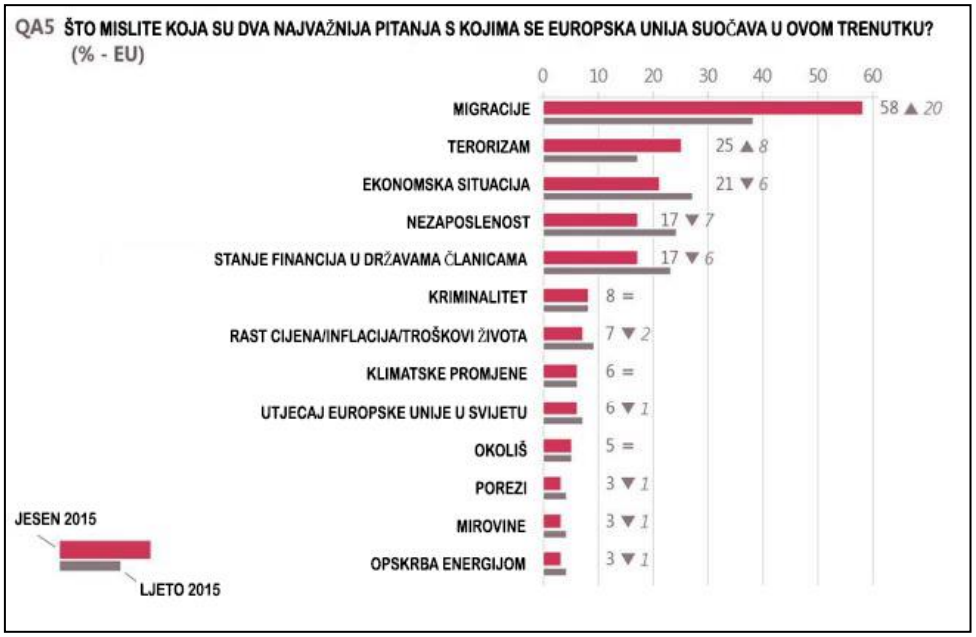
[566] Prilozi Komunikaciji Komisije Europskom parlamentu i Vijeću, Izvješća o napretku provedbe žarišnih točaka u Grčkoj i Italiji (dva odvojena dokumenta) COM(2015) 678 i COM(2015) 679 od dana 15.12.2015. godine https://ec.europa.eu/transparency/regdoc/rep/1/2015/HR/1-2015-679-HR-F1-1-ANNEX-1.PDF i https://ec.europa.eu/transparency/regdoc/rep/1/2015/HR/1-2015-678-HR-F1-1-ANNEX-1.PDF (preuzeto 20. veljače 2016)

pristupa tržištu rada i uključivog obrazovanja, razvijanje međukulturalne razmjene te promicanje kampanja za jačanje svijesti podjednako usmjerenih na lokalno stanovništvo i migrante. Važan dokument na tom polju je Rezolucija Europskog parlamenta od 16.1.2016. godine koja ističe kako je upravo bogatstvo kulturne raznolikosti u Europi obilježje europskog identiteta temeljenog na suživotu, toleranciji i uvažavanju različitosti.[567]

5. SEKURITIZACIJA MIGRACIJA

Kao što je to u uvodu naglašeno, važnu dimenziju stanja unutarnje sigurnosti Europske unije čini stav njezinih građana prema pojedinoj stvarnoj ili percipiranoj prijetnji., tj. subjektivni osjećaj sigurnosti pojedinca.

Eurobarometer istraživanje o migracijama 2015.[568] je provedeno u 28 država članica Europske unije i pet država kandidatkinja (Albaniji, Crnoj Gori, Makedoniji, Srbiji i Turskoj) te dijelu Cipra koji nije pod nadzorom vlade Republike Cipra, između 7. i 17.11.2015. godine pokazalo je kako su migracije pitanje oko kojega su građani Europske unije (na razini Unije) najviše zabrinuti i to 58% građana, s 20% porastom od ljeta 2015. Na drugom mjestu je terorizam. (vidi sliku 7.)

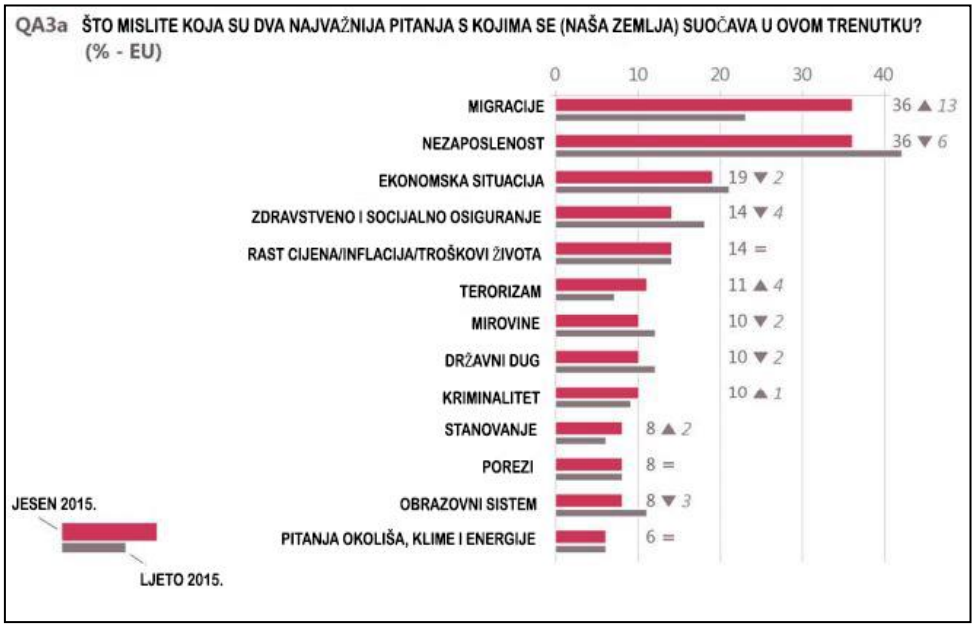


Slika 7. - Glavne zabrinutosti na razini Europske unije
(European Commision, Standard Eurobarometer 84, 20. veljače 2016., url)

[567] Rezolucija Europskog parlamenta od 19. siječnja 2016. o ulozi međukulturnog dijaloga, kulturne raznolikosti i obrazovanja u promicanju temeljnih vrijednosti EU-a (2015/2139(INI)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0005+0+DOC+XML+V0//HR (preuzeto 15. veljače 2016.)

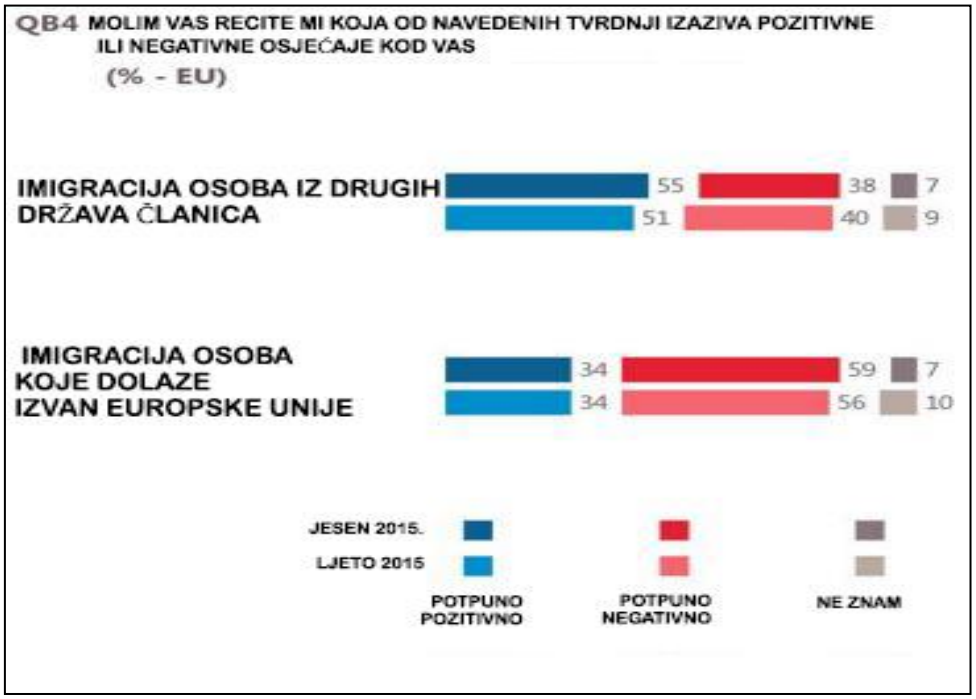
[568] European Commision,, Standard Eurobarometer 84, http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/Survey/getSurveyDetail/instruments/STANDARD/surveyKy/2098 (preuzeto 20. veljače 2016.)

Na razini pojedinih država, kao najveće pitanje s kojim se država ispitanika suočava, većina ispitanih je opet odgovorila da su to migracije (36%). Terorizam je ovdje na šestom mjestu (11%, slika 8).



Slika 8. - Glavne zabrinutosti na razini države ispitanika (European Commision, standard Eurobarometer 84, 20. veljače 2016., url)

Osjećaji stanovnika Europske unije prema osobama koje imigriraju u njihove zemlje se razlikuju ovisno o tome dolaze li oni iz drugih zemalja članica ili dolaze s prostora izvan Europske unije, tako da 55% ispitanih ima pozitivan stav prema prvima, no samo 34% njih ima pozitivan stav prema imigrantima koji dolaze izvan Europske unije. (vidi sliku 9.)



Slika 9. – Osjećaji ispitanika prema osobma koje imigriraju u njihovu zemlju (European Commision, standard Eurobarometer 84, 20. veljače 2016., url)

Postavlja se pitanje odakle potječu takvi negativni stavovi prema izbjeglicama i migrantima. Jesu li oni imanentni europskom društvu ili su fabricirani, potpomognuti medijskim i političkim kampanjama.

Prema Huysmansu (2000) u Europi je još od 1980-ih godina prisutan trend sekuritizacije migracija. Bogate države Zapadne Europe suočavaju se s mnoštvom izazova u svojim mehanizmima socijalne integracije i političkog legitimiteta. To uključuje ekonomsku i financijsku globalizaciju, rast siromaštva, srozavanje životnih uvjeta u gradovima, povratak rasističkih i ksenofobnih stranaka i pokreta, otuđivanje izbornog tijela od političke klase i porast multikulturalizma. U takvom je okruženju migracija sve više predstavljena kao opasnost za javni poredak, kulturni identitet i stabilnost domaćeg tržišta i tržišta rada. Ona je, dakle, sekuritizirana. Kao ključni element navodi tehnokratsko i politički proizvedeno prelijevanje ekonomskog projekta unutarnjeg tržišta (otvorenih granica) u unutarnje-sigurnosni projekt.

Prema Solomunu (2012), obrazac interpretacije nekog društvenog pitanja razvijen je na pravcu od nepolitiziranosti, preko politiziranosti do sekuritizacije.

Neko pitanje je nepolitizirano, ako nije dio javne rasprave i država se njime ne bavi. Razinu više označava politiziranost kada se s pitanjem postupa unutar nekog političkog sustava i dio je javnih politika te zahtijeva državnu odluku. Sigurnosno najznačajnija razina je sekuritiziranost određenog pitanja kada je ono označeno kao sigurnosni problem jer akteri sekuritizacije politizirano pitanje definiraju kao egzistencijalnu prijetnju referentnom objektu. (Solomun 2012; prema Emmers, 2010). Nadalje, ističe kako važnost dinamike svake sigurnosne kategorije određuje provoditelj sekuritizacije i referentni objekt.

Huysmans (2000) tvdi da je uvrštavanje politike azila i migracija u politički okvir koji definira i regulira sigurnosna pitanja prizašlo iz ukidanja kontrola na unutarnjim granicama, no da je angažman Europske unije još širi od toga. Prema njemu eksplicitno privilegiranje državljana država članica u odnosu na državljane trećih zemalja i općenito restriktivne regulacije u području migracija podržavaju širi proces delegitimacije prisutnosti imigranata, tražitelja azila i izbjeglica. Tako tvrdi da politike Europske unije, često indirektno, podržavaju izraze prosperitetnog šovinizma i ideje o kulturnoj homogenosti kao stabilizirajuće faktore. U suvremenom Europskom političkom kontekstu te politike omogućavaju prikazivanje migracija kao destabilizirajućeg ili opasnog izazova za zapadno-europska društva.

Pitanje koje proizlazi iz toga je kako se razvoj zajedničke migracijske politike uklapa u šire politike pripadanja koje je borba za kulturne, rasne i socio-ekonomske kriterije za distribuciju prava i dužnosti u zajednici.

U javnosti su bile vidljive kritike međunarodnih organizacija poput UNHCR-a, IOM-a i mnogih drugih na račun migracijske politike Europske unije u segmentu poštivanja ljudskih prava. Posebno su bile kritizirane push-back operacije pojedinih država kao što su Italija,

Grčka i Španjolska, no i Frontex.[569] Kritizirano je i financiranje prihvatnih centara u trećim zemljama, ulaganje ogromnih sredstava u operacije vraćanja, u jačanje nadzora granica Sve je to poslužilo kao argument za tvrdnje da Europska unija ne želi izbjeglice unutar svojih granica. U drugom dijelu javnosti za izbjeglice i migrante često se koristi naziv ilegalci i sl. Opisuje ih se kao nasilnike prema ženama, potencijalne teroriste, širitelje bolesti, iskorištavatelje beneficija itd[570]. Stvaranje ovakve medijske slike svakako ide u prilog tezama o sekuritizaciji izbjegličkog pitanja. Europska agencija za temeljna prava (FRA) navodi kako su u Austriji u porastu protesti krajnje desnih grupacija i zločina iz mržnje koji su i dalje na visokom nivou u Bugarskoj, Njemačkoj, Italiji i Švedskoj. Medijska kampanja mađarske vlade opisuje izbjeglice kao potencijalnu prijetnju nacionalnoj sigurnosti, a u nekim slučajevima su i prijavljena zlostavljanja izbjeglica od strane policije.[571]

6. ZAKLJUČAK

Dinamika i složenost zbivanja koja obilježavaju migracijsku krizu predstavljaju dosad možda najveći izazov konceptu unutarnje sigurnosti Europske unije. Realno, globalni uzroci ratnih kriza koje su dovele do najvećeg egzodusa ljudi prema Europi nakon drugog svjetskog rata u ograničenom su dosegu sigurnosnih politika Europske unije i predmet su jednog mnogo šireg geopolitičkog diskursa.

Civilizacijska je dužnost svake pojedine države, a tako i Europske unije kao nadnacionalne zajednice država pružiti zaštitu ljudima koji bježe od progona i stradanja.

U kontekstu migracijske krize, napori koje Europska unija poduzima u ostvarivanju funkcije unutarnje sigurnosti sastoje se od kreiranja sveobuhvatnih politika provedivih kroz operativno djelovanje institucija Europske unije i zemalja članica. One doista počivaju na širokom, multisektorskom pristupu i posvećene su inovacijama i novim tehnologijama. U okviru institucija i agencija Unije razvijeni su ljudski potencijali koji su svojim specijalističkim znanjima sposobni pružiti pomoć najugroženijim državama članicama. Brojni društveni faktori izvan sigurnosnog institucionalnog okvira pozvani su sudjelovati u tim politikama. To se odnosi kako na međunarodne organizacije, tako i na platforme civilnog društva, znanstveni, poslovni i industrijski sektor, lokalne zajednice i pojedince.

Uvažavajući kontekst njihovog nastanka, Europska unija nastoji odigrati ključnu ulogu i dati doprinos rješavanju uzroka nesigurnosti izvan svojih granica kroz diplomatski, humanitarni i stručni angažman u Africi i Aziji. Sinergija unutarnje i vanjske dimenzije sigurnosti vidljiva je i u akcijama spašavanja života izbjeglica i borbe protiv krijumčara na moru. Napori na tom polju su kadrovski i financijski umnogostručeni.

---

[569] European Parliament, Directorate General for External Policies, Policy Department, STUDY Migrants in the Mediterranean: Protecting human rights, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/535005/EXPO_STU%282015%29535005_EN.pdf (preuzeto 20. veljače 2016.)

[570] Xpressed an open journal, Hrvatskoj: Sekuritizacija izbjegličkog pitanja od strane političkih elita, http://www.x-pressed.org/?xpd_article=croatia-securitisation-of-the-refugee-issue-by-the-political-elites&lang=hr (preuzeto 20. veljače 2016.)

[571] FRA, Highlights: 1 January - 31 January 2016, http://fra.europa.eu/en/theme/asylum-migration-borders/overviews/january-2016 (preuzeto 20. veljače 2016)

Ipak, praksa je pokazala kako politike unutarnje sigurnosti nisu uvijek lako provedive u. U pružanju zaštite kroz institut azila, obujam i intenzitet operativnog zahvaćanja u problem često ovisi o dnevnopolitičkim *ad hoc* odlukama država članica. U bliskoj budućnosti nužno će biti preispitivanje postojećeg sustava jer sadašnji ne pruža adekvatnu zaštitu i predmet je mnogih kritika. Pojedinac, tj. osoba kojoj je potrebno pružiti zaštitu trebao bi biti primarni referentni objekt sigurnosti, no on je u ovoj fazi pomaknut prema zaštiti vanjskih granica, tj. prema državi i dalje Europskoj uniji, a oni najugroženiji počinju se doživljavati kao prijetnja. Ne dovodeći u pitanje nužnost zaštite vanjskih granica Unije legitimno je upitati se štiti li Europska unija izbjeglice ili se Europska unija štiti od izbjeglica?

Briga o stanju unutarnje sigurnosti na vlastitom teritoriju je u primarnoj nadležnosti države kao njenog neotuđivog suverenog prava. Nekontrolirani i masovni ilegalni prelasci granica ugroza su suverenosti države, pogotovo u subjektivnom smislu. Oni opravdano stvaraju osjećaj nesigurnosti među stanovništvom. Osjećaju nesigurnosti doprinosi i napuštanje dogovorenih politika i praksi uslijed nedovoljnih kapaciteta za njihovu provedbu. Time se također stvara slika o nemoći države. Države to dakako nisu spremne u potpunosti priznati. Razloge za odstupanje od dogovorenog sklone su pripisati odlukama drugih država, čime se stvara domino efekt neučinkovitosti. Angažman s razine Europske unije na poljima gdje države članice nisu u mogućnosti ili ne žele provesti svoje obveze često se doživljava kao diranje u suverenost. Sekuritizacija migracija kroz medije od strane dijela političke javnosti, čak i od vladajućih elita pojedinih država bitno doprinosi takvoj slici stanja. Napadi na izbjeglice i migrante kao i jačanje ekstremističkih desnih pokreta za sada ostaju u sjeni fabricirane prijetnje od migracija koja je u medijima neraskidivo povezana s nedavnim terorističkim napadima u Parizu i strahom od budućih napada. U tom smislu nužna je jasnija komunikacija o migracijskoj krizi od strane relevantnih aktera prema široj javnosti kroz ugledne masovne medije. Politika socijalne uključenosti i međukulturnog dijaloga bi dugoročno trebala pridonijeti zdravijem pogledu na problem i njegovom lakšem rješavanju, barem u onom dijelu koji se tiče uključivanja izbjeglica i migranata u europsko društvo.

Većina današnjih ugroza i mehanizama za suočavanje s njima bili su predviđeni u strateškim dokumentima Europske unije i prije izbijanja migracijske krize. Kriza je ipak intenzivirala njihov daljnji razvoj i mobilizirala veća financijska sredstva za njihovu primjenu. Ona je ukazala i na mane u sustavu, od sporosti donošenja političkih odluka, do njihove neadekvatnosti u praksi.

Migracijska kriza je u užem sigurnosnom smislu kriza sustava, a u širem kriza vrijednosti i zajedničkog europskog identiteta. Jedno je drugome potrebno i to uzajamno. Zajednička sigurnost se može graditi samo na zajedničkim vrijednostima, a te se vrijednosti mogu štititi jedino udruženo i solidarnom podjelom odgovornosti.

Pravi test za provjeru napretka tek dolazi. S povoljnijim meteorološkim prilikama u lipnju očekuje se ponovni porast broja dolazaka izbjeglica i migranata. Europska unija je imala godinu dana da se pripremi.

LITERATURA

Knjige i stručni članci

Bilandžić, M., (2012). Prema strategiji "nacionalne" sigurnosti EU. *Policija i sigurnost,* 21(1), 49-69.
Dragović, F. i Mikac, R., (2012), Stvaranje sigurnosnih politika EU. *Policija i sigurnost,* 21(1), 22-48.
Horjan i Šuperina, (2012.), Izgradnja strategije unutarnje sigurnosti EU. *Policija i sigurnost,* 21(1), 70-104.
Huysmans, J., (2000.), The European Union and the Securitisation of Migration. *Journal of Common Market Studies,* 38(5), 751-77.
Ivanda, S. (2001.), *Schengenski sporazumi i unutarnja sigurnost*. Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske.
Rošić, M., (2012), Policijska suradnja u schengenskom prostoru. *Policija i sigurnost,* 21(1), 170-187.
Solomun, D. (2012). Ekstremističko nasilje i mogućnosti policije u Republici Hrvatskoj u svjetlu nove sigurnosne paradigme, Zbornik radova s Međunarodne konferencije "Rat protiv terorizma nakon 10 godina", Zagreb: MUP RH, Policijska akademija, 241.-259.
Solomun, D. (2013). Sigurnost kritične infrastrukture u proširenom konceptu nacionalne sigurnosti // Nove sigurnosne ugroze i kritična nacionalna infrastruktura, Zagreb: MUP RH, Policijska akademija, 346.-362.
Solomun, D. (2015). Integracijom policijske prakse, teorije i znanosti do više kompetencija i sigurnijeg društva, Zbornik radova IV. Međunarodne znanstveno-stručne konferencije „Istraživački dani Visoke policijske škole u Zagrebu“, Zagreb: Ministarstvo unutarnjih poslova

Internetski izvori

Business Insider UK, The European economy will take a €100 billion hit if it re-establishes permanent border controls, http://uk.businessinsider.com/france-strategie-schengen-area-gdp-significantly-affected-by-eu-immigration-border-controls-2016-2 (preuzeto 20. veljače 2016.)
European Commision,, Standard Eurobarometer 84, http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/standard/surveyky/2098 (preuzeto 20. veljače 2016.)
EU Internal Security Strategy, http://www.consilium.europa.eu/uedocs/cms_data/docs/.../en/.../113055.pdf , 6.4.2014.
Europe Direct Nova Gradiška: Kako funkcionira Europska unija, str. 5, http://eudirect.ipng.hr/_Data/Files/150713132340302.pdf (preuzeto 17. rujna 2015)
European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the State of Play of Implementation of the Priority Actions under the European Agenda on Migration, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda- igration/proposal-implementation-package/docs/managing_the_refugee_crisis_state_of_play_20160210_en.pdf (preuzeto 16. veljače 2016.)
European Parliament, Directorate General for External Policies, Policy Department, STUDY Migrants in the Mediterranean: Protecting human rights, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/535005/EXPO_STU%282015%29535005_EN.pdf (preuzeto 20. veljače 2016.)

European union External Action, EUNAVFOR MED operation SOPHIA, http://eeas.europa.eu/csdp/missions-and-operations/eunavfor-med/index_en.htm (preuzeto 20. veljače 2016.)
Europska komisija, Komunikacija Komisije Europskom parlamentu i Vijeću, Osmo polugodišnje izvješće o funkcioniranju schengenskog područja 1. svibnja - 10. prosinca 2015., https://ec.europa.eu/transparency/regdoc/rep/1/2015/HR/1-2015-675-HR-F1-1.PDF (preuzeto 20. veljače 2016.)
Europska komisija - Priopćenje za tisak, Europska granična i obalna straža za zaštitu europskih vanjskih granica, http://europa.eu/rapid/press-release_IP-15-6327_hr.htm (preuzeto 20. veljače 2016.)
Europska komisija - Priopćenje za tisak, Bolje upravljanje svim aspektima migracija: Europski migracijski program, http://europa.eu/rapid/press-release_IP-15-4956_hr.htm (preuzeto 18. veljače 2016)
Europski program za sigurnost http://data.consilium.europa.eu/doc/document/ST-8293-2015-INIT/hr/pdf (preuzeto 22. rujna 2015.)
FRA, Highlights: 1 January - 31 January 2016, http://fra.europa.eu/en/theme/asylum-migration-borders/overviews/january-2016 (preuzeto 20. veljače 2016)
Frontex, Frontex launches rapid operational assistance in Greece, http://frontex.europa.eu/news/frontex-launches-rapid-operational-assistance-in-greece-u3rqPy (preuzeto 19. veljače 2016.)
FRONTEX, Annual Risk Analysis, http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2015.pdf#page=59 (preuzeto 15. veljače 2016.)
Human security in theory and practice, An Overview of the Human Security Concept and the United Nations Trust Fund for Human Security http://www.un.org/humansecurity/sites/www.un.org.humansecurity/files/human_security_in_theory_and_practice_english.pdf (preuzeto 4. veljače 2016.)
Ministarstvo vanjskih i europskih poslova, Ugovor o funkcioniranju Europske unije, pročišćeni tekst, http://www.mvep.hr/custompages/static/hrv/files/pregovori/111221-lisabonski-prociscena.pdf (preuzeto 19. veljače 2016.)
Ministero Della Difesa, Mare Nostrum Operation, http://www.marina.difesa.it/EN/operations/Pagine/MareNostrum.aspx, (preuzeto 16. veljače 2016.)
Missing Migrants Project, http://missingmigrants.iom.int/mediterranean (preuzeto 16. veljače 2016.)
Police and Judicial Co-operation in Criminal Matters https://en.wikipedia.org/wiki/Police_and_Judicial_Co-operation_in_Criminal_Matters (preuzeto 16.rujna 2015.)
Prague Post, Change in Czech refugee policy, http://www.praguepost.com/eu-news/49584-change-in-czech-refugee-policy (preuzeto 20. veljače 2016.)
Prilog Komunikaciji Komisije Europskom parlamentu i Vijeću, Izvješće o napretku provedbe žarišnih točaka u Grčkoj COM(2015) 678 https://ec.europa.eu/transparency/regdoc/rep/1/2015/HR/1-2015-678-HR-F1-1-ANNEX-1.PDF (preuzeto 20. veljače 2016)
Prilog Komunikaciji Komisije Europskom parlamentu i Vijeću, Izvješće o napretku provedbe žarišnih točaka u Italiji COM(2015) 679 https://ec.europa.eu/transparency/regdoc/rep/1/2015/HR/1-2015-679-HR-F1-1-ANNEX-1.PDF (preuzeto 20. veljače 2016)

Republika Hrvatska, MVEP, Ugovor iz Lisabona http://www.mvep.hr/custompages/static/hrv/files/EUugovori/12007L_Ugovor_iz_Lisabona_hrv.pdf (preuzeto 17. rujna. 2015.)
Rezolucija Europskog parlamenta od 19. siječnja 2016. o ulozi međukulturnog dijaloga, kulturne raznolikosti i obrazovanja u promicanju temeljnih vrijednosti EU-a (2015/2139(INI)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0005+0+DOC+XML+V0//HR (preuzeto 15. veljače 2016.)
Reuters, Defying EU, Hungary suspends rules on asylum seekers, http://uk.reuters.com/article/uk-europe-migrants-austria-hungary-idUKKBN0P31ZB20150623 (preuzeto 20. veljače 2016.)
Službeni list Europske unije, Uredba (EU) br. 604/2013 Europskog Parlamenta i Vijeća, http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32013R0604&from=EN (preuzeto 20. veljače 2016.)
The Washington Post, 8 reasons Europe's refugee crisis is happening now, autorice Liz Sly od 18. rujna 2015., https://www.washingtonpost.com/news/worldviews/wp/2015/09/18/8-reasons-why-europes-refugee-crisis-is-happening-now/ (preuzeto 15. veljače 2016.)
UNHCR, Refugees/Migrants Emergency Response – Mediterranean, http://data.unhcr.org/mediterranean/regional.php (preuzeto 16. veljače 2016.),
UNHCR u Republici Hrvatskoj, Zajednička izjava za medije UNHCR-a i IOM-a Milijun izbjeglica i migranata u bijegu prema Europi u 2015. godini, http://www.unhcr.hr/component/content/article/165-unhcr/news-and-views/news/277-zajednicka-izjava-za-medije-unhcr-a-i-iom-a-milijun-izbjeglica-i-migranata-u-bijegu-prema-europi-u-2015-godini (preuzeto 14. veljače 2016.)
UNHCR, Mixed Migration Flows in the Mediterranean and Beyond, http://data.unhcr.org/mediterranean/regional.php, (preuzeto 15. veljače 2016.)
UNHCR, Syria Regional Refugee Response, Inter-agency Information Sharing Portal, http://data.unhcr.org/syrianrefugees/regional.php# (preuzeto 16. veljače 2016.)
Vijeće za pravosuđe i unutarnje poslove, www.consilium.europa.eu/hr/council-eu/configurations/jha/ (preuzeto 15. rujna 2015.)
Xpressed an open journal, Hrvatskoj: Sekuritizacija izbjegličkog pitanja od strane političkih elita, http://www.x-pressed.org/?xpd_article=croatia-securitisation-of-the-refugee-issue-by-the-political-elites&lang=hr (preuzeto 20. veljače 2016.)
Završno izvješće o provedbi Strategije unutarnje sigurnosti EU-a 2010. – 2014. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2014)0365_/com_com(2014)0365_hr.pdf (preuzeto 15. rujna 2015.)

Popis slika

Slika 1. – Schengensko područje, Europsko vijeće, Vijeće Europske unije, http://www.consilium.europa.eu/hr/documents-publications/publications/2015/the-schengen-area-map/, (preuzeto 8. veljače 2016.)
Slika 2. - Kreiranje politika unutarnje sigurnosti Europskoj uniji (autorska slika)
Slika 3. - Migranti i izbjeglice kumulativno pristigli u Europu - po nacionalnostima, autorski prevedena slika, UNHCR, Mixed Migration Flows in the Mediterranean and Beyond, http://data.unhcr.org/mediterranean/regional.php, (preuzeto 15. veljače 2016.)
Slika 4. - Glavne migracijske rute u Europsku uniju - kopnom i morem, autorski prevedena slika, FRONTEX, Migratory Routes Map, http://frontex.europa.eu/trends-and-routes/migratory-routes-map/ (preuzeto 15. veljače 2016.)
Slika 5. – Dolasci izbjeglica i migranata morem u Grčku i Italiju od siječnja do prosinca 2015. prema podacima UNHCR-a, autorski prevedena i prilagođena slika, Wikipedia, European

migrant Crisis, https://en.wikipedia.org/wiki/European_migrant_crisis (preuzeto 16. veljače 2016.)
Slika 6. - Broj smrti izbjeglica i migranata na Sredozemlju po mjesecima u 2014. i 2015. godini (autorski prevedena slika, Missing Migrants Project, http://missingmigrants.iom.int/mediterranean (preuzeto 16. veljače 2016.)
Slika 7. - Glavne zabrinutosti na razini Europske unije, autorski prevedena slika, European Commision,, Standard Eurobarometer 84, http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/Survey/getSurveyDetail/instruments/STANDARD/surveyKy/2098 (preuzeto 20. veljače 2016.)
Slika 8. - Glavne zabrinutosti na razini države ispitanika, autorski prevedena slika, European Commision,, Standard Eurobarometer 84, http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/Survey/getSurveyDetail/instruments/STANDARD/surveyKy/2098 (preuzeto 20. veljače 2016.)
Slika 9. – Osjećaji ispitanika prema osobma koje imigriraju u njihovu zemlju, autorski prevedena slika, European Commision,, Standard Eurobarometer 84, http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/Survey/getSurveyDetail/instruments/STANDARD/surveyKy/2098 (preuzeto 20. veljače 2016.)

Matija Frčko
Davor Solomun

EU INTERNAL SECURITY IN RELATION TO RECENT CIRCUMSTANCES CONCERNING THE MIGRANT CRISIS

Summary

The paper analyses the cooperation in the field of internal security of the European Union and evaluates the suitability of its security policies and operational practices to new challenges and threats. The European Union implies as security integration the partnership and solidarity of Member States and a commitment to common institutions in the creation of enforceable security policies based on common values, taking into account specificities of the Member States. In terms of contemporary threats and menaces the current migration crisis in the Mediterranean and on so-called Western Balkan route proved to be a potential catalyst for an already increasingly prominent terrorist threat but also for an increase in intolerance and xenophobia in Europe. As such, it also creates a fertile ground for transnational organized crime and thereby actualizes the issue and the importance of strengthening security at the external borders of the Union. Secure external borders are a prerequisite and a guarantee for the preservation of the Union as an area of freedom and security. They depend on closer inter-state and inter-institutional collaboration, specialization of law enforcement officers and the introduction of new technologies. Elements of security decisions, their applicability and effectiveness in operational actions of law enforcement bodies with the purpose to protect and secure borders and thus the internal security of the Union represent challenges in terms of this paper.

Key words: *European Union, internal security, external borders, migration, organized crime.*

PREGLEDNI ZNANSTVENI RAD

Vojin Pilipović[572]
Tanja Kaurin[573]

JAVNOST U RADU POLICIJE I ZAŠTITA PODATAKA O LIČNOSTI

Sažetak

U radu se obrađuju osnovni problemi (pitanja) pravnog i etičkog karaktera, koja su značajna za javnost rada policije i zaštitu podataka o ličnosti, koja je deo osnovnog ljudskog prava na privatnost. Ustavno-pravna zaštita ljudskih prava i osnovnih sloboda podrazumeva, da svako ima pravo na to, da se poštuje njegov privatni i porodični život, stan i prepiska i da se javne vlasti (policija) neće mešati u vršenje ovog prava. To pravo može biti ograničeno samo zakonom, i kad je to neophodno u interesu nacionalne bezbednosti, javne bezbednosti ili ekonomske dobrobiti zemlje, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih. Građanin, kao aktivni učesnik društvenih i demokratskih procesa, ali i subjekat prava na zaštitu podataka o ličnosti, mora biti adekvatno obavešten o svom pravu, načinu ostvarivanja, kao i mehanizmima zakonske zaštite. U svim komunikacijama policije i javnosti (internet stranica, pisana saopštenja, dostupni materijali i sl.) pravo građana na privatnost, mora biti zaštićeno u skladu sa važećim standardima i sa sistemom zaštite podataka o ličnosti.

Ključne riječi: *građanin, policija, zaštita prava, javnost rada, podaci o ličnosti.*

1. Uvod

Nakon početnih dobrih rezultata u reformi policije (period od 2001-2003. godine), u poslednjih deset godina, propuštena je prilika da se potpuno izgradi jak institucionalni okvir rada u okviru Ministarstva unutrašnjuh poslova (MUP), što je prouzrokovalo neujednačen razvoj pojedinih oblasti, ključnih za pravni i etički integritet policije. Međutim, ipak se došlo do određenog nivoa unapređenja transparentnosti rada policije, usvojeni su ***Plan integriteta*** i ***Strategija razvoja***. I pored toga, na integritet policije i dalje, najviše utiču politizacija i neodgovarajuće upravljanje ljudskim resursima. Policija u Srbiji, mora da ima veću operativnu nezavisnost, a time i odgovornost za izvršavanje poverenih zadataka, a ne u

[572] Prof. dr. Vojin Pilipović, Univerzitet Union, Fakultet za pravne i poslovne studije dr Lazar Vrkatić Novi Sad, Bulevar oslobođenja br. 76, e-mail: vpilipovic@useens.net
[573] Doc. dr. Tanja Kaurin, Univerzitet Union, Fakultet za pravne i poslovne studije dr Lazar Vrkatić Novi Sad, Bulevar oslobođenja br. 76, e-mail: tanja.kaurin@useens.net

interesu političkih stranaka[574]. Sektor MUP, koji je zadužen za upravljanje ljudskim resursima, još uvek je više tehničko, a treba da bude pre svega operativno telo. Najzad, ne funkcioniše skladan sistem unutrašnje kontrole policije, koji istovremeno treba da obezbedi, da delovanje policije bude u skladu sa pravilima i da se poveća integritet policije. Spoljašnja kontrola rada policije[575] i dalje je nedovoljno pristupačna javnosti, odnosno nije ni dovoljno uređena, kako normativno (institucionalno), tako i funkcionalno.

Javnost rada policije prilično otežava još uvek ograničeno tumačenje pojma *transparentnosti*[576]**.** Unapređenje transparentnosti rada policije je posebno značajan cilj u ***Strategiji razvoja MUP***-a. za period 2011-2106.god. Utvrđene su i organizacione celine koje sprovode ovaj cilj, to je *Biro za informacije od javnog značaja*, koji postupa prema zahtevima za pristup javnim podacima u posedu MUP-a, i *Biro za saradnju sa medijima*, koji izveštava javnost o aktivnostima MUP-a. Postignut je napredak u saradnji sa Agencijom za borbu protiv korupcije, Zaštitnikom građana i Poverenikom.

Postoji i zakonska obaveza MUP-policije da redovno informiše javnost o svojim aktivnostima (godišnji i tromesečni izveštaji). Međutim, javnost rada ne podrazumeva samo postupanje prema zahtevima za pristup informacijama od javnog značaja, niti samo izveštavanje javnosti na internet stranici MUP-a. Veću transparentnost moguće je ostvariti uspostavljanjem građanskog nadzora[577] nad krivičnim istragama, naročito nad onim koje se odnose na rad policajaca. Posebno su značajne mere tajnog prikupljanja podataka, koje predstavljaju osetljivu sferu delovanja državnih organa u kojoj potpuna transparentnost, iz razumljivih razloga, nije moguća.

Međutim, to ne znači da nije potrebno i moguće ostvariti određen stepen javnosti u ovoj oblasti. S druge strane, kako se posebnim merama privremeno ograničavaju prava građana, a rizik od zloupotreba je izražen, neophodan je određen nivo transparentnosti koji bi omogućio spoljni nadzor nad primenom ovih mera. Povećanjem transparentnosti posebno bi se unapredilo poverenje građana u institucije i osećaj sigurnosti koji bi građani imali, ukoliko su upoznati sa delovanjem države u sferi određivanja i sprovođenja posebnih mera. Transparentnost rada policije u ovoj oblasti, bi omogućila, da udruženja građana i stručna

---

[574] Tokom februara 2013. godine u javnosti započeta rasprava o novom direktoru policije, koja se razvila u „dilemu", da li će direktor policije biti blizak Aleksandru Vučiću ili Ivici Dačiću, predsednicima vodećih stranaka u izvršnoj vlasti. Niko ne priča o tome, šta bi zaista trebalo da radi novi direktor policije i koji su njegovi budući zadaci u daljem toku procesa reforme policije. Pre toga, javnosti je bila poznata situacija nastala povodom izbora načelnika policijskih uprava u Nišu i Novom Sadu, koji je zbog političkih interesa kasnio više od tri godine. Poslednji slučaj odnosio se na smenu pet načelnika uprava u sedištu MUP, bez odgovarajućeg obrazloženja (iako su u prethodnom periodu dobro ocenjeni za svoj rad).

[575] Zakon o policiji "Službeni glasnik RS" br.06/2016. (članovi 219-223), uređuje, da se spoljašnja kontrola rada MUP vrši od strane Narodne skupštine (preko nadležnog Odbora za unutrašnje poslove), zatim skupštine pokrajinske autonomije i lokalne samouprave, pravosudnih organa, nezavisnih državnih organa, građana i javnosti. Međutim, zakon ne pominje nikakve oblike kontrole i uvida u rad MUP od strane građana i javnosti.

[576] Transparentnost u radu policije možemo shvatiti kao javni nadzor, odnosno javno nadgledanje i praćenje rada i efikasnosti policijskih službenika u svakodnevnom postupanju u zaštiti lične bezbednosti građana, njihove lične imovine, obezbeđenju javnog reda, i u drugim poslovima određeni zakonom.

[577] U Hrvatskoj je to učinjeno u julu 2014. godine zbog sumnje javnosti u korektan rad policije. Formiranjem Vijeća za građanski nadzor nad primenom policijskih ovlašćenja, uvida u telefonske listinge i prikrivene policijske radnje povećani su transparentnost i spoljna kontrola rada policije (Izvor:www.novilist.hr/vijesti/hrvatska,dana 06.02.2014. godine, autor D.Radaljac).

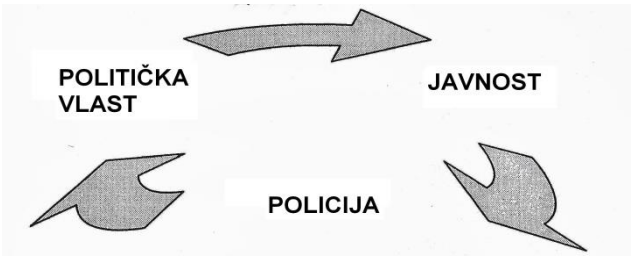
javnost, analiziraju primenu posebnih mera, te da na osnovu toga sačinjavaju predloge za unapređenje kako njihove primene tako i nadzora nad njima.

Do sada, najznačajniji doprinos u sagledavanju javnosti rada policije, u okviru ukupnog procesa reforme sistema bezbednosti u Srbiji, dao je *Centar za bezbednosnu politiku* (bivši Centar za civilno vojne odnose), kroz objavljivanje studija o reformi sistema bezbednosti u periodu od 2004-2009. godine, kao i istraživanja medijskih kuća iz Beograda (period 2011-2014. godine), koje su ispitivale stavove javnog mnjenja o radu policije, i u vezi s tim ocene građana[578].

2. Odnosi policije i javnosti

2.1. Društveno-psihološke i normativne osnove odnosa policije i javnosti

Policijska organizacija u Republici Srbiji deluje u veoma različitom društvenom, ekonomskom, vojnom i političkom okruženju. Procesi privatizacije bezbednosnih poslova su još u toku, reforma sistema bezbednosti još nije završena, a i pristupni pregovori sa EU, zahtevaju nov pristup u definisanju položaja i uloge policije, odnosno definisanje novih oblika i sadržaja saradnje policije i javnosti. S pravom može tvrditi, da je odnos policije i javnosti upravo odraz ukupnih odnosa građanin – država, odnosno, da je neodvojiv od položaja i uloge čoveka u političkom sistemu (Kešetović, 2000:522). Najopštije pretpostavke za uspostavljanje dobrih odnosa policije i javnosti u društvu su: *stabilni odnosi u društvu*; *politička neutralnost policije*; *politika koju vodi Vlada*; i *specifičnosti policijske profesije (zakonitost, visoki profesionalizam, upotreba policijske prinude, policijska etika)*. Moglo bi se reći, da se policija nalazi u specifičnom položaju, odnosno, zajedno sa političkom vlasti i javnosti čini „trougao“ odnosa koji se mogu posmatrati sa aspekta policijske profesije (*shema 1*.).



Shema1.Odnos policije, javnosti i vlasti u našem društvu (izvor: Pilipović, 2009:179)

Kontakti policije i građana svakodnevno su na „ispitu“, odnosno proveri javnosti, jer policijske greške u radu i postupanju, a naročito kada je u pitanju primena policijske prinude, veoma snažno utiču na javni lik i ocenu ugleda policijske profesije. Na odnose javnosti i

[578] Beogradski Centar za bezbednosnu politiku: „*Organizacija civilnog društva i sektor bezbednosti“, Skupštinski nadzor sektora bezbednosti*“, i *Javni nadzor politike bezbednosti*“, u periodu 2004-2009. godine, kao i Godišnjak reforme sektora bezbednosti u Srbiji–*Nadzorna uloga nezavisnih državnih organa* (2008-2011.). Istraživanje javnog mnjenja: CeSID- *Stav građana prema radu policije*, novembar 2011. godine; OEBS-Misija u Srbiji-*Stav građana prema policiji*, decembar 2012. godine i TNS Medium Gallup- *Stav građana prema radu policije*, novembar 2013. godine.

policije utiču još i: policijska kultura, sociološki položaj profesije, stepen centralizacije, efikasnost u suzbijanju kriminaliteta, rešavanje pritužbi, kontrola rada, selekcija i obuka policijskih službenika i drugo. Zbog svega navedenog, neophodna je nova organizaciona struktura i nov model u policijskoj delatnosti prilagođavati novonastalim promenama, pre svega u prevenciji kriminaliteta i drugih društveno opasnih pojava i ponašanja. Bez građana, svi napori i aktivnosti policije neće imati velikog uspeha, što znači, da je jedno od najvažnijih pitanja, odnos policije prema građanima.

U suštini, odnos policije i javnosti znači izgradnju poverenja, razumevanja i tolerancije, kao i uspostavljanje humanijih odnosa među ljudima na ravnopravnoj osnovi. S jedne strane, policiji je i te kako potreban **sud javnosti** (ocena) kada je u pitanju njena efikasnost i ostvarivanje osnovne uloge, a to je bezbednost države i njenih građana dok, sa druge strane, građani očekuju maksimalan stepen zaštite lične i imovinske sigurnosti na svakom mestu i u svako vreme. Zato su upućeni jedni na druge, pa će izgradnjom dobrih odnosa i poštovanja biti ostvaren visok stepen sloboda i prava, odnosno nivo demokratizacije odnosa u celom društvu.

Normativne pretpostavke[579] za uspostavljanje pravilnih odnosa između policije i javnosti, kao i potpuno informisanje javnosti, garantuju, da se ovim pitanjima od strane MUP-a, odnosno policije, pridaje značajna pažnja. U sedištu MUP-a, pri kabinetu ministra, nalaze se unutrašnje organizacione jedinice, *Biro za saradnju sa medijima* i *Biro za pritužbe i predstavke*. U svim upravama u sedištu, kao i u područnim policijskim upravama, određena su odgovorna lica za postupanje po zahtevima za slobodan pristup informacijama.

Dakle, posebna pažnja u radu MUP posvećena je javnosti u radu u cilju njegove prezentacije i kontrole rada. U skladu s tim, pripremaju se *saopštenja* za javnost i održavaju redovne i vanredne konferencije za novinare, na kojima se javnost upoznaje sa stanjem bezbednosti, rezultatima rada i angažovanju policije. Saradnja sa medijima se ostvaruje i davanjem različitih *intervjua* o radu policije, učešćem predstavnika policije u TV emisijama, te obaveštavanjem javnosti o radu MUP-a u pogledu svih drugih pitanja iz njegove nadležnosti, kao što su, npr., problemi oko putnih isprava, ličnih karata, izdavanja novih registarskih tablica, viza za putovanja u inostranstvo i dr. Takođe, radi se na otvaranju MUP prema organima lokalne samouprave, u cilju unapređenja sistema informisanja, i u skladu s tim je izrađeno Uputstvo.[580]

Na osnovu svega navedenog, mogu se definisati glavni ciljevi policije u oblasti odnosa sa javnošću, a to su: informisanje na otvoren i korektan način o događajima koji su vezani za policiju; informisanje građana o radu policije; poboljšanje razumevanja uloge i odgovornosti policije kroz transparentne, aktivne i redovne javne i medijske kampanje; susreti sa medijima kako bi se prikazao rad policije; i primena standardne procedure u odnosima sa medijima.

---

[579] U skladu sa ustavnim odredbama i Zakonom o slobodnom pristupu informacijama od javnog značaja, *Službeni glasnik RS*, br. 104/04, i Uputstvom za objavljivanje informatora o radu državnih organa, *Službeni glasnik RS*, br. 57/06, regulisana su sledeća pitanja: davanje informacija, lica ovlašćena za davanje informacija, obaveze i ovlašćenja, način informisanja, i druga.

[580] *Uputstvo o osnovnim standardima u postupanju sa medijima*, koje je izdao ministar unutrašnjih poslova, kojim je kao novina u radu predviđeno radno mesto portparola „PR“, u svim organizacionim jedinicama MUP-a, centrala – 2, uprave u sedištu – 20 i u svim područnim policijskim upravama 27, kao i u Koordinacionoj upravi za KiM-7 lica, koja su ovlašćena da daju informacije od javnog značaja.

2.2. Neke pretpostavke – uslovi za uspešno uspostavljanje dobrih odnosa policije i javnosti

Radi uspešnog ostvarivanja policijske funkcije uopšte, a posebno na području policijske uprave (stanice), odnosno bezbednosnog sektora (pozorničkog rejona), policajci[581] moraju dobro poznavati: geografsko-topografske karakteristike područja, stanovništvo, naseljena mesta, objekte, komunikacije, kao i političke, ekonomske, kulturne, socijalne i druge prilike na teritoriji za koju su bezbednosno odgovorni.

Poznavanje stanovništva podrazumeva opštu obaveštenost o broju, strukturi (nacionalnoj, socijalnoj, starosnoj i slično) stanovnika po delovima naselja, ulica, zaseoka, kao i na području cele policijske uprave, odnosno policijske stanice. Takođe, važno je poznavanje bezbednosno interesantnih lica, pre svega registrovanih izvršilaca krivičnih dela, lica sklonih vršenju krivičnih dela, i drugih lica koja su bezbednosno interesantna.

Poznavanje naseljenih mesta i objekata je važno zbog sticanja ukupne obaveštenosti o: veličini, broju, gustini naseljenosti, nazivu pojedinih mesta i objekata, udaljenosti od sedišta policijske uprave ili policijske stanice i drugo. Sve ovo će doprineti lakšem i boljem komuniciranju između policajaca međusobno, i policajaca i građana, kada se rešavaju pojedini bezbednosno interesantni problemi. Znamo u praksi da građani brzo primete šta u postupanju policajaca, odnosno u službenim radnjama, nije u redu. Oni prate svaku reakciju i postupanje policajca, očekujući da njegova intervencija bude brza, pravična, objektivna i zakonita.

Prilikom preduzimanja službenih radnji u ophođenju sa građanima, kao i prilikom primene ovlašćenja, policajci moraju voditi računa i o: izrazu lica; izražavanju i upotrebi reči, visini tona, vođenju razgovora, odnosu prema prekršiocima zakona i posebno prema žrtvama krivičnog dela, da budu pažljivi, i uvek spremni da pomognu. Isto tako, i ovom prilikom treba istaći i neke lične kvalitete (poželjne vrline) koje bi svi policajci trebalo da poseduju, a pre svega: inteligenciju, samopouzdanje, pozitivni karakter, dobro rasuđivanje, hrabrost, dovitljivost, komunikativnost, dinamičnost, objektivnost, prilagodljivost – snalaženje u promeni situacije, ambicioznost i želju za usavršavanjem i karijernim napredovanjem u službi[582].

Mesta i situacije koje zahtevaju poseban odnos policijskih službenika prema građanima su: *obaveštavanje o smrtnim slučajevima; obaveštavanje o povredama građana; obaveštavanje o licima koja su lišena slobode ili zadržana u policiji; ponašanje u slučaju zemljotresa, poplave, požara, elementarnih nepogoda* i druge slične situacije, takođe, zahtevaju specifičan odnos policijskih službenika prema građanima.

Policijski službenik kao *građanin u javnom životu* je stalno izložen oceni-sudu javnosti (uniforma, primena ovlašćenja, ponašanje i sl. Pilipović, 2009:191). Lični život i svakodnevno ponašanje policijskih službenika deo je stvaranja ukupnih odnosa javnosti i policije. Policajac je istovremeno građanin i državljanin, stanovnik određenog mesta, otac, suprug, prijatelj, komšija i slično, ali ga sredina u kojoj živi i radi uvek doživljava kao policajca, odnosno državnog službenika. Stav građana prema njemu je skup ili odraz opštih

[581] U smislu čl. 7 Zakona o policiji, ovaj izraz ima jednako rodno značenje, bez obzira da li se koristi u muškom ili ženskom rodu.

[582] Zakon o policiji, čl. 165 definiše sistem karijernog razvoja policijskih službenika: određivanje čina/zvanja prema poslovima na koje je policijski službenik raspoređen, zatim prema istom ili neposredno višem nivou, kao i za sticanje generalskog čina, na rukovodećim mestima strateškog i visokog nivoa.

utisaka koje oni imaju o policiji. Činjenica je, da će građani uvek „strože“ tretirati svako nepristojno ili nezakonito ponašanje policajca, za razliku od ostalih građana, što je i razumljivo. Tradicionalno se na našem prostoru različito gleda na policiju. Nema sumnje da prema policiji niko nije ravnodušan. Postoje delovi društva koji imaju negativan stav prema policiji (Krstić, 2007:204/205). Ovo je posledica zatvorenosti policijskog delovanja, odnosno nedostatak uvida šire javnosti u policijsku delatnost, što se naročito ispoljilo u poslednjoj deceniji prošlog veka. Pored stručnih znanja i veština kojima je ovladao, od policajca se traži da uvek bude uljudan, strpljiv, obazriv, predusretljiv, kulturan i profesionalan u ophođenju sa građanima i da uvek bude spreman da pomogne. Društvena sredina drugačije, daleko „strožije“ vrednuje i ponašanje članova porodice policijskog službenika. Dakle, od policajca i njegove porodice se očekuje da budu znatno bolji od okoline koja ih okružuje (Jovanović, 2001:51).

Na kraju ističemo, kao i sada veoma aktuelno, zapažanje *Augusta Vollmera* koje je on, kao utemeljivač modernog upravljanja policijom u SAD, zabeležio još 1936. godine. „Kada bi sve to imao, bio bi dobar policajac“ – Volmer je zabeležio: „Policajac treba da ima *mudrost Solomona, hrabrost Davida, snagu Samsona, strpljenje Jova, predvodništvo Mojsija, ljubaznost dobrog Samarićanina, strategiju Aleksandra Velikog, veru Danijela, diplomatiju Linkolna, toleranciju drvodelje iz Nazareta, i, konačno, solidno znanje iz svake grane prirodnih, bioloških i društvenih nauka*“ (Milosavljević, 1997:234). Pored navedenog, istaknuto je i sledeće: „Policajca ogovara javnost, ismevaju ga u filmovima, kritikuju u listovima i ne podržavaju ga ni tužioci ni sudije, … kriminalci ga mrze, … svi ga varaju. Izložen je brojnim iskušenjima i opasnostima, osuđuju ga kada primenjuje propise, a otpuštaju iz službe ako to ne čini. Misle da mora imati obrazovanje vojnika, lekara, pravnika, diplomate i vaspitača za platu, koja je manja od one koju ima nadničar“.

2.3. Ciljevi i značaj dobrih odnosa policije i građana

Osnovni okvir za ostvarivanje svih principa u radu policije, proizilazi iz Strategije[583], gde su definisani glavni ciljevi policije u zajednici. ***Vizija***-bezbedna zajednica sa dostupnom i nepristrasnom policijskom službom koja odgovorno deluje u partnerstvu sa zajednicom i građanima na rešavanju bezbednosnih problema. ***Misija***-profesionalni i etički razvoj policijske službe u skladu sa demokratskim vrednostima, bezbednosnim izazovima i potrebama građana i zajednice.

Vrednosti delovanja policije u zajednici se izražavaju kroz sledeće aktivnosti policije:

- *odgovorno služenje građanima;*
- *ravnopravan odnos prema svima uz uvažavanje različitosti ljudi, uvažavanje zajednice i njihovih potreba;*
- *uključivanje zajednice u rešavanje bezbednosnih problema; i*
- *posvećenost ostvarivanju bezbednosti građana i zajednice.*

Strateški ciljevi i vodeći elementi u razvoju policije biće usmereni na: uspostavljanje savremenih standarda u radu policije; jačanje poverenja građana i zajednice u policiju;

[583] *Strategija policije u zajednici*, Vlada Republike Srbije, Beograd, br. 05/021-1082/2013-003., od 30. aprila 2013. godine, str. 5-8.

saradnja i partnerstvo policije sa zajednicom; uspostavljanje delotvorne bezbednosne prevencije; problemski orijentisan pristup bezbednosnoj zaštiti; i posvećenost poštovanju etičkih principa i različitosti.

U praktičnoj primeni, strateški ciljevi policije u zajednici se ostvaruju primenom četiri vodeća elementa, i to:

1) prevencija, što predstavlja delovanje na redukciju uzroka kriminala, nereda, straha od nasilja i drugih bezbednosnih pretnji, u većoj meri proaktivno nego reaktivno;

2) rad policije usmeren na zajednice, kao adekvatan odgovor na prioritetne i druge potrebe građana i specifičnosti lokalnih zajednica, etničkih, verskih i drugih društvenih grupa;

3) problemski orijentisan rad, kao metod koji se zasniva na izvorima informacija, i koristi ih za identifikaciju obrazaca kriminala i tenzija u zajednicama; i

4) bezbednosno partnerstvo, koje se odnosi na sporazumno delovanje policije i zajednice, u bezbednosnoj prevenciji, rešavanju bezbednosnih problema i razvoju bezbednosnih strategija uključujući predstavnike i kapacitete drugih državnih organa, lokalnih samouprava i civilnog društva.

Policija, kao centralna organizaciona jedinica MUP-a, svakodnevno je izložena sudu javnosti, pa je utoliko značajnije, da uspostavi i neguje odnos ***poverenja*** i ***razumevanja***, kako u izvršavanju profesionalnih zadataka, tako i u pružanju pomoći u slučajevima kada nije nadležna. Ovo je važno, pre svega, jer građani nisu u situaciji da poznaju sve propise i nadležnosti pojedinih organa i institucija, ali će postupanje, davanje obaveštenja ili informacija od strane policajca, pomoći da građani svoje probleme brže rešavaju, tako da će autoritet policajca u konkretnom slučaju biti veći, odnosno, građani će prihvatati policiju kao svoju.

3. Odnos policije i medija

U skladu sa glavnim ciljevima policije Republike Srbije u oblasti odnosa sa javnošću, posebno mesto treba da zauzima odnos prema medijima. Ovaj odnos se može definisati kroz određene institucionalizovane, odnosno formalne oblike saradnje. **Otvorenost** i **korektnost** u informisanju, razumevanje uloge i odgovornosti policije, kao i češći susreti sa medijima, mogu se posmatrati i kao osnovni principi u uspostavljanju dobrih odnosa policije sa medijima. Mediji, kao sredstva za prenošenje informacija (radio, televizija, novine, knjige, plakati, video-materijali i slično), namenjeni su širokom krugu korisnika, pa je utoliko i obaveza policije veća (Milosavljević, 1997:277). U odnosu prema medijima, policija mora da se pridržava određenih zakonskih načela[584], kao što su: *dostupnost*, *jednakost* i *nepristrasnost*, *zabrana diskriminacije*, kao i *ograničenje* pod određenim zakonskim uslovima.
Načelo *dostupnosti* obavezuje policiju, da svakom da informaciju od javnog značaja, tako što će mu se omogućiti uvid u dokument koji sadrži informaciju, kao i pravo na kopiju tog

[584] Pored načela u Zakonu o policiji (članovi 5., 6, 33), u ***Strategiji zaštite podataka o ličnosti***, predvidena su ključna načela, opšti i posebni ciljevi u sprovođenju zaštite podataka, kao i obaveze iz ***Direktive*** 95/46/EZ, što u svom radu moraju da primenjuju svi državni organi, pa tako i policija. Strategija zaštite podataka o ličnosti, II poglavlje, str. 2 i 3.

dokumenta, odnosno pravo da se, na zahtev, kopija dokumenta dostavi poštom, faksom, elektronskom poštom ili na drugi način.
Načelo *jednakosti* garantuje svima, da će od policije pod jednakim uslovima dobiti informaciju, bez obzira na državljanstvo, nacionalnost, versku pripadnost, prebivalište, pol, rasu i slično. Policija ne sme stavljati u povoljniji položaj nijednog novinara ili javno glasilo, u slučaju kada je više njih uputilo zahtev za informaciju, na šta je obavezuje načelo *zabrane diskriminacije* novinara i javnih glasila. Isto tako, pod određenim uslovima, policija može ograničiti davanje informacija ako su u interesu život, zdravlje, sigurnost, odbrana zemlje, nacionalna i javna bezbednost, tajna, kao i ekonomska dobrobit zemlje. U sprovođenju ovih načela u praksi, policija je odgovorna i dužna da štiti ***privatnost***[585] i druga prava ličnosti, kao i da spreči zloupotrebe slobodnog pristupa informacijama od javnog značaja.

3.1. Značaj dobrih odnosa policije i pojedinih medija

Policijska aktivnost, kao i problematika na koju se ta aktivnost odnosi, mogu biti veoma značajni za medije.[586] Poznata je izreka: „*ono što nije objavljeno, nije se ni desilo*“, ali danas, praktično da nema dnevnih novina, koje se na bilo koji način ne bave aktivnostima policije. Nezavisno od određenih slabosti koje postoje u slobodi štampe, mediji poseduju moć koju policija ne sme da zanemari. Mediji su u samom centru (žiži) interesovanja kada su u pitanju odnosi policije i javnosti, a slika koju mediji kreiraju može direktno da utiče na podizanje autoriteta i očuvanje ugleda koji policija ima. Mediji mogu da budu u ulozi spoljašnje ili neformalne kontrole rada policije.

Štampa se u poslednje vreme (kraj XX i prva decenija XXI veka) razvila u takozvanu „sedmu silu“ modernog društva (Milosavljević, 1997:268) i ostvarila snažan uticaj na javnost, odnosno kreiranje javnog mnjenja ili suda javnosti. Nezavisnost i sloboda štampe u svetu, a tako i kod nas, garantuju se svim propisima i smatraju se „bazom demokratskih institucija“. Upravo štampa i treba da služi za slobodu iznošenja mišljenja, razmenu i komentare o dobrim postupcima policije–razmenjuju se ideje i kritikuju loši potezi policije, odnosno zloupotreba policijskih ovlašćenja. Dobri odnosi policije i štampanih medija višestruko su korisni policiji (Kešetović, 2000:544), jep se tako podstiče saradnja i podrška značajnog dela javnosti. U cilju uspostavljanja dobrih odnosa, policija treba da obezbedi isti tretman svim glasilima, bez obzira na njihova stranačka i/ili politička opredeljenja. Dostavljanje brze, tačne i potpune informacije od javnog značaja, omogućava blagovremeno i tačno informisanje javnosti, jer zakasnela („bajata“) informacija ponekad ništa ne znači. U svim tim kontaktima policija se pridržava propisane procedure.[587]

---

[585] Zakon o policiji, čl. 49., obavezuje policijske službenike da u prikupljanju obaveštenja, ne otkrivaju identitet lica, od koga su dobili podatak, ako bi se time lice izložilo opasnosti po život, zdravlje ili bi time bila ugrožena sloboda i imovina lica.
[586] http://www.b92.net (pristup 02. februara 2016.godine).
[587] Zakonom o slobodnom pristupu informacijama od javnog značaja (članovi 15-21), propisan je postupak policije-od podnošenja zahteva, odlučivanje, rokovi, stavljanje na uvid, izrada kopije, kao i obaveze policije prema Povereniku.

Radio i televizija se javljaju kao konkurent štampi, jer ne zahtevaju veću pažnju i brže prenose tekst, uz sliku, o akcijama policije, čime mogu preneti značajne sadržaje i uverljivije postići određene efekte. Poznata je izreka da „*slika zamenjuje hiljadu reči*“. Radio i TV reportaže određenih događaja sa lica mesta i postupanje policije na najuverljiviji način mogu doprineti blagovremenom i tačnom informisanju gledalaca, odnosno slušalaca, čime građani mogu dati legitimitet preduzetoj akciji policije, odnosno mogu osporavati takve postupke. Informacije koje se ovim putem prenose, a u vezi su sa policijskim poslovima, uz ravnopravan tretman svih radio i TV stanica koje su prisutne na mestu događaja, mogu se reprizirati (ponoviti) na zahtev određenih subjekata, pri čemu se stiče šira (kompletnija) slika o nekim događajima. Na taj način će se doprineti jasnom i transparentnom odnosu policije i građana, odnosno policije i javnosti u celini. U nekim državama, članicama EU, postoje posebni TV kanali za policijske aktivnosti, pa se sada opravdano postavljaju zahtevi, da se to uradi i kod nas.

Film ili ***video-zapis***, kao i ***fotografije***, imaju tu prednost što „hipnotišu“ pažnju i izazivaju jake emocije kod gledalaca, prevazilaze jezičke barijere i ostavljaju trajniji utisak ili određenu poruku. Odnos policije prema ovom mediju takođe mora biti pažljiv, jer su ti prezentovani podaci nezamenjivi i pouzdani i mogu biti i dokazi u spornim situacijama, a policija ih može koristiti u kasnijem postupku. ***Internet***, kao značajno sredstvo masovne komunikacije policije i građana, u poslednje vreme je veoma aktuelan, o čemu će biti više reči u narednom izlaganju.

Cilj negovanja dobrih odnosa policije i medija ne sme da bude pridobijanje „naklonosti“ pojedinih medija, već *partnerski odnos,* zasnovan na razumevanju i saradnji, koja može biti izražena na različite načine. Policijska delatnost je veoma složena, pa mediji mogu dati značajan doprinos, kako u prevenciji, odnosno edukaciji građana, tako i u sprečavanju kršenja zakonskih propisa. Policijska organizacija ne sme da se otuđuje od javnosti, odnosno medija, niti joj je zagarantovana naklonost javnosti. Upravo zbog toga visoki policijski rukovodioci moraju stalno da brinu o tim odnosima, da ih unapređuju, edukuju mlađe kadrove, kako bi se ta aktivnost policije i medija usmeravala na sprečavanje i suzbijanje društveno negativnih pojava, što je briga cele društvene zajednice.

3.2. Oblici komunikacije policije i medija

Internet je jedan od pouzdanijih i najkompletnijih oblika komuniciranja policije i medija, ali objektivno postoji problem kod informisanja građana[588] koji nemaju to sredstvo za komunikaciju. Najčešće, u praksi, to se ostvaruje putem izrade internet stranice MUP-a ili uže organizacione jedinice, preko TV ili javnim objavljivanjem pojedinih podataka ili informacija. Policija preko ovih sredstava masovnog komuniciranja prezentuje različite podatke i informacije o svom radu, a najčešće se koriste sledeći oblici komuniciranja:

- *saopštenja za javnost o pojedinim događajima ili akcijama policije*;
- *redovne i vanredne konferencije za štampu*;

[588] Prema javno objavljivanim podacima, u više navrata, u periodu 2010-2015. godine (Jutarnji program RTS), u Republici Srbiji, samo oko 10% građana, redovno koristi *INTERNET*, po čemu je Srbija, na dnu liste evropskih zemalja.

- *intervjui pojedinih ovlašćenih policijskih rukovodilaca*;
- *učešće predstavnika MUP-a u televizijskim emisijama*;
- *objavljivanje propagandnih materijala (plakati, spotovi, leci, flajeri i slično)*;
- *bilbordi i druge reklamne poruke propagandnog karaktera*;
- *obaveštenja o stanju bezbednosti ili aktuelnim bezbednosnim događajima*; i
- *izrada biltena dnevnih – nedeljnih događaja ili povremenih informacija za organe lokalne samouprave*.

Pored navedenih oblika komuniciranja policije i građana preko medija, moguće je preko ovih sredstava istraživati (ispitivati) odnos i poverenje građana, odnosno ocenu građana o pojedinim pitanjima iz oblasti policijske delatnosti.[589] Tu se radi se o sledećim pitanjima: *anketiranju građana o ulozi i efikasnosti policijskog rada u određenoj sredini, popularizaciji policijskog poziva, prezentaciji pojedinih sredstava i metoda u radu, češćim saopštenjima i davanju informacija o bezbednosno važnim događajima, prihvatanju i priznavanju propusta, oceni građana o kontroli rada policije; demantovanju neistinitih sadržaja argumentima i dokazima*, i slično. Prednost navedenih oblika komuniciranja policije i medija je u preciznom, tačnom, blagovremenom, kao i zakonitom informisanju, gde su definisani cilj, obim, izvor informacija, kao i odgovornost lica koje daje podatke ili informacije od javnog značaja. Na kraju, može se sa sigurnošću utvrditi, da su međusobni odnosi policije i medija od obostrane važnosti, kako za ostvarivanje njihovih uloga u užem smislu, tako i za odvijanje ukupnih političkih procesa u našem društvu.

4. Načelo tajnosti u radu policije i zaštita podataka

Mesto i uloga policije u okviru MUP-a Republike Srbije, je zakonski regulisana i određena sa jasnim zadacima, oblastima angažovanja i odgovornosti.[590] Policija štiti i unapređuje bezbednost građana i imovine, poštujući Ustavom zajemčena ljudska i manjinska prava i slobode i druge zaštićene vrednosti u demokratskom društvu, uz mogućnost na Ustavu i zakonu zasnovane upotrebe sredstava prinude. MUP-a, što znači da i policija ima obavezu, da redovno blagovremeno i potpuno obaveštava javnost o svom radu, osim u slučajevima preduzimanja mera i radnji u skladu sa zakonom, kojim se uređuje krivični postupak i kada bi to onemogućilo neometan operativni rad policije ili ako bi se time:

- *povredio propis o tajnosti podataka;*
- *povredilo dostojanstvo građana; i*
- *ugrozilo pravo na ličnu slobodu i bezbednost.*

MUP jednom godišnje, a najkasnije u roku od tri meseca od završetka kalendarske godine, objavljuje: 1) ***izveštaj o stanju bezbednosti u Republici Srbiji*** koji na transparentan i javan način obaveštava javnost o proceni bezbednosti, trendovima kretanja kriminala i drugih bezbednosnih pojava od značaja za bezbednost i prava građana; i 2) ***izveštaj o radu Ministarstva***, koji na transparentan i javan način obaveštava javnost o

[589] http://www.b92.net/info/vesti (pristup 07. februara 2016).
[590] *Zakon o policiji*, članovi 3-6.

razvoju policije, statističkim podacima o sprovedenim aktivnostima i postignutim rezultatima. Pored izveštaja o radu i stanju bezbednosti za tekuću godinu, MUP-a je u obavezi da objavi na svojoj internet prezentaciji i tromesečne informacije o radu, koje usvaja nadležni odbor Narodne skupštine Republike Srbije za unutrašnje poslove.

Policija primenjuje ***posebne mere tajnog prikupljanja podataka***, što predstavlja osetljivu sferu delovanja, u kojoj potpuna transparentnost, iz razumljivih razloga, nije moguća. Međutim, to ne znači da nije potrebno i moguće ostvariti određen stepen javnosti u ovoj oblasti[591]. S druge strane, kako se posebnim merama privremeno ograničavaju prava građana, a rizik od zloupotreba je izražen, neophodan je određen nivo transparentnosti koji bi omogućio spoljni nadzor nad primenom ovih mera. Povećanjem transparentnosti posebno bi se unapredilo poverenje građana u policiju i osećaj sigurnosti, koji bi građani imali ukoliko su upoznati sa delovanjem države u sferi određivanja i sprovođenja posebnih mera. Transparentnost rada u ovoj oblasti bi takođe omogućila, da udruženja građana i stručna javnost analiziraju primenu posebnih mera te da na osnovu toga sačinjavaju predloge za unapređenje kako njihove primene tako i nadzora nad njima.

4.1. Zaštita informacionih sistema i podataka

U informacionim sistemima skoncentrisana je ogromna količina filtriranih, proverenih i uređenih podataka i informacija koji, po svojoj prirodi, mogu da izražavaju materijalnu vrednost (na primer, „elektronski novac“ ili stanje robe na skladištu), ali isto tako mogu da predstavljaju ličnu, poslovnu, profesionalnu, bezbednosnu, vojnu ili državnu tajnu. Ako se u obzir uzme i činjenica da računari brzo i sigurno preuzimaju brojne, pa i najvitalnije funkcije ljudske delatnosti, povezane sa najsloženijim i najosetljivijim odnosima, pojavama i procesima u društvu, nije nerazumna hipoteza, da se društvo ubrzano kreće pravcem koji ga vodi ka velikoj zavisnosti od ove tehnologije, i to u svim oblastima i na svim nivoima. Zbog ozbiljnosti, složenosti i značaja, zaštita informacionih sistema, a posebno njen pravni aspekt, je već godinama predmet studija, rasprava i odluka različitih nacionalnih i međunarodnih tela i organizacija, a broj zemalja koje su ovu materiju u manjoj ili većoj meri, na ovaj ili onaj način, regulisale – stalno se uvećava.

Pod pojmom ***zaštite*** podrazumevaju se sredstva, mere i aktivnosti namenjeni za sprečavanje ili umanjenje ugrožavanja materijalnih dobara, prava i života ljudi, životne sredine, države i društva. U domenu informaciono-komunikacionih tehnologija (IKT) pojam zaštite obuhvata zaštitu IKT opreme, infrastrukture, programa i podataka.

Potencijalni izazivači ugrožavanja informacionih sistema i podataka mogu biti svrstani u sledeće kategorije:

- “Viša sila”,
- Nedostaci (kvarovi) na opremi i u programima,

[591] Poverenik za informacije od javnog značaja Rodoljub Šabić, saopštio je, da je nezadovoljan odnosom nadležnih organa, posebno Vlade prema oblasti zaštite podataka o ličnosti. U pismu Vladi, poverenik podseća da je prošlo pet i po godina od usvajanja Strategije, a ne postoji posebno radno telo, ni akcioni plan, ni uredba o zaštiti naročito osetljivih podataka. Izvor: ***Dnevni list „Blic***“, od 18.02.2016.godine (glavni i odgovorni urednik M. Stjepanović), str. 11.

- Ljudski faktor sa atributom nenamernosti, i
- Ljudski faktor sa atributom namernosti.

Ciljevi zaštite su sprečavanje ugrožavanja, otkrivanje ugrožavanja, dejstvovanje u slučaju nastanka ugrožavanja i otklanjanje posledica ugrožavanja. Da bi ispunila postavljene ciljeve, zaštita mora biti planirana, projektovana i realizovana sveobuhvatno, organizovano, stručno i racionalno. Zaštita je onoliko jaka koliko je jaka najslabija karika u njoj!

Polazni elementi pri uvođenju zaštite su odgovori na sledeća pitanja:

- Šta štititi?
- Od koga ili čega štititi?
- Zbog čega štititi?
- Čime štititi? i
- Kako štititi?

Vlade mnogih zemalja, kao i brojne profesionalne i komercijalne organizacije, asocijacije i institucije ulagale su i ulažu velike napore u cilju razrešavanja problema zaštite automatizovanih informacionih sistema. U oblasti zaštite informacionih sistema vredna pažnje na međunarodnom planu je svakako i aktivnost Organizacije za ekonomsku saradnju i razvoj OECD (Organisation for Economic Cooperation and Development) i Saveta Evrope. Izveštaj The British Younger Commission Report donet 1972. godine, jedan je od značajnijh i predstavlja bazu na koju su se oslonili mnogi nacionalni zakoni i medjunarodna akta. On predlaže usvajanje deset principa pri zaštiti podataka:

- Informacije se mogu koristiti samo sa unapred utvrđenom svrhom;
- Pristup informacijama treba ograničiti samo na one koji imaju ovlašćenja da ih koriste za ono za šta su namenjene;
- Za zadovoljenje odredjene svrhe (potrebe) prikupiće se minimalan broj podataka koji je dovoljan da se realizuje postavljeni zahtev;
- U kompjuterskim sistemima moraju se odvojiti identifikacioni od ostalih podataka;
- Informacije moraju biti tako sređene da se problem može izložiti kroz informacije koje se na njega odnose;
- Izabrani nivo zaštite mora biti prilagođen potrebama i zahtevima korisnika;
- Sistem kontrole mora da obezbedi otkrivanje bilo kakve povrede sigurnosti;
- Moraju se definisati periodi posle kojih se informacija neće koristiti;
- Sadržaj podataka mora biti ažuran i tačan;
- Sistem vrednovanja odluka, presuda, koji podrazumeva pravo žalbe subjekta podataka ukoliko vlasnik BP prekorači svoja ovlašćenja.

Ujedinjene nacije su donele Smernice u vezi baza podataka informacionih sistema u kojima se utvrđuje deset osnovnih principa koje svaka zemlja treba da obezbedi u nacionalnom zakonodavstvu:

- Zakonitost i nepristrasnost;
- Tačnost;
- Postojanje tačno utvrđene svrhe;
- Dostupnost;
- Neizdvajanje, nediskriminacija;
- Posebno odobrenje za izuzimanje;
- Zaštita;
- Nadzor i sankcije;
- Uređivanje prekograničnog protoka;
- Oblast primene.

Zaštita podataka koju policija preduzima obuhvata:

- ***Privatnost:*** i to kao privatnost korisnika i privatnost subjekta podataka, a obuhvata privatnost pristupanja u sistem, privatnost govora, privatnost podataka, privatnost korisnikove lokacije i identifikacije, kao i privatnost finansijskih transakcija.
- ***Sigurnost podataka***: obuhvata obezbeđenje podataka od slučajnog ili namernog otkrivanja neovlašćenim licima, kao i zaštitu od neovlašćenog menjanja, brisanja, i korišćenja od strane ovlašćenih korisnika ili celokupnog gubitka.
- ***Poverljivost podataka***: pretpostavlja da se poverljivi podaci ne smeju otkriti od strane neautorizovanih pojedinaca i drugih entiteta, ili u neovlaštenim procesima. Kad su u pitanju mreže proverljivost postaje veliki problem u "saobraćaju" podataka obuhvatajući i frekvencije, izvor, destinacije...
- ***Raspoloživost podataka***: pretpostavlja da samo ovlašćeni korisnik može blagovremeno doći do podataka, bez barijera.
- ***Integritet:*** obuhvata integritet podataka, integritet izvora, i tačnost.

4.2. Zaštita privatnosti

Informaciona tehnologija[592] koju primenjuje MUP-policija, ima zadatak da prikupi, obradi, memoriše i distribuira ogromnu količinu podataka i informacija, od kojih se veliki deo odnosi na podatke o ličnosti. Ovim je problem privatnosti dobio sasvim nove dimenzije, pa je dijagnoza pravnika gotovo svuda ista: u automatizovanom ambijentu privatnost pojedinaca je ozbiljno ugrožena i potreban je odgovarajući sistem zaštite. Privatnost je jedno od osnovnih ljudskih prava i kao takvo odnosi se na ona prava koja su vezana za ličnost čoveka, kojima se obezbeđuje integritet i dignitet ljudskoj ličnosti i koja zahtevaju očuvanje tajnosti i slobode privatnog života. Od brojnih koncepcija najtipičnija i najprihvaćenija je koncepcija, po kojoj privatnost podrazumeva pravo pojedinaca, da sami odrede obim ličnih informacija koje žele da dele sa drugima. Ona uključuje njihovo pravo da kontrolišu prikupljanje, memorisanje i

[592] Zakon o zaštiti podataka o ličnosti, „Službeni glasnik RS“, br. 97/2008, 104/2009, i 68//2012. članovi 46-52.

diseminaciju njihovih podataka ili informacija o njima samim. Ovaj vid privatnosti dobija i posebno ime-informaciona privatnost (*information privacy*). Ovakav koncept priznaje pravo pojedincima da odobravaju i kontrolišu prikupljanje i korišćenje podataka o njima samim. Naravno, ovo pravo nije apsolutno i može, u strogo predviđenim slučajevima i okolnostima, od strane unapred određenih subjekata, biti „narušeno“. S druge strane, pravo na informacionu privatnost predstavlja kompleksno pravo koje obuhvata:

- Pravo na obaveštenost;
- Pravo na odgovarajuće korišćenje podataka;
- Pravo pristupa i uvida;
- Pravo ispravke;
- Pravo na pravna sredstva.

OECD je izdao Smernice za zaštitu privatnosti i međunarodnih tokova ličnih podataka. Smernice su bazirane na osam osnovnih principa namenjenih za nacionalnu upotrebu:

- **Princip limitiranog prikupljanja podataka**
  Podrazumeva da mora da postoji ograničenje za prikupljanje ličnih podataka i da svi takvi podaci moraju biti dobijeni na zakonit i ispravan način i, gde je moguće, sa znanjem i pristankom subjekta na kojeg se podaci odnose.
- **Princip kvaliteta podataka**
  Podaci o ličnosti moraju biti relevantni za potrebe za koje se prikupljaju i u obimu neophodnom za te potrebe i moraju biti tačni, kompletni i ažurni.
- **Princip specificiranja potreba**
  Potrebe zbog kojih se podaci o ličnosti prikupljaju moraju biti specificirane pre prikupljanja samih podataka, a njihovo kasnije korišćenje ograničeno samo na zadovoljenje specificiranih potreba ili potreba koje nisu inkompatibilne sa specificiranim.
- **Princip ograničenog korišćenja**
  Podaci o ličnosti ne bi smeli biti obelodanjeni, raspoloživi ili korišćeni za druge potrebe koje nisu specificirane u skladu sa prethodnim principom, izuzev uz saglasnost subjekta ili na osnovu zakonskih ovlašćenja.
- **Princip zaštite**
  Podaci o ličnosti moraju biti zaštićeni razumnim merama od rizika gubitka, neovlašćenog pristupa, destrukcije, korišćenja, modifikacije ili obelodanjivanja.
- **Princip otvorenosti**
  Mora da postoji generalna politika otvorenosti razvoja, prakse i politike u odnosu na lične podatke. Načini uspostavljanja i utvrđivanja prirode ličnih podataka i glavne svrhe njihovog korišćenja bi morali biti raspoloživi, kao i mesto i uloga kontrolora podataka.
- **Princip individualne participacije**
  Pojedinac treba da ima pravo:
  - da dobije potvrdu (dokaz) da li se o njemu vode neki podaci;

- da može da komunicira sa odgovornim licem u vezi sa podacima koji se odnose na njega;
- da mu se daju razlozi ukoliko su njegovi zahtevi u vezi prethodnog odbijeni, kao i da mu se omogući da osporava takvu odluku;
- da osporava podatke koji se odnose na njega i ukoliko se zadovolji njegovom zahtevu – da se podaci izbrišu, odbace, dopune ili izmene.

1. **Princip odgovornosti**

Podrazumeva odgovornost kontrolora podataka za poštovanje navedenih principa.
Cilj ovih smernica je, s jedne strane, zaštita fundamentalnih ljudskih prava, kao što su zaštita od nezakonitog prikupljanja ličnih podataka, čuvanja netačnih ličnih podataka, zloupotrebe ili neovlašćenog obelodanjivanja takvih podataka, i s druge strane, otklanjanje ili umanje opasnosti da razlike u nacionalnim zakonodavstvima budu prepreka slobodnim prekograničnim tokovima ovakvih podataka.

4.3. Mere zaštite

Za razvijanje adekvatnog celovitog i pouzdanog sistema zaštite IS i podataka potrebno je izvršti identifikaciju svih mera koje stoje na raspolaganju. Sve te mere, po svojim prirodnim svojstvima koja ih karakterišu, mogu se razvrstati na sledeći način: *normativne; fizičko-tehničke; logičke; i kriptološke.*

Ovakva klasifikacija raspoloživih mera omogućava navođenje njihovih, sa stanovišta efikasnosti i troškova, najbitnijih karakteristika, koje mogu poslužiti kao vrlo pouzdani kriterijumi prilikom njihovog izbora.

Mere normativnog karaktera, u koje spadaju pravne mere, organizacione mere i kadrovske mere, pripadaju kategoriji netehničkih mera. Osnovna karakteristika ovih mera je da ne degradiraju rad sistema, već naprotiv, znatno doprinose povećanju njegove raspoloživosti i produktivnosti, a istovremeno značajno utiču na efikasnost sistema zaštite. Njihovom realizacijom stvara se „temelj“ na koji će se, primenom fizičko-tehničkih, logičkih i kriptoloških mera, nadograđivati sistem zaštite do konačne finalizacije.

Fizičko-tehničke mere mogu biti vrlo efikasne za određene probleme zaštite, ali isto tako povlače za sobom i znatne troškove. Njihova zajednička karakteristika je da uslovljavaju finansijske investicije pre nego što počnu da dejstvuju. Pozitivna strana se ogleda u činjenici da se svi ovakvi troškovi mogu tačno proceniti i izbor planski podesiti raspoloživim finansijskim mogućnostima. Ono što svakako treba imati u vidu je činjenica da efikasnost ovih mera značajno opada u ambijentu u kojem normativne mere nisu primenjene na adekvatan način.

Logičke mere za ne mali broj problema zaštite automatizovanih informacionih sistema predstavljaju jedino, ali i vrlo snažno sredstvo. Visok stepen efikasnosti se prvenstveno postiže korišćenjem logičkih mera „u paketu“. S druge strane, ove mere povlače za sobom tzv. „nevidljive“ (prikrivene) troškove, jer direktno utiču na smanjenje raspoloživosti i efikasnosti računarskog sistema.

Kriptološke mere zaštite omogućavaju ostvarivanje najvišeg mogućeg nivoa zaštite. Međutim, ove mere, kao i bilo koje druge, jesu potrebne, ali i pored mogućnosti zadovoljenja širokog spektra zahteva za zaštitom informacionih sistema, one nisu i dovoljne da samostalno obezbede potrebnu zaštitu. Razlog je u činjenici da efikasnost i ovih mera značajno opada u ambijentu u kojem normativne mere nisu primenjene na adekvatan način.

Iz izloženog se jasno nameće zaključak da bi kod izbora mera zaštite nesumnjivu prednost trebalo dati merama normativnog karaktera. Od njih bi trebalo početi, maksimalno ih iskoristiti i sa njima bi trebalo prekriti ceo informacioni sistem, nezavisno od nivoa zaštite koji se zahteva. Takvo stanje bi trebalo dograditi fizičko-tehničkim i logičkim merama zaštite u meri koja će obezbediti željeni nivo zaštite, koji može biti, na primer, standardni ili srednji, a za viši ili najviši nivo, zavisno od potreba konkretnog informacionog sistema, trebalo bi zaštitu ojačati kriptološkim merama i merama zaštite od kompromitujućeg elektromagnetnog zračenja.

5. Zaključak

Potpuna depolitizacija policije, transparentan nastavak reforme policije, i uspostavljanje delotvornog sistema spoljašnje, a tako i unutrašnje kontrole, ključni su preduslovi za dalji razvoj i izgradnju novog modela odnosa policije i građana. Potrebno je konačno prevazići tradicionalno shvatanje koncepta bezbednosti, gde je policija dugo bila primarni (glavni) činilac bezbednosti. Kroz dalje procese tranzicije, nameće se potreba za uspostavljanjem odgovarajućih odnosa između policije, građana i javnosti u najširem smislu. Razmena informacija, saradnja i međusobna pomoć, kao i odnosi poverenja i korektnosti između ovih subjekata, obezbediće bolji pristup u međusobnim odnosima, a u interesu opšte bezbednosti i zaštite prava građana i imovine.

Postoje i značajni sistemski, zakonski i profesionalni izazovi za uspostavljanje ove saradnje. Za značajno uspostavljanje i unapređenje partnerstva u ovoj oblasti, potrebno je izgraditi odgovarajući podzakonski okvir. Nesumnjivo je, da na ovom putu komparativni pristup i primeri najbolje prakse, mogu biti od koristi prilikom koncipiranja strateške politike u ovoj oblasti, a partnerstvo policije i građana, bi vodilo uspostavljanju jakog sistema integralne bezbednosti.

Ovim radom smo pokušali ukratko pojasniti osnove odnosa javnosti i policije, neke pretpostavke dobrih odnosa policije i građana, kao i obavezu policije u zaštiti ličnih podataka i privatnosti građana. Osnovne zakonske pretpostavke su date, a daljim jačanjem integriteta policije i ostvarivanje strateške funkcije policije, mogu se graditi i unapređivati novi modeli odnosa i saradnje policije, građana, javnosti i ostalih subjekata bezbednosti u društvu.

LITERATURA

Daničić, M. Stajić, Lj. (2008). Fizičko obezbeđenje. U: Mitrović, LJ. (ur.) *Privatna bezbjednost*. Banja Luka: Visoka škola unutrašnjih poslova, 89-116.
Jovanović, D. (2001). *Policajac i bonton*. Beograd: autorsko izdanje, „Print graphic trade D.O.O.“.
Kaurin, T. Anucojić, D. (2011). *Zaštita informacionih sistema i podataka*. Novi Sad: Fakultet za pravne i poslovne studije, dr Lazar Vrkatić.
Kešetović, Ž. (2000). „Odnos policije i javnosti“. *Časopis Bezbednost*, br. 5-6, Beograd: MUP Republike Srbije, 522-534.
Krstić, O. (2007). *Prevencija kriminaliteta*, Banja Luka: Fakultet za bezbjednost i zaštitu.
Krivični zakonik, „Službeni glasnik RS”, broj 85/2005, 88/2005.
Kodeks policijske etike, „Službeni glasnik RS”, broj 92/2006.
Lilic, S. Prlja, D. (2008). *Pravna informatika veština – Internet za pravnike*, Beograd: Dosije.
Milosavljević, B. (1997). Pregled istorijskog razvoja policije na području Jugoslavije. U: Stajić, Lj. (ur.) *Nauka o policiji*, Beograd: Policijska akademija, 91-122.
Pilipović, V. (2009). Doktorska disertacija, tema: *Policijska funkcija u procesu reformi političkog sistema Srbije,* Fakultet političkih nauka, Beograd: autorsko izdanje, 178-197.
Strategija nacionalne bezbednosti (2009), Poglavlje III-V.,Vlada R.Srbije, Beograd, 13-33.
Strategija policije u zajednici, br. 05/021-1082/2013-003.,Vlada R. Srbije, Beograd.
Strategija zaštite podataka o ličnosti, br. 05/021-5864/2010.,Vlada R.Srbije, Beograd.
Unijat, J. (ur.), (2008), Ključni nalazi istraživanja i preporuke (I). *Privatne bezbednosne kompanije u Srbiji – prijatelj ili pretnja?*. Beograd: Centar za civilno vojne odnose, 8-26.
Uputstvo o osnovnim standardima u postupanju sa medijima, 01 br. 2134/2006. Beograd: MUP Republike Srbije
Uputstvo za objavljivanje informatora o radu državnih organa, „Službeni glasnik RS, br. 57/2006.
Zakon o državnoj upravi, „Službeni glasnik RS“, broj 79/2005., 101/2007., 95/2010.
Zakon o ministarstvima, „Službeni glasnik RS“, broj 65/2008. 36/2009, 73/2010.
Zakon o slobodnom pristupu informacijama od javnog značaja, „Službeni glasnik RS“, br. 120/2004, 54/2007.
Zakon o zaštiti podataka o ličnosti, „Službeni glasnik RS“, br. 97/2008, 104/2009, i 68//2012.
Zakon o policiji, „Službeni glasnik RS“, broj 06/2016.

Internetski izvori

http://www.blic.rs/vesti
http://www.b92.net/info/vesti.
http://www.mup.gov.rs/vesti
www.novilist.hr/vijesti/

Vojin Pilipović
Tanja Kaurin

RELEASE THE POLICING AND PROTECTION OF PERSONAL DATA

Summary

This paper discusses about basic problems (issues) of legal and ethical nature, which are important for the publicity of police work and the protection of personal data, which is part of the basic human right to privacy. Constitutional and legal protection of human rights and fundamental freedoms implies that everyone has the right to do so, to respect for his private and family life, home and correspondence, and that the public authorities (the police) will not interfere with the exercise of this right. This right may be restricted by law, and when necessary in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. The citizen, as an active participant in social and democratic processes, but also the subject of the right to protection of personal data, must be adequately informed of their rights, ways of exercising, as well as the mechanisms of legal protection. In all communications, the police and the public (internet pages, written statements, available materials and the like.), the right of citizens to privacy, must be protected in accordance with applicable standards and the system of personal data protection.

Keywords: *citizen, police, property rights, transparency, personal data.*

STRUČNI RAD

Ljubo Pejanović[593]

PRETNJE I ZAŠTITA INFORMACIONOG SISTEMA

Sažetak

Ovim radom se želi ukazati na pretnje, opasnosti i posledice, po bezbednost računarsko-informacionog sistema, zatim metode i oblike pretnji i posledica po sistem, podataka i bezbednost vlasnika računara. Između većeg broja pretnji računarskom sistemo, posebna pažnja posvećena je virusima i virusnom sistemu, kao i pretnjama pljačkom i drugim oblicima kriminaliteta sa osvrtom na izvršioce protivzakonitih delovanja, među kojima su i hakeri. Zatim se posvetila pažnja, problemima ostvarenja bezbednosti računarskih sistema i zaštiti istih.

Ključne reči: *računari, sistem, pretnja, bezbednost, zaštita.*

1. U V O D N E N A P O M E N E

Rad pod predmetnim naslovom predstavlja kombinaciju definicija citata i orginalnog rada, stečenog drugogodišnjim iskustvima autora u bezbednosnoj praksi i nauci na visokoobrazovnim institucijama. U radu su predstavljene i dokazane postavljene predpostavke preko odgovarajućih hipoteza o značaju računarsko-informacionih sistema, njihovoj rasprostranjenosti i mogućnosti komunikacije, sadržaju sistema i lagerovanju podataka. Pored ukazanog značaja i mogućnosti ovog sistema, ukazani su i navedeni mogući problemi i pretnje kojima se vrše pljačke, promene podataka, razaranje sistema i u ništenje računara. Isto tako se ukazuje na mogućnost i nemogućnost društva u ostvarenju bezbednosti ovih sistema i metoda delovanja bezbednosnih institucija i ljudi koji su vlasnici i nosioci ovih sistema. Da bi se ostvarila bezbednost računarima, ukazuje se na teškoće i nemogućnosti suprostavljanja i obezbeđenja adekvatnih odgovora kriminalnim pretnjama od strane institucija koje obezbeđuju zaštitu računarskim sistemima u prostoru Međunarodne zajednice.

1.1. Problem i predmet ugrožavanja računarskog sistema

Ovim radom se obrađuje predpostavljeni problem i hipoteza, putem koje se želi ostvariti krajnji cilj da se ukaže na saznanja preko predpostavke o mogućim pretnjama i opasnostima i rizicima, kao i zaštiti informacionog sistema od istog. Postavljeni cilj istraživanja ugroženosti i zaštite informacionog sistema, koji je upravo postao stalna meta napada i delovanja pojedinaca i kriminalnih i terorističkih grupa, koji žele naneti štetu ili

[593] Prof. dr. Ljubo Pejanović, vanredni profesor, Fakultet za pravne i poslovne studije dr Lazar Vrkatić Novi Sad, e-mail: pejanovicljubo@gmail.com

ostvariti protivzakonitu korist za pojedinca ili grupu. Te u ovom slučaju, hipoteza ovog problema je predpostavka, tj nagađanje, domišljanje, osnovica, ili zamisao koji se uzima kao instinkt putem kojeg bi se na osnovu nje premostila neznanje o stvarnosti koja predstavlja problem svim društvima na planeti. U ovom slučaju, naše neznanje se posmatra kao neznanica i novi, savremeni i veoma veliki problem po bezbednost informacionog sistema stoga što se ne posvećuje tolika pažnja izučavanju ovog problema savremene dobi, tako i kompjuterske adekvatne zaštite. „Hipoteza o bezbednosti, kao i svaka hipoteza uopšte ima svoje izvore saznanja. Izvori hipoteze o bezbednosti, obično su: 1. teorija o pojavi, stvaranju i razaranju bezbednosti, u ovom slučaju kompjuterskog sistema; 2. iskustvo iztraživača bezbednosnih pojava, odnosa i procesa u istraživanju ugroženosti sistema; 3. rezultati istraživanja i hipoteze drugih naučnih disciplina iz oblasti društvenih nauka; 4. kritički ili naučni odnos prema iskustvima saznanja, činjenicama odnosno dosledno izvedena objektivnost bezbednosnih podataka i informacija“ (Unčanin, 2009, 272-273). Stim u vezi, informacioni sistem je organizovani sistem koji je sadržan od tehnologije, tehničke opreme (računara i prateće opreme), informacionog sistema sa konpletnim programom, sadržajem ogromnog broja podataka kako tajnih, odnosno zaštićenih tako i drugih, znanja i veština rukovanja istim, zaštitnih mera, radnji i aktivnosti, napajanja električnom energijom i drugim potrebama i sadržajima. Istraživanjem ovog problema obuhvata se i radnje rukovanja sa tehnikom i kompjuterskim sistemom.

Ako sagledamo celinu sadržaja informacionog sistema, isti je programski sadržajan sa više njegovih podsistema i celina koje su osetljive na mnoge oblike pretnji i ugrožavanja i rizika. Informacioni sistem je između mnogih oblika ugrožavanja osetljiv u potpunosti na svaku pretnju, za neke pretnje je zaštićen, a za neke nije. Između većeg broja oblika pretnje, sistem je osetljiv između ostalih i na: osetljivost na električne instalacije, osetljiv je na fizičke pretnje, osetljiv je krađe podastaka, novca, pljačke, terorizam, zatim je osetljiv na elektronske viruse i druge pretnje.

Dakle, mnogobrojni su oblici i pretnje, a time i rizici računarskom sistemu, a imajući u vidu ograničenost ovog rada, mi se osvrćemo na neke od navedenih pretnji informacionom ili računarskom sistemu. Pretnje računarskom sistemu su velike, između kojih je jedan od najopasnijih pretnji - virus „Flame“. U pitanju je malware modularnog tipa (takođe poznat kao i Skywiper) otkriven 2012. godine. Ovaj virus je napadao windows i korišćen je u špijunske svrhe naručito na Bliskom istoku.“[594] Pored ovog, postoje i mnogi noviji virusi koji mogu razoriti kompjuterski sistem.

Drugo, „35 hakera pokušalo je upasti i omesti bezbednost sistema SAD. Rečeno im je da su u ulozi hakera i da su unajmljeni od strane Severne Koreje i da im je primarni cilj Pacifička komanda SAD na Havajima.“[595]

„Postoji računarski virus koji sadržava instrukcije, naknadno ubačene u regularni program, sa ciljem da postojeće programe i podatke na računaru izmene ili potpuno unište. Za izradu

[594] http://liat25.com/25-biggest.cuber-attaks-in-history/?view=all
[595] Dan Verton, Crni led: nevidljiva pretnja sajberterora, Nev York, 2003.

virusa neophodna je veština u programiranju i poznavanje ciljnih sistema da bi se direktno ili indirektno izmenio računarski program. Najčuveniji metod napada, *virus,* dobio je ime po sposobnosti programa da se prikači („inficira“) za druge računarske programe, navodeći ih da i sami stvaraju viruse. Aktivira se veoma jednostavnim učitavanjem, odnosno presnimavanjem na računaru „zaraženog“ programa ili podataka. Može da se širi kroz računarski sistem vrlo brzo. Zbog masovnog korišćenja telekomunikacijonih veza i interneta, virusi mogu da se prošire na mnoge organizacije širom sveta. Neki od najzloglašenijih virosa su „međunarodni“ *virusi:* Mikelanđelo, Pakistanski mozaik i Jerusalim. Zaštitu od virusa pružaju antivirus programi.“ (Ivančević, 2009, 813-814).

S tim u vezi, kriminalci ili kriminalno-terorističke skupine ubacivanjem virusa u računarski sistem, predstavljaju veliku pretnju kako uništenja sistema u celini ili njegovog dela, promenom podataka i njegovog sadržaja, ubacivanjem podataka koji menjaju ceo sistem, vrše pljačku novčanih vrednosti i na kraju uništavaju sistem delimično ili potpuno. Pored uništenja sistema i pljačke, navedene skupine predstavljaju pretnju i životima kod ljudi. Preko računarskog sistema pretnja ljudima može biti ispoljena ugrožavanju zdravlja pa i života. Kriminalci ili teroristi pribegavaju metodama ubijanja ljudi preko računarskog sistema, što im menjaju terapiju ako su na lečenju, a time često i ubistvo. Promenom terapije vrši se ugrožavanje zdravlja, a često i života kod ljudi. Ubacivanjem virusnih sistema, može doći do paljevina, pa i neke vrste eksplozija, čime se ugrožavaju i životi i zdravlje kod ljudi. Prema tome, sa aspekta *bezbednosti*, ovaj vid savremenog oblika pretnje, vrši se drastično ugrožavnje ljudske bezbednosti, bezbednosti imovine, bezbednost života i nameće se psihička patnja, strah, panika i slično, usled čega dolazi i do drugih pretnji preko psihičkih i zdrastvenih posledica. Što se tiče *pravne* pretnje, u ovom slučaju se čine krivična dela kojim se ugrožavaju računarski sistemi, vrše pljačke, uništavaju se podaci i tehnička oprema, a time zdravlje i životi ljudi preko psihičkog stresa, patnje i bola zbog gubitka finansijskih sredstava, gubitka opreme, podataka i drugih vrednosti. Kad se govori o *zaštiti* računarskog sistema, takođe se pojavljuju problemi i teškoće u zaštiti ovog sistema u nedostatku adekvatnih i sigurnosnih sistema tehničke zaštite, zbog čega dolazi do uništenja vrednosti u računarskom sistemu, Zatim se pojavljuju problemi zbog malog broja stručnjaka koji se mogu adekvatno i blagovremeno suprostaviti kriminalnom delovanju. Na kraju često se problem rešava istragom, pronalaženjem i dokazivanjem kriminalnih radnji, pronalaženje izvršioca i njihovo sankcionisanje. Stim u vezi se ukazuje na problem prevencije i njeni nedostaci u blagovremenom otkrivanju i time sprečavanju izvršenja krivičnih i kriminalni aktivnosti.

Dakle, „ugrožavajuća delatnost u pravnom smislu je krivično delo sa manjom društvenom opasnošću i prekršaji činjenjem rušilačke delatnosti..., tj one aktivnosti kojima se napadaju osnovne vrednosti, koje čine organizovane skupine radi rušenja ... računarskog sistema.“ (Đorđević, 1986, 392-393). Prema tome, ugrožavajuća hakerska i druga delatnost od strane destruktivnih pojedinaca ili skupina u čestim slučajevima postala je profesije ili zanimanje. Iako se radi o protivzakonitoj aktivnosti, činioci navedenih dela pribegavaju ovoj vrsti delovanja, kako bi se na lak način bez teškog rada obogatili ili na ovaj način ugrozili nekog ili neku instituciju. Svaka vrsta ove delatnosti predstavlja pre svega krivično delo,

zatim pretnju i opasnost po bezbednost računarskog sistema i njegovih vlasnika, a time se nameću posledice koje mogu biti katastrofalne, velike ili retko manjeg značaja.

1.1.1. Hakeri kao pretnja računarskom sistemu

Između većeg broja kriminalnih radnji je hakerska delatnost, pomoću koje se vrši pre svega pretnja, a zatim i opasnost po bezbednost računarskog odnosno informacionog sistema, i na kraju posledice po sistem i njegovog vlasnika. Sistemi su ugroženi od neželjenih radnji koje čine kriminalci, teroristi ili kriminalno-terorističke skupine radi nanošenja straha, panike, štete pa i bezbednosti zdravlja i života kod ljudi. S tim u vezi, „haker je osoba koja ilegalno ili neetički način pristupa tuđem računarskom sistemu. Lice van sistema koji najčešće putem komunikacionih linija, bez potrebnih ovlašćenja pristupa računarskom sistemu: zlonamerno haker može biti ozbiljan problem kompaniji. Nakon pristupa sistemu haker može neovlašćeno menjati podatke ili, koristeći tehniku programiranja, može direktno ili indirektno izmeniti računarske programe. Da bi neko bio haker neophodno je da poseduje veštine i znanja u programiranju, ali i da poznaje ciljne sisteme.“ (Ivančević, 2009, 266-267).

Hakerskom delatnosti bave se i pojedinci ili grupe koje nisu ili ne pripadaju organizovanim kriminalnim grupama, već to čine u cilju sticanja neke koristi bilo da je u pitanju finansijska, materijalna ili druga korist. Zatim pristupaju nelegalnim aktivnostima radi činjenja materijalne ili druge štete onome čiji je sistem ili nekom za koga služi taj računarski sistem sa ciljem osvete i nanošenja bola, patnje i psihičkog stresa. Navedeni izvršioci ove vrste kriminalnih dela, iako ne pripadaju kriminalno-terorističkim skupinama, oni čine protivzakonite radnje i aktivnosti preko kojih postaju kriminalna grupa, jer ugrožavaju bezbednost. Kad su u pitanju pojedinci ili kriminalne grupe koje u svojim sastavima imaju profesionalne „hakere“ čije znanje i veštine dostižu visoki stepen intelengencije, pri čemu upadaju u sisteme sa najvećom i najnovijom bezbednosnom zaštitum koji probijaju i ostvaruju svoje ciljeve. Najčešći ciljevi kriminalnih grupa i njihovih predstavnika u hakerskim aktivnostima je napad i upadanje u računarske sisteme, kako bi izvršili *pljačku* novčanih vrednosti i na kraju uništenje sistema. Ova vrsta pljački najčešće se dešava napadom na računarske sisteme banaka zbog postojanosti ogromne količine novčanih vrednosti u ovim ustanovama. Nisu retki slučajevi da u ove sisteme napadaju kriminalci u vlasništvu drugih institucija u cilju pljački ili skidanja zaštićenih podataka koji bi poslužili grupi za ostvarenje drugih ciljeva. Često se dešavaju ove aktivnosti i pri obračunu između kriminalnih grupa, koje takođe štite svoje odabrane lokacije ili napadaju lokacije koje kontrolišu njihovi rivali na tržištu kriminaliteta. Kad se radi o terotrističkim grupacijama, takođe se vrše napadi i pretnje na računarske sisteme sa ciljem pljački novčanih ili drugih vrednosti, kao i uništenje zaštićenih podataka ili drugih vrednosnih ponadaka političkim protivnicima ili neistomišljenicima. Terorističke grupe preko svojih hakera, vrše pretnju, strah i paniku napadima na računarske sisteme državnih institucija sa ciljem njihovog uništenja, izazivanja panike i straha kod državnih institucija protiv koji se bore terorističke grupe. Česti su napadi usled nacionalističkih, separatističkih i religijskih motiva napadima na sisteme u cilju nanošenja štete i posledica protivničkim snagama, narodima i državama. Sve su to pretnje napadima na računarsko-informacione sisteme, motivisani sticanjem finansijske i druge koristi, kriminalnih obračuna i terorističkih aktivnosti koje predstavljaju čestu pretnju, izazivaju opasnost i time nanose nesagledive posledice po žrtvu hakerskih napada.

2. PREVENCIJA, ZAŠTITA I OSTVARENJE BEZBEDNOSTI RAČUNARSKO-INFORMACIONOG SISTEMA

Obzirom da je računarski ili informacioni sistem društva, državnih institucija, pravnih lica i pojedinaca postao česta meta napada od strane pojedinaca, grupa i kriminalnih organizacija. Ovim je računarsko-informacioni sistem postao drastično ugrožen. Metode, radnje i aktivnosti napada na računarski sistem su kvalitetno organizovane, stručno usavršene, precizno primenjene i na kraju efikasno ispunjene odnosno ostvarene. Dakle, bezbednost i zaštita informacionog sistema u ovim uslovima je teško ostvarljiva, često neefikasna i ređe potpuno ostvarljiva. S tim u vezi, „bezbednosne mere, predstavljaju skup aktivnosti i radnji koje preduzimaju politička tela, organizacije i državni organi radi ostvarivanja zaštite datih društvenih vrednosti.“ (Đorđević, op.cit., 24-25). Shodno navedenoj definiciji, bezbednost računarskog sistema podrazumeva objektivnost unutrašnje i spoljne sigurnosti i zaštita materijalnih dobara u ovom slučaju računarskog sistema od neoružanih izazova, rizika i pretnji. Te u tom smislu, postoji više sektora bezbednosti, preko kojih se štiti sistem. „Ostvarenje bezbednosti podrazumeva eliminisanje svih negativnih pojava koje ugrožavaju računarski sistem spoljneg i unutražnjeg oblika ugrožavanja. Ukoliko se eliminišu sve pretnje, stvaraju se uslovi bezbednosti računarskog sistema. (Pejanović, Bejatović, 2015, 56-57). Prema tome bezbednost računarskog sistema je stanje u kojem ne postoje pretnje ili su iste eliminisane i računarski sistem je bezbedan. Bezbednost računarskog sistema ostvaruju stručne institucije društva, vojna i policijska na unutrašnjem planu, vojni i policijski organi, kao i proizvođači zaštitnog sistema spoljnjeg karaktera, tajna i javna, bezbednost, kao i korisnik sistema. Kad su u pitanju zaštitni subjekti, u Republici Srbiji su vojno-bezbednosni organi i privatne institucije „bezbednosti i samozaštite.“ Što se tiče bezbednosti podataka u računarskom sistemu podrazumeva se organizacija svih subjekata bezbednosti u zaštiti društvenih sistema, kao i drugih pravnih lica, a građani samostalno vrše zaštitu svojih sistema. Dakle, „bezbednost podataka, podrazumeva zaštitu podataka od njegovog slučajnog ili namernog otkrivanja neovlašćenim osobama ili neovlašćenih izmena ili uništenja. Funkcija obezbeđenja podataka sprovodi se kroz operativne sistema; programe za kontrolu pristupa; proizvode za razmenu podataka/baze podataka; procedure za pravljenje rezervne (sekundarne) kopije orginalnih (primarnih) podataka i za njihovo obavljanje; aplikativne programe spoljašne kontrole procedure. Bezbednost podataka trebalo bi da se zasniva na dva osnovna principa: princip minimalne previlegije (korisniku treba staviti na raspolaganje samo informaciju neophodne da bi obavio zadatke koje mu je poveren) i principu minimalne izloženosti (samo osobe čije dužnosti za to zahtevaju mogu da saznaju informacije dok se obrađuje pohranjuje ili prenosi.“ (Ivančević, op.cit., 74-75). Međutim, pod zaštitom informacionog sistema i podataka smatra se, „zaštita tajnih podataka, primena metoda, mera, radnji i postupaka od službi bezbednosti, radi tajne zaštite tajnih podataka koji su označeni kao državna, službena,, vojna i poslovna tajna...“. (Đorđević, op.cit., 428-429). S tim u vezi, informacioni sistem je podhranjen svim vrstama podataka između kojih su: vojna tajna, državna tajna, službena tajna, interna tajna i drugi podaci koji nisu tajna i oni se štite od napada. Dakle, zaštita informacionog sistema i svih podataka u njegovom sadržaju predstavlja, preduzimanje odgovarajućih metoda, radnji i aktivnosti, koje preduzimaju

bezbednosni subjekti i pojedinci u cilju eliminacije svake pretnje i njeno sprečavanje da ne bude nametnuta. Stim u vezi, „Ciljevi ustanove, su ustanove pre svega zadovoljenje potreba i zahteva, kupca, odnosno korisnika usluge. Ustanova ima za cilj da proizvodi dobra koja služe za zadovoljenje potreba pojedinaca, članova društva, čime se ostvaruje potreba društva (Unčanin, 2009, 112-113).

3. Z A K LJ U Č A K

Računarsko-informacioni sistem jedan je on savremenih sistema koji je pronašao svoje mestu na celokupnom prostoru međunarodne zajednice. Sistem je ušao u svaki dom, svaku instituciju i kod najvećeg broja građana u međunarodnoj zajednici. Zbog svog kapaciteta, značaja i kvaliteta predstavlja neophodnost za ostvarenje savremenog načina poslovanja, komunikacije i lagerovanja podataka. Zbog svog značaja za svakog korisnika, neki pojedinci, grupe i organizacije pribegli su ugrožavanju istog sa svim mogućim metodama i oblicima pretnji, kako uništavanjem podataka, uništavanjem sistema i promene podataka, tako pljačke i nanošenja pretnji ljudima i njihovoj imovini, kao i pretnji državi i njenim institucijama. Savremene pretnje su višestruke, između kojih su najčešće, ilegalna ugradnja "*virusa*" odnosno virusnih sistema kojim se razaraju podaci, sistem i računarska mreža. Dakle, ako uzmemo u razmatranje i time zaključivanje u vezi zaštite i ostvarenja bezbednosti računarskim sistemima, jedan je od najvećih problema svih država i institucija u međunarodnoj zajednici. Koliko tehničke institucije uspevaju u izradi tehnuičkih i bezbednosnih sistema sa kojima se štite računari, toliko u korak ih prate kriminalne grupe, koje uspevaju da pronađu nove virusne sisteme koji poništavaju zaštitu. Jedan od velikih promlema je što neke proizvodne institucije koje izrađuju zaštitne sisteme, istovremeno izrađuju i njihovo poništavanje ili narušavanje, kako bih ponovo prodavali zaštitne sisteme. Na kraju se stiče utisak i zaključak, da su računarski sistemi bili ugroženi, ugroženi su i biće ugroženi od ove opasne pojave i bezbednosni subjekti nemaju adekvatne i potpune odgovore.

L I T E R A T U R A

Dan Verton (2003). Crni led: nevidljiva pretnja sajberterora, New York: McGraw-Hill.
Đorđević, O. (1986). Leksikon bezbednosti, Beograd: Partizanska knjiga.
Ivančević, V. (2009). Poslovni leksikon, Beograd: Velarta.
Pejanović. Lj., Bejatović. M. (2015). Osnovi bezbednosti-drugo izdanje, Pravni fakultet za pravo i pravosuđe, Univerzitet Privredna akademija, Novi Sad.
Pejanović Lj., Habuš, B. (2012). Zaštita od sajber terorizma, Naučni Skup, Fakultet bezbednosti, Banja Luka.
Unčanin, R. (2009). Poslovni leksikon, Beograd: Velerta.

Ljubo Pejanović

THREATS AND PROTECTION OF INFORMATION SYSTEM

Summary

This paper aims to point out the dangers, risks and consequences for the security of a computer information system, then it deals with the methods and forms of threats and consequences for the system, for data security and the computer owner. Among a large number of threats to a computer system, special attention is given to viruses and viral systems, as well as to threats of robbery and other forms of crimes with a view on the perpetrators of illegal activities, including hackers. Then, attention is given to problems in achieving security of computer systems and how protect them.

Key words: *computers, system, threat, security, protection.*

PREGLEDNI ZNANSTVENI RAD

Jure Tadić[596]
Filip Dragović[597]
Tonči Tadić[598]

MIGRACIJSKA I IZBJEGLIČKA KRIZA - SIGURNOSNI RIZICI ZA EU

Sažetak

Europska unija se danas suočava sa najvećim nekontroliranim priljevom migranata i izbjeglica u svojoj povijesti tako da se slobodno može govoriti o migracijskoj i izbjegličkoj krizi. Uzroci koji su doveli do, slobodno možemo reći, eksplozije migrantske krize u 2015. su dijametralno različiti: bijeg od ratnih stradanja, potraga za boljim životom, odlazak iz nefunkcionalnih država te bijeg od različitih vidova ekstremizma i terorizma. Procijenjuje se kako je 2000. godine bilo oko 150 milijuna migranata u svijetu, deset godina kasnije 214 milijuna uz pretpostavku rasta na 405 milijuna do 2050. godine. Glavni tokovi migracija su usmjereni prema redom visoko razvijenim zemljama i područjima gdje Europska Unija unatrag nekoliko godina predstavlja najpoželjniju ali i najlakše dostižnu destinaciju. Ostale ciljne države, prvenstveno SAD, Kanada i Australija su mnogim migrantima nedostižne zbog velikih udaljenosti te pojačanih kontrola granica od navedenih država. Ogroman te prvenstveno nekontroliran priljev (nezakonitih) migranata u 2014 i 2015 godini u Europsku Uniju, neovisno o poduzetim mjerama i pravnim ograničenjima, učinio je ustupak da se to pitanje, kao i pitanje nadzora i sigurnosti granice, pozicionira u žarište zaštite nacionalnih interesa određenih država. Tako se pitanje unutarnje sigurnosti nekih država danas povezuje s migrantima, to jest s njihovim nekontroliranim priljevom i mogućim utjecajem na sigurnosno, ekonomsko i političko stanje u državi. Može se ustvrditi da izbjeglička kriza nije samo stigla na vrata Republike Hrvatske i EU, nego je sa svim svojim rizicima koje nosi u cijelosti zahvatila ovo područje. Čini se kako izbjeglička kriza nikada nije bila aktualnija kao danas, a usljed velikog priljeva kako migranata tako i izbjeglica iz Bliskog istoka čije je krajnje odredište Europska unija. No ono, što je evidentno jeste da su države i institucije Europske unije kasno prepoznale ili točnije rečeno podcijenile migracijski problem kao pojavu koja sa sobom nosi ogroman sigurnosni rizik. Pored toga, djelomično se pristupilo jačanju kontrole na vanjskim granicama Europske unije, prvenstveno na južnim granicama što nije dalo očekivane rezultate. Otežavajuća okolnost u kvalitetnom riješavanju ove krize je bio nedostatak zajedničkog postupanja europskih država i zauzimanja konkretnih političkih stavova po ovom pitanju.

Ključne riječi: *izbjeglice, migrantska i izbjeglička kriza, sigurnosni rizici, migranti, izbjeglice, nezakonite migracije.*

---

[596] Jure Tadić, predavač, MUP, Policijska akademija, nastavnik stručnih predmeta, jure.tadic@gmail.com
[597] Dr. sc. Filip Dragović, regionalni savjetnik Programa Ujedinjenih naroda za razvoj (UNDP)
[598] Dr. sc. Tonči Tadić, predsjednik Euro-Mediteranskog Foruma Hrvatska (EMEF); koautor studije EuroMeSCo-SSN Joint Research Study „Arab Spring in Comparative Prospective“

1. UVOD

Republika Hrvatska kao i Europska unija u u posljednje vrijeme suočila se s ogromnim dolaskom izbjeglica na svoj teritorij i u samo nekoliko dana cijeli nacionalni sustavi su se pokazali nemoćnima odgovoriti na ovaj izazov. Jedna od dimenzija problema u slučaju Republike Hrvatske je pravna regulativa, odnosno učinkovita provedba Zakona o nadzoru državne granice, Zakona o azilu i Zakona o strancima, kao i sposobnost institucija da se nose s kriznim situacijama. Naši zakoni su tijekom pregovora sa EU u potpunosti usklađeni sa europskom pravnom stečevinom i kao takve trebalo ih je i implementirati. Međutim, cijeli sustavi u tom pogledu pokazali su se nedjelotvornim. Posljedica ovakvih propusta su stotine tisuća migranata na teritoriju Europske unije kojima pri ulasku nije utvrđen identitet niti su kvalitetno registrirani (fotografija i otisci prstiju). Otvaranje koridora za nekontrolirani priljev migranata urušilo je pravni i sigurnosni poredak Europske unije. Izbjeglicama je pomoć morala biti pružena u skladu s međunarodnim i europskim pravom, a na ovom planu je Europska unija potpuno zakazala ostavljajući države da se same suoče s ovim problemom. Političari su pokazali nedostatak liderstva i hrabrosti, što je rezultiralo i slabom potporom sigurnosnim službama.

Ono što je za Republiku Hrvatsku otežavajuća činjenica jest da je bilo dovoljno vremena da se pripremi za novonastalu situaciju (Mađarska je najavila zatvaranje granica) i da se s ostalim zemljama Europske unije, a prvenstveno Slovenijom, Austrijom i Mađarskom, uskladi postupanje. Umjesto toga, otvoreni su nepotrebni sukobi, uglavnom putem medija što nije moglo pridonijeti usklađivanju stavova na međunarodnom planu. Republika Hrvatska je članica Europske unije i probleme je trebala rješavati bilateralno ili u Briselu, posebno stoga što Europsko pravo ne prepoznaje tzv. otvaranje koridora za migrante ili izbjeglice. Republika Hrvatska je trenutno u vrlo nepovoljnoj situaciji jer je na hrvatske granice sa zemljama članicama EU postavljena žičana ograda što zasigurno ne pridonosi njenom zahtjevu za ulazak u schengenski prostor.

Migrantski/izbjeglički val posljedica je višegodišnjih tranzicijskih procesa na Bliskom istoku i Sjevernoj Africi u sklopu tzv. Arapskog proljeća. Ovi procesi su u Siriji i Libiji rezultirali građanskim ratom, ali i uzrokovali nestabilnost i humanitarnu krizu u njima susjednim zemljama, posebno u Turskoj i Libanonu, gdje su najveći izbjeglički centri. Prateći stanje u Siriji i Libiji, mogao se predvidjeti ovaj izbjeglički val, te se za njega pripremiti uz odgovarajuće analize i procjene. To, nažalost nije učinjeno u Hrvatskoj ni u drugim zemljama na tzv. Balkanskoj ruti – od Grčke do Njemačke, jer se nije vodilo računa o karakteru ovih tranzicijskih procesa. Riječ je, naime, o dugotrajnim i sveobuhvatnim procesima u arapskom svijetu, koji bitno mijenjaju političko i gospodarsko stanje na Mediteranu. Naime, Hrvatska i ostatak EU se trebaju pripremiti za višegodišnje, možda i desetljetno, bavljenje izbjegličkim valom i s njegovim uzrocima i posljedicama.

Radne migracije prije izbjegličkog vala

Postojeća izbjeglička kriza zapravo je sinergija ranijih radnih migracija iz nerazvijenih dijelova Mediteranskog bazena prema EU i bijega od ratom uzrokovane nesigurnosti u dijelu arapskih zemlja Mediterana i Podsaharskoj Africi . Migracija iz arapskog dijela Mediterana prema EU postojala je i prije „Arapskog proljeća“ 2011. godine. Za sve ove zemlje, naime, karakterističan je veliki prirodni priraštaj - u razdoblju od 1980. do 2010. su udvostručile svoje stanovništvo što je rezultiralo velikim udjelom mladog i nezaposlenog stanovništva. Spori gospodarski rast, praćen znatnim tehnološkim zaostajanjem za EU, unatoč rudnom bogatstvu (posebno u ugljikovodicima) rezultirao je iznadprosječnom nezaposlenosti mladih i prije prevrata u „Arapskom proljeću“, u prosjeku većom od 25%, uz primjere Egipta i Tunisa s 30% nezaposlenog mladog stanovništva. Uzme li se u obzir činjenica da je javni sektor bio i ostao glavni poslodavac, većina mladih bez političkih veza nije mogla naći posao te je redovito migrirala prema mediteranskim članicama EU.

Razlog uspona islamista

S druge strane, indikativno je da je u svim tranzicijama „Arapskog proljećg“ sekularna oporba „gurnuta u stranu“, te su u središte političkih zbivanja postupno dospjeli islamisti. Prije prevrata u Tunisu, Egiptu, Libiji, Siriji i Jemenu su na vlasti bile „sekularne“ diktature, ali je Islam i tada bio u izvorišnim osnovama njihovih Ustava. Unatoč postojanju sekularne oporbe, ključna oporbena snaga u tim zemljama destljećima su bili i ostali razni islamistički pokreti i stranke, koji su bili meta progona režima. Upravo zato su i doživljavani u javnosti kao jedina „prava“, beskompromisna oporba režimu, što je jamčilo nove članove. Unatoč višedesetljetnom progonu Muslimansko Bratstvo u Egiptu i srodne organizacije u Tunisu i Siriji nakon početka tranzicije preuzele su igru, u prvom redu zato jer su bile najbolje organizirane (u svakom slučaju bolje organizirane i s većom bazom birača nego tek nedavno nastale stranke ili pokreti), ali i zato jer je njihova populistička kampanja bila uspješnija. Jer lakše je populistički zagovarati tradicionalno prepoznatu etnički čistu arapsku državu uređenu po šerijatskim pravilima, nego se zalagati za više-etničku sekularnu više-stranačku demokraciju, sličniju kakvim zapadnim modelima.

Uloga stranih faktora

Za tranzicijski proces u „Arapskom proljeću“ posebno je svojstveno uplitanje stranih faktora s vlastitim ciljevima i interesima, bilo pri rušenju diktatora (npr. intervencija NATO-a pomogla je pri rušenju Gaddafija u Libiji), bilo pri podržavanju strana u višegodišnjem građanskom ratu – Rusija, Iran i libanonski Hezbollah su na strani al-Assada u Siriji, a Turska, Katar i Saudijska Arabija na strani oporbenog Sirijskog Nacionalnog Vijeća (SNC). Stoga opstanak režima al-Assada ili dolazak na vlast oporbenog SNC više ovise o dogovoru stranih faktora nego sirijskog naroda. U vjerski i klanski podijeljenome Jemenu je u tijeku vojna intervencija Saudijske Arabije i drugih arapskih država kako bi se slomio blok oporbe ustrojene oko tamošnje šijitske manjine na isti način kako je to učinjeno u Bahreinu, a sve u cilju suzbijanja utjecaja Irana. U Egiptu su Turska i Katar bili otvoreno na strani Mohameda Morsija i njegovog Muslimanskog bratstva za razliku od Saudijske Arabije koja se svrstala uz vojni režim.

Polazišne točke migrantskog vala prema EU: Sirija i Libija

Početak građanskog rata u Siriji 2011.

Sirijska Arapska Republika je prije 2011. bila „sekularna“ diktatura vladajuće Arapske socijalističke Ba'ath stranke, po državnom ustroju slična istočno-europskim režimima prije 1989. General Hafez al-Assad došao je na vlast vojnim udarom 13. studenog 1970., a nakon njegove smrti 2000. ga je naslijedio sin Bashar al-Assad na čelu Sirije. Iako sirijski „sekularni“ režim prividno nije bio definiran vjerskom nego stranačkom pripadnošću, Sirija je svoj vladajući sloj prvenstveno crpila iz svega 12% stanovništva ili 2.600.000 Arapa-alawita, islamske sekte bliska Šijitima. Alawiti, naseljeni mahom na zapadu Sirije, su bili i ostali unutar-sirijski oslonac režima al-Assada, njegove vojske i sigurnosnih službi.

Većinu od 22,5 milijuna Sirijaca, njih oko 60% ili 13,5 milijuna čine Arapi-Suniti, iz čijih se redova regrutira sirijska oporba, ali i ISIS. Kurda-sunita je 2011. bilo oko dva milijuna, naseljenih uz granicu s Turskom, na sjeveru i sjeveroistoku, dok na sjeverozapadu živi još i manji broj Turkmena. Bile su tu još i dvije islamske sekte: oko 670.000 Arapi-Druza, naseljenih u planinama na zapadu, te 450.000 Arapa-Ismailita. Kršćana, mahom Arapa naseljenih u gradovima u zapadnoj Siriji bilo je oko 2 milijuna, a među njima još i oko 400.000 Armenaca. Prosvjeda i oružanog otpora režimu bilo je i prije „Arapskog proljeća“. Gušeći ustanak Muslimanskog bratstva 1982. u gradu Hami režimske snage su pobile tisuće ljudi, a grad je sličio na Vukovar nakon napada JNA 1991.

Prosvjedi za promjenu režima u Siriji, započeti u gradu Daraa 15. ožujka 2011. širili su se Sirijom i do 29. srpnja iste godine su prerasli u otvoreni rat (ovaj datum se koristi kao prijelomica jer je tada konstituirana Slobodna Sirijska Vojska – FSA). Teško je govoriti o jedinstvenoj FSA s jedinstvenim zapovjednim lancem i glavnim stožerom, jer je većina oporbenih postrojbi bila je vezana za određeno područje ili naselje u kojem su prije toga bili prosvjedi, uz dio vojnika i časnika režimske vojske koji su dezertirali i pridružili im se.

Sirijsko nacionalno vijeće (SNC), sastavljeno od predstavnika nedefiniranog broja političkih oporbenih skupina, kao političko krilo FSA, priznale su članice EU, među njima i Hrvatska, kao novu vlast u Siriji. Za uspostavljanje povjerenja među raznim oporbenim frakcijama, uz postojeću etničku vjersku i regionalnu podvojenost, potrebna je velika politička vještina, a nje u Siriji nije bilo.

Rasplamsavanju rata doprinijela je tradicionalna oštrina režima u obračunu s neistomišljenicima, ali i rascjepkanost oporbenih snaga i nedostatak jedinstvenog zapovjednog lanca, što je dovelo do atomizacije oružanih skupina u oporbi – od početnih desetak do nekoliko desetaka skupina. Uz to, glavnina postrojbi FSA nije nikada imala topništvo i veće oklopne postrojbe, a pogotovo ne zrakoplovstvo. S teškim oružjem raspolagale su samo režimske snage, koje su prema svakom gradu ili dijelu grada u vlasti postrojbi FSA postupale kao s Hamom 1982. Očekivanja FSA i SNC, u prvom redu očekivanje NATO-ve vojne intervencije protiv al-Assada, poput one koja je srušila

Gaddafijev režim u Libiji, nikada se nisu ispunila. Jedina intervencija koju su dobili bila je iranska i ruska vojna intervencija na strani al-Assada.

Nakon početnog šoka i raspada dijela vojske u 2011., režim je tijekom 2012. i 2013. oporavio svoju vojsku uz obilnu rusku i iransku vojnu pomoć. Vojska je „alawitizirana“, odnosno uz nju sirijske paravojne postrojbe (Shabiha) i libanonskog šijitskog Hezbollaha, te uz pomoć iranskih savjetnika, a od nedavno i uz pomoć Rusa, nastoje zadržati kontrolu na zapadu Sirije.

Radikalizacija sukoba i strani utjecaji

Rat uvijek naglašava postojeće političke trendove radikalizacije: u totalitarnim režimima jača totalitarizam i isključivost režima, a u više-etničkim i više-vjerskim državama dovodi do među-vjerskih i među-etničkih sukoba. Tako je bilo i u Siriji: režim se sve više oslanjao na Alawite, te na druge vjerske manjine zgrožene mogućom islamističkom vizijom Sirije. S druge strane, vrlo je malo trebalo da rat sekularnih snaga za i protiv režima tijekom 2012. preraste u međuvjerski sukob između sunita i alawita, odnosno šijita općenito, posebno uzme li se u obzir vjerska i etnička struktura Sirije 2011. Tome su doprinijeli sa šijitske strane paravojne skupine: sirijske milicije Shabiha i libanonski Hezbollah, a sa sunitske strane sirijski i strani islamski radikali. Radikalizacija sukoba značila je više financijske pomoći i više dragovoljaca za radikalnije skupine, prateći istu matricu kao u Afganistanu, što je dovelo do jačanja radikalne islamističke Jabhat-Al Nusre (sirijske podružnice al-Qaide), te konačno do stvaranja ISIS i onda tzv. Islamske Države.

Nakon prevage skupnih oporbenih snaga početkom 2015., tek je povećana pomoć Rusije i njena izravna vojna prisutnost u Siriji u jesen 2015. vratila ravnotežu snaga, ali je rat daleko od završetka. Naime, svaka strana u tom ratu ima svoje sponzore: al-Assadov režim Iran i Rusiju, protivnici režima arapske bogate zemlje Zaljeva, Tursku, SAD i druge NATO članice, dok Kurdi imaju svoju subraću u Iraku te PKK u Turskoj. Pri tome svaki od sponzora ujedno ima i vlastitu agendu, odnosno prioritete.

Primarni cilj Rusije i Irana je opstanak režima al-Assada (i ostanak ruskih baza u Siriji), što može, ali i ne mora značiti i pobjedu nad ISIS-om. Važniji cilj je nametanje al-Assada kao čimbenika s kojim se mora pregovarati o budućnosti Sirije, te s time u vezi smanjivanje moći oporbene FSA, posebno na zapadu Sirije. Primarni cilj zemalja Zaljeva je eliminacija režima, ma tko je proveo (makar i ISIS). Primarni cilj Turske je eliminacija sirijskog Kurdistana i režima, ma tko to proveo. Primarni cilj SAD i saveznika iz NATO-a je dugo bila Sirija bez al-Assada (koji ionako predstavlja manjinu stanovništva) i bez ISIS-a, nego Sirija s novom vlasti, koju je pak teško formirati iz postojeće rascjepkane i raznolike oporbe.

Mogućnost kraja rata

Obzirom na sastav zaraćenih strana i na njihove sponzore, rat u Siriji može biti završen jedino općom mirovnom konferencijom, a ne pobjedom tj. vojnom prevlasti jedne strane, a pogotovo ne isključivo zračnim udarima. Preduvjeti za to su: definiranje oporbene

platforme na čemu radi Saudijska Arabija[599], odgovarajuća Rezolucija VS UN o Siriji[600] kojom bi se stvorio okvir za pregovore i mirovni sporazum al-Assadovog režima (s njim ili bez njega) sa oporbom i Kurdima, te na kraju zajednički obračun sa ISIS-om i drugim radikalnim skupinama koje ne žele mirovni sporazum. Zračni udari za to neće biti dovoljni, jer samo jačaju uvjerenje među stanovništvom kako „ubojica Arapa-sunita“ nije samo Bashar al-Assad, nego je to i Vladimir Putin, ali i vođe NATO zemalja.

Nužna je, dakle, kopnena vojna operacija u Siriji, u kojoj niti žele niti smiju sudjelovati snage NATO-a ili Rusije, jer bi to stvorilo dojam „novog križarskog rata“ i izazvalo opći revolt, sličan onome kod američke invazije i okupacije Iraka 2003. Tu kopnenu operaciju protiv ISIS i al-Qaide trebaju predvoditi sami Sirijci uz pomoć postrojbi drugih arapskih-sunitskih režima, naravno, tek nakon jednodušne osude ISIS-a na sastanku šefova država Arapske Lige. Kako je to ipak teško dostižan cilj, u postojećim uvjetima rat u Siriji i s njime povezani izbjeglički val može potrajati i više desetljeća.

Podjela Sirije i progoni gubitnika

Sirija je danas de facto teritorijalno podijeljena. Zapadnom četvrtinom zemlje koja je i najnaseljenija, od Damaska na jugu do Latakije na Sjeveru, uz morsku obalu i granicu s Libanonom, dominiraju snage al-Assadovog režima, ali ne u cijelosti. Na istom području, južno od Damaska do Golanske visoravni, te na sjeveru prema Turskoj su široka područja pod kontrolom FSA i/ili al-Nusre, koje režim nastoji suzbiti uz pomoć Rusa, Iranaca i Hezbollaha. Na sjeveroistoku, uz granicu s Turskom, je sirijski Kurdistan koji ratuje sa ISIS-om. Skoro polovicu Sirije, odnosno njen slabo naseljeni, ali naftom i plinom bogati istočni i središnji dio, kontrolira ISIS. Sa ISIS-om formalno ratuju svi: režim, FSA, Al-Nusra, Kurdi, te sve strane sile.

Vjerska i etnička podjela Sirije, uz vjerski karakter rata, jamči da strana koja gubi bitke biva prognana: jačanje al-Assada znači jačanje izbjegličkog vala Arapa-sunita, jačanje oporbene FSA ili Jabhat Al-Nusre znači izbjeglički val Arapa-alawita, dok pobjeda ISIS-a znači izbjeglički val svih ostalih. Nacionalne i vjerske manjine – Armenci, odnosno Arapi – kršćani, druzi i ismailiti su posebno sumnjivi ISIS-u, Al-Nusri i islamistima općenito, te su bili meta progona i među prvima su otišli iz svojih domova ako su mogli.

Sastav izbjegličkog vala iz Sirije

Budući da su Kurdi stvorili vlastite oružane snage i žele svoj dio na sjeveru Sirije, te da Turskoj nije stalo do povećavanja domaće kurdske populacije, može se isključiti jačanje kurdskog izbjegličkog vala. Sa teritorija pod kontrolom ISIS-a su pobjegli svi koji su mogli na teritorij pod kontrolom režima ili FSA ili pak izvan Sirije. Alawiti i kršćani su se sklanjali u dijelove pod kontrolom režima ili u susjedni Libanon, dok su se suniti iz područja pod udarom režimskih snaga sklanjali ili dalje na oporbeno područje (manje vjerojatno) ili izvan Sirije što je vjerojatnije. Glavninu sirijskih izbjeglica ipak čine ljudi koji sebe ne vide na strani režima, ni na strani oporbene FSA, a pogotovo ne na strani ISIS.

---

[599] http://www.diplomatie.gouv.fr/en/country-files/syria/events/article/final-statement-of-the-conference-of-syrian-revolution-and-opposition-forces
[600] http://www.un.org/press/en/2015/sc12171.doc.htm

Glavnina izbjeglica su Arapi-suniti, koji su i inače većina stanovništva, i to iz oporbenih dijelova Sirije koje su napadale režimske snage, među kojima može lako biti i boraca FSA ili al-Nusre. Manjina u izbjegličkom valu su alawiti i kršćani, odnosno ostale vjerske i etničke manjine. Prema UNHCR-u , u Siriji je od 22,5 milijuna stanovnika iz svojih domova iselilo njih oko 11 milijuna. Od toga je izvan Sirije 4,39 milijuna izbjeglica i to najviše u Turskoj – 2,29 milijuna, Libanonu – 1 milijun, Jordanu – 632.000, Iraku – 244.500, Egiptu – 123.500 i Libiji – 26.000.

Prema analizi UNHCR-a[601] objavljenoj u rujnu 2015. sedam je osnovnih razloga za izbjeglički val prema EU. Na prvom mjestu je gubitak nade. Za mnoge sirijske izbjeglice, svaki tračak nade da će se situacija u njihovoj zemlji promijeniti nabolje ili da je bilo kakvo rješenje na vidiku jednostavno su nestali. Na drugom mjestu je povećanje siromaštva. Izbjeglice koje su našle utočište u Libanonu suočavaju se s visokim troškovima života što je glavni uzrok napuštanja ove zemlje, dok izbjeglice u Egiptu i Jordanu - zemljama koje su bile bogatije od Sirije prije nego što je rat u toj zemlji počeo - kažu kako ne mogu sebi priuštiti ni osnovne stvari.

Na trećem mjestu je ograničena mogućnost zaposlenja. Mnogi Sirijci u Jordanu, Egiptu i Libanonu žele zaraditi za život, ali su u tome zakonski ograničeni. Izbjeglice u Iraku kažu da veliki broj interno raseljenih osoba (prognanih od ISIS-a u Iraku) snizio cijenu rada i povećao konkurenciju na tržištu rada u Iraka. Istodobno je gospodarska aktivnost gotovo zamrla zbog pada cijena nafte. Nedostatak pravih poslova tjera izbjeglice na crno tržište rada, čime riskiraju eksploataciju, nesigurne uvjete rada i prevarante koji ne isplaćuju zarađeno. Uz sve pobrojano, u pojedinim izbjegličkim logorima raste problem prostitucije. Izbjeglice mogu biti kažnjene za rad na crno. Prema novim propisima u Libanonu, izbjeglice moraju potpisati obavezu da neće raditi kada obnavljaju svoj status.

Četvrti razlog za masovan odlazak u Evropu je nedovoljna pomoć i zdravstvena zaštita. Programi pomoći za izbjeglice i zemlje u susjedstvu Sirije koje su ih primile stalno se suočavaju s nedostatkom sredstava. Postojeći međuagencijski plan za izbjeglice iz Sirije imao je samo 50% potrebnih sredstava za 2015. godinu – ili samo 2,1 milijardi USD u odnosu na očekivanih 4,3 milijarde USD što je dovelo do ozbiljnih smanjenja u broju, količini i kvalitetu obroka, a za svakog izbjeglicu je predviđeno nešto manje od pola dolara na dan za hranu i vodu. Mnoge izbjeglice u Jordanu rekle su UNHCR-u kako je racionalizacija hrane u izbjegličkim centrima bila "kap koja je prelila čašu," nakon čega su odlučili napustiti Libanon. Mnogi od njih su se odali prosjačenju i iznajmljivanju djece za rad. Nedovoljno sredstava dovelo je i do pogoršanja zdravstvene zaštite: u 2015. godini 58,3% izbjeglica nema pristup lijekovima i/ili zdravstvenoj skrbi.

Na petom mestu su, navodi UNHCR, prepreke da se obnovi izbjeglički status u Libanonu i Jordanu. Prema novim propisima, izbjeglice koje su došle u Libanon do 2014. godine moraju platiti 200 USD kako bi obnovile svoj izbjeglički status, pa je mnogo njih

[601] http://data.unhcr.org/syrianrefugees/regional.php

krenulo u Tursku. Također, od njih se traži da potpišu jamstvo da neće raditi i da imaju potpisani ugovor o iznajmljenom stanu. U Jordanu, pak, prema novim propisima, svaka novoregistrirana izbjegla osoba mora pribaviti certifikat o zdravstvenom stanju, koji košta 42 USD. Kao šesti razlog za migraciju, navode se oskudne mogućnosti za obrazovanje. Zbog otežane situacije i pogoršanih uvjeta života u Jordanu, 20 posto djece koja su izbjegla napuštaju školu kako bi radila, dok se u nekim slučajevima djevojčice prisiljavaju da uđu u rane brakove. Procjenjuje se da skoro 90.000 djece školskog uzrasta porijeklom iz Sirije nemaju nikakvo formalno obrazovanje. Sedmi razlog je nesigurnost u zemljama u okolini Sirije, odnosno strah od širenja sukoba i od negativnih reakcija domicilnog stanovništva.

Sastav izbjegličkog vala iz Libije

Iz gore navedenog je očito kako ne postoji jedinstvena državna vlast na čitavom teritoriju Libije, niti jedinstveni vojni i sigurnosni sektor koji bi jamčio sigurnost građanima ili nadzirao morske i kopnene granice Libije. Nasilje islamističkih skupina prema kršćanima Koptima potiče njihovo iseljavanje. Međutim, paradoksalno je to što Libijci ne sudjeluju u izbjegličkom valu usmjerenom prema EU. Tijekom borbi 2011. oko 4000 izbjeglica je dnevno prelazilo granice s Tunisom i Egiptom, te se procjenuje da je ukupno 200.000 Libijaca izbjeglo u Egipat i Tunis, među njima i etničke manjine: Egipćani (Kopti), Tunižani i Turci, ali i doseljeni stanovnici iz država pod-Saharske Afrike[602], te Libijski crnci npr. iz grada Tawergha. Crne državljane Libije i pod-Saharskih zemalja ustanici su smatrali „Gadafijevim plaćenicima“, te su ih posebno progonili.

Prema podacima UNHCR[603], od 6,2 milijuna Libijaca, njih 435.000 su prognanici u samoj Libiji. Uz njih je u Libiji oko 28.000 izbjeglica, od čega 26.000 Sirijaca, a ostali su iz zemalja pod-Saharske Afrike, ali i iz Bliskog Istoka i Somalije. Aktivnosti islamističkih skupina u Sahelu, ali i sukobi libijskih oružanih skupina otežavaju životi izbjeglica i prognanika, te dostavu humanitarne pomoći. Zato se dio njih odlučuje za prekomorsko putovanje do talijanske Lampeduse.

Tijekom 2011., tj. na početku rata u Libiji je 62.000 izbjeglica iz libijskih luka stiglo do Italije. Broj prekomorskih izbjeglica se smanjio na trećinu u 2012.[604] , ali je tijekom 2013. dosegnuo 59.600, a Sirijci i Palestinci iz Sirije činili su polovicu svih izbjeglica. Tijekom 2014. je broj prekomorskih izbjeglica iz libijskih luka porastao od oko 2.000 mjesečno u siječnju do 15.000 mjesečno od sredine 2014., od čega su petina Sirijci. Za ovu izbjegličku rutu je posebno karakterističan veliki broj obitelji s djecom.

Nužnost praćenja političkog stanja na Mediteranu

Koliko će ova migracijska i izbjeglička kriza utjecati na cjelokupno stanje sigurnosti u Europskoj uniji predstoji za vidjeti, ali posljednji teroristički napad u Parizu nedvojbeno je pokazao da su terorističke skupine iskoristile ovu krizu za nesmetani prelazak europskih granica. Polazeći od definiranja pojma državne granice, odnosno granične crte kao krajnjeg

---

[602] Scott Sayar i Alan Cowell (2011). Libyan Refugee Crisis Called a 'Logistical Nightmare, *The New York Times, 3. ožujka 2011.*

[603] http://www.unhcr.org/pages/49e485f36.html

[604] https://data.unhcr.org/syrianrefugees/download.php?id=6810

dosega vlasti neke zemlje, proizlazi da se prve mjere, koje se mogu poduzeti s namjerom zaštite nacionalne odnosno unutarnje sigurnosti, mogu ili moraju poduzeti upravo na "samoj državnoj crti", a službe koje poduzimaju takve mjere i radnje preuzimaju dio odgovornosti za cjelokupno stanje sigurnosti na unutarnjem planu. S druge strane, nužno je praćenje političkih i gospodarskih procesa ne samo u neposrednom susjedstvu Hrvatske, nego i na čitavom prostoru Mediterana jer se svaka nestabilnost u mediteranskim zemljama preslikava na EU, ali i obrnuto.

2. SIGURNOSNI RIZICI U POGLEDU GRANIČNOG PODRUČJA - SIGURNOST GRANICA I MIGRACIJE

Europska unija nastala je 1992. godine nakon nekoliko desetljeća uspješne izgradnje i razvoja ekonomske zajednice na zapadnoeuropskom prostoru i gospodarskog prosperiteta na području razrušene Europe nakon II. svjetskog rata. Nakon demokratskih promjena u državama srednje i istočne Europe, završetka blokovske i hladnoratovske podjele, ujedinjenja Njemačke te nastanka novih suvremenih i demokratskih zemalja u Europi, dolazi do promjena u poimanju i nadzoru granica između istočnih i zapadnih europskih zemalja. Devedesetih godina prošlog stoljeća, nakon pada Berlinskog zida, u zapadnim se zemljama bilježi pojačan imigracijski pritisak stanovnika istočnoeuropskih zemalja koji je do tada bio uglavnom politički motiviran. Međutim, prema zemljama zapadne Europe, uglavnom zbog ratnih zbivanja, ali i želje za boljim životom, kreću i migranti iz azijskih i afričkih zemalja te u devedesetima i s područja bivše Jugoslavije. Tada dolazi do promjena u političkim stavovima prema useljavanju te visokorazvijene zemlje mijenjaju zakone i praksu kako bi otežale ulazak i zapošljavanje, čime se otvarao prostor za nezakoniti ulazak i boravak. Migracije koje su bile pokretači razvoja zapadnih zemalja postaju tema rasprava u negativnom kontekstu, točnije, ograničavaju se zakonite migracije[605]. Tako su se zemlje Europske unije, tadašnje zemlje kandidatkinje za članstvo u Europskoj uniji, ali i tranzitne zemlje koje su se nalazile na pravcu kretanja istok - zapad, vrlo brzo suočile s valom nezakonitih migracija, ali i sa svim oblicima prekograničnog kriminala koji je postao transnacionalan. Također, proširenje Europske unije zahtijevalo je ponovno proučavanje i promišljanje kako se vanjske granice jedne takve zajednice mogu najbolje štititi od transnacionalnog kriminala, nezakonitih migracija, krijumčarenja ljudi i robe, zloupotrebe sustava azila te prijetnji povezanih s terorizmom[606]. Proces tzv. internacionalizacije unutarnje sigurnosti Europske unije zasigurno je bio determiniran i potaknut zahtjevima globalizacije - posebno mogućnostima koje je pružao napredak u transportu i komunikacijskim tehnologijama, pojavom novih kriminalnih organizacija u bivšim komunističkim zemljama pa čak i nesnalaženjem tijela za borbu protiv ovih pojava u novim okolnostima[607].

---

[605] Opširnije: Huntington P. S. (1997). Sukob civilizacija i preustroj svjetskog poretka, Izvor d.o.o., Zagreb, 245-255

[606] Marenin O.; Challenges for Integrated Border Management in the European Union, Geneva Centre for the democratic control of armed forces (DCAF), Occasional Paper – No17.

[607] Anderson M., Apap J.(2002). Striking a balance between Freedom, Security and Justice in an enlarged European Union, Centre for European Policy Studies, Brusseles, Monograph, str.6.

Ono što je više nego očito jest da priljev nezakonitih migranata postaje jedno od važnih pitanja nacionalnih interesa i unutarnje sigurnosti kako Republike Hrvatske tako i svih članica EU. Ipak, potrebno je naglasiti da sve države članice EU nisu u istoj mjeri opterećene nezakonitim migracijama. Pod najvećim pritiskom tradicionalno su najrazvijenije države, ali u posljednjih desetak godina i sredozemne države članice Unije bilježe veliki rast nezakonitih migracija. Nezakonite migracije predstavljaju sigurnosni rizik i za Republiku Hrvatsku koja je, uz već navedenu činjenicu da se prostorno nalazi na području kojim prolaze krijumčarski pravci prema zapadnoj Europi[608], ali i čega smo svjedoci posljednjih mjeseci, uslijed vala izbjeglica iz ratom zahvaćene Sirije. Suočene s velikim migracijskim pritiskom i sve većom pojavom aktivnosti vezanih uz nezakonite migracije, članice EU su došle do zaključka da više nisu sposobne same na nacionalnoj razini adekvatno djelovati na fenomen nezakonitih migracija te da moraju koordinirati mjere na europskoj i međunarodnoj razini, prvenstveno na području pravosuđa i unutarnjih poslova.[609]

U zadnje vrijeme, pitanje sigurnosti nacionalnih teritorija stavlja se u žarište interesa. Razmatranje nacionalne sigurnosti razvilo se od tradicionalnih vojno-političkih pitanja na međudržavnoj razini, kao što su zaštita nepovredivosti granica zemalja ili konstantni otpor prema vanjskim opasnostima, u mnoga nova područja, uključujući izbjeglice i migracijske trendove.[610] Ako se pođe od definicije državne granice odnosno granične crte kao krajnjeg opsega vlasti određene zemlje, može se zaključiti da se prve mjere koje bi se mogle poduzeti s ciljem zaštite nacionalne ili unutarnje sigurnosti, mogu ili moraju poduzeti upravo na "samoj državnoj crti", a službe koje poduzimaju takve mjere i radnje preuzimaju dio odgovornosti za cjelokupno stanje sigurnosti na unutarnjem planu.[611]

Određeni autori izravno povezuju unutarnju sigurnost sa stanjem na granici države[612] uslijed čega se postavlja pitanje potrebe pojmovnog određenja granične sigurnosti ili sigurnosti područja uz državnu granicu. Danas je širom svijeta, posebno u zemljama koje su izložene problemu migracija, ali i drugim ugrozama nacionalne sigurnosti često korišten pojam granične sigurnosti. Nadalje, pojedini autori razinu granične sigurnosti navode kao izazov tvorcima politike jer ona mora biti primjerena vanjskim prijetnjama, ali treba omogućiti nesmetan i zakonit prijelaz državne granice osobama i robama i ujedno omogućiti zaštitu ljudskih prava i sloboda, dok savezne agencije zajedno moraju omogućiti odgovarajuću razinu granične sigurnosti.[613]

---

[608] „Strategija nacionalne sigurnosti Republike Hrvatske" (2002) Zbirka propisa i strateških dokumenata iz područja obrane.

[609] Trauner F. i Kruse I. (2008). Visa Facilitation and Readmission Agreements: Implementing a New EU Security Approach in the Neighbourhood, CEPS Working Document No. 290/April 2008, prikazano na: http://www.ceps.eu/book/ec-visa-facilitation-and-readmission-agreements-implementing-new-eu-security-approach-neighbour (pristupljeno: 26.11.2015.).

[610] Loescher, G. (1995). International security and population movements, The Cambridge Survey of World Migration, edited by Robin Cohen, University of Warwick, Cambridge University Press, 557 – 560.

[611] Dragović, F. (2003). Nezakonite migracije – sigurnosni fenomen kraja 20. stoljeća, Ministarstvo unutarnjih poslova Republike Hrvatske.

[612] Hellenthal, M. (1998). Granična sigurnost - kamen temeljac unutarnje sigurnosti, Izbor, 2-3, MUP, Zagreb, 141.

[613] CRS Report for Congress, RL31019, Terrorism: Automated Lookout Systems and Border Security Options and Issues, 18. lipnja 2001. godine, http://www.fas.org/irp/crs/rl31019.pdf

Na europskim prostorima također se sve više govori o graničnoj sigurnosti, a jedan od akata[614] Vijeća EU definirao je novi koncept: integrirani model granične sigurnosti koji pokriva sve segmente granične politike. Navedenim konceptom obuhvaćeno je pet pitanja i to:

1. Granična kontrola na vanjskim granicama (granične provjere i nadzor državne granice definirane Schengenskim pravilima, uključujući analizu rizika i kriminalističko – obavještajni rad);
2. Otkrivanje i istraživanje prekograničnog kriminala u koordinaciji sa svim agencijama za provođenje zakona;
3. Četveroslojni model pristupa kontroli:
   a) mjere kontrole u području slobode kretanja, uključujući i vraćanje osoba;
   b) granične i carinske kontrole;
   c) suradnja sa susjednim zemljama;
   d) mjere u trećim zemljama.
4. Međuagencijska saradnja u upravljanju granicom (granična policija, carina, policija, nacionalne sigurnosne i druge nadležne agencije i organi i internacionalna saradnja);
5. Koordinacija i koherentnost aktivnosti država članica i institucija i drugih agencija i tijela EU kroz provedbu mjera unutar teritorija.

Oslanjajući se na navedeno, sigurnost graničnog područja mogla bi se definirati kao stanje na državnoj granici o kojem vode brigu sva nadležna tijela, posebno policija i carina, koje uz osiguranje nesmetanog odvijanja prometa putnika i roba preko državne granice, obuhvaća i poslove s ciljem onemogućavanja bilo kakvih kažnjivih radnji čije je izvršenje neposredno povezano s državnom granicom, a ujedno ima implikacije na unutarnjem i vanjskom planu, pri čemu se misli na povrede nacionalnog zakonodavstva i međunarodnog prava. Dodatna kvaliteta ili bolje rečeno razina granične sigurnosti se postiže bilateralnom i multilateralnom suradnjom nadležnih tijela susjednih zemalja, bilo razmjenom informacija ili provedbom zajedničkih akcija.

Nadalje, osnivanjem Europske agencije za kontrolu vanjskih granica – Frontex[615] i njezinim jačanjem postavljen je sadašnji okvir za intenzivnu i učinkovitu suradnju na ovom području[616]. Posljednjih godina nezakonite migracije, kao vrsta kažnjivih radnji vezane uz državne granice, nesumnjivo predstavljaju sigurnosnu pojavu koju mnogi povezuju s ugrožavanjem nacionalne sigurnosti zbog velikog broja migranata[617] koji padaju na teret svake države koja im pruža "*utočište ili boravak*" i zbog činjenice da su u jednom svom

[614] Council Conclusions on Integrated Border Management, 2768th Justice and Home Affairs Council meeting Brussels, 4-5 December 2006

[615] Council Regulation (EC) 2007/2004. on the establishment The European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex), Official Journal L 349/25.11.2004.

[616] Trenutno se na europskoj razini raspravlja o preimenovanju Frontexa u Europsku graničnu agenciju sa većim ovlastima za djelovanje na teritoriju EU (European Border and Coast Guard Agency)

[617] "Strategija nacionalne sigurnosti Republike Hrvatske" ,"Narodne novine", broj 32/02., članak 33.

dijelu povezane s kriminalnim skupinama na nacionalnoj i međunarodnoj razini, te se prema procjenama Ujedinjenih naroda godišnja zarada organizacija koje se bave krijumčarenjem osoba kreće oko 7 milijardi dolara.[618] Ovdje treba snažno naglasiti važnost demistifikacije fenomena migracija sa sigurnosnog aspekta i navesti kako se u najvećem broju slučajeva radi o osobama čiji je razlog migracije primarno ekonomske naravi. Izbjeglice iz ratom zahvaćenih područja su kategorija koja zahtijeva svu pomoć sukladno međunarodnim (ne samo pravnim, nego i humanim i moralnim) pravima, ali u standardiziranim i propisanim uvjetima, nikako nekontroliranim. No, ono što je zabrinjavajuće, jest činjenica kako uvijek u velikom broju postoje skupine ili pojedinci koji se pokušavaju sakriti i proći neopaženo jer su njihove pobude dolaska u Europu sasvim druge prirode (što je pokazao i posljednji teroristički napad u Parizu). Teroristički napadi koji su se dogodili na tlu Europske unije pokazuju da su počinitelji uglavnom osobe koje su rođene ili su veći dio života provele na teritoriju Europske unije, dok se kao pomagači ili poticatelji mogu pojavljivati novi migranti. To su izazovi takozvanih mještovitih migracijskih tokova. Otežavajuća činjenica je da se radi o generacijama koje su odrasle u neprestanim sukobima koji su bili kulturološke, religiozne i civilizacijske prirode.

Mora se navesti da migranti ne predstavljaju izravnu sigurnosnu prijetnju, ali jedan dio njih može biti radikaliziran i sklon činjenju raznih kaznenih djela zbog vlastitih frustracija ili utjecaja okoline. Tako je i Frontex upozorio na pojavu odlaska na bojišta europskih državljana, njihovu daljnju radikalizaciju i povratak u Europu u svojstvu migranata bez identifikacijskih isprava *("Considering the ongoing conflict in Syria and Iraq, which attracts more and more radicalised foreigners, it is possible that such persons transit the region posing as migrants"*[619])

Slijedom navedenog, najveći sigurnosni izazov ovakvih nekontroliranih migracija predstavlja povezanost migranata s terorističkim organizacijama (*Europol: "The large and growing number of illegal immigrants from countries and regions in which Islamist terrorist groups are active – such as Chechnya, Afghanistan, Iraq, Pakistan and Somalia – raises the possibility that channels for illegal immigration will be used increasingly by those seeking to engage in terrorist activity in the EU"*[620]) Kod ovih sigurnosno najosjetljivijih izazova moramo biti posebno oprezni u postavljanju uzročno-posljedičnih veza.[i] Za pojedine autore priljev nepoznatih i potencijalno opasnih migranata s pravom predstavlja velik sigurnosni izazov, pogotovo u njihovom spoju s onim krugovima u Europi koji su spremni na najradikalnije poteze. Za tako nešto Bruce Hoffman je na europskom tlu detektirao slabo primjetnu i nepredvidljivo malu bazu u ogromnoj muslimanskoj dijaspori koja predstavljaja veliku sigurnosnu prijetnju.[ii] Carlos Ortiz se nadovezuje na Hoffmana te misli kako tokovi migracija uspostavljeni tijekom prošlog stoljeća i obogaćeni velikim priljevom političkih

---

[618] a/ Iskazano u Palermu gdje je od 12. do 15. prosinca 2000. godine održana Konferencija UN-a na kojoj je od 148 predstavnika zemalja članica UN-a njih 121 potpisalo Konvenciju o borbi protiv međunarodnog organiziranog kriminala (među njima i Republika Hrvatska).

b/ Isti podaci; Gosh, B. (1999). Irregular Migration, Migration News, 6, 1.

[619] WB ARA 2015, Western Balkans Annual Risk Analysis, http://frontex.europa.eu/assets/Publications/Risk_Analysis/WB_ARA_2015.pdf

[620] Europol (2011) "EU Organised Crime Threat Assessment", OCTA 2011, str. 18, prikazano na: https://www.europol.europa.eu/sites/default/files/publications/octa_2011.pdf, učitano 17. listopada 2011. godine

izbjeglica nakon 1990-tih, postali su medij za pojedine radikalne krugove muslimanskih zajednica u Europi koje su osiguravale džihadiste za sukobe na Bliskom istoku, te utjecale na uspostavu terorističkih ćelija u Europi. Ovdje je potrebno ponovno naglasiti kako je potrebno paziti i izbjeći identifikaciju većine s manjinom jer u svakom društvu postoje oni koji djeluju protiv sustava. Pored već spomenutih izazova, možda najfluidinije područje predstavljaju prijetnje koje proizlaze iz radikalizacije određenog broja pripadnika muslimanske zajednice u Europi te njihovog dvosmjernog puta kojim odlaze u terorističke kampove u pretežno nekontroliranim područjima Pakistana na granici između Pakistana i Afganistana gdje prolaze trening i radikalizaciju te se vraćaju u Europu s ekstremnim stavovima i planovima.

U posljednjih nekoliko godina stotine tisuća ljudi je uspjelo ući na teritorij Europske unije i u pravilu zatražiti azil. Međutim Dublinski sustav azila, uspostavljen u okviru Schengenskih sporazuma, nije primjeren za takav masivan priljev izbjeglica dok klasični sustav za prihvat izbjeglica u ovakvom opsegu nije bio kvalitetno riješen. Prelazak vanjske granice Europske unije je moguć samo na graničnim prijelazima i sve osobe koje uđu nezakonito na teritorij, moraju se registrirati, točnije podnijeti zahtjev za azil, što u ovom migracijskom valu nije poštivano na cijeloj ruti od Grčke do Njemačke.
Statistički pokazatelji o broju nezakonitih migranata na teritoriju Europske unije prema dostupnim podacima pokazuju značajno povećanje što će biti još izraženije kada se uzme u obzir i 2015. godina za koju postoje podaci od približno milijun nezakonitih migranata (može ih se nazvati izbjeglicama, azilantima i sl., ali većina je ušla ilegalno uvođenjem tzv. koridora). Iako je Europska unija jako gospodarsko tržište, postavljanje pitanja o realnim kapacitetima prihvata i uključivanja u društveno-gospodarski život nedovoljno se pojavljuje i postavlja. Ukoliko se ne ispune subjektivna očekivanja, postoji bojazan njihovog okretanja činjenju raznih kaznenih djela ne isključujući i ona nasilna povezana s rasom, vjerom, a u Njemačkoj su zabilježeni i napadi na ženske osobe[621]. Zasigurno, nepostojanje jasnih planova za izbjeglice i migrante uzrokovati će jačanje otpora prema migrantima i porast potpore radikalnim desnim strankama u europskim zemljama. U nekim zemljama su već i formirane tzv. skupine za zaštitu (u Finskoj tzv. Odinova vojska), što dodatno otežava sigurnosnu situaciju jer jedan konflikt vodi drugome.

Europska unija bi trebala žurno predstaviti jasne strateške i akcijske planove integracije stranaca koji dolaze iz drugih dijelova svijeta iz dva temeljna razloga ili cilja:

- smanjenje radikalizacije migranata, ali i europskih građana
- migranti moraju vidjeti pozitivan cilj integracije u novo društvo.

Nadalje policijsko-obavještajni sustav Europske unije, uključujući i njezin pravni okvir, treba redefinirati kako bi se učinkovito suprostavio novim oblicima sigurnosnih prijetnji uz

[621] Ono što je još tragičnije od samog događaja je činjenica da je Sami Abu-Yusuf, imam džamije u Koelnu je u ekskluzivnom i intervjuu za TV REN objasnio da su žene iz Njemačke same krive zbog seksualnih napada koje su doživjele u Koelnu. jer su ih one izazivale svojom odjećom i parfemima koje su koristile. Ovakve izjave pokazuju da se radi o sukobu civilizacija I kultura a ne o klasičnim kaznenim djelima jer počinitelji to ne smatraju kaznenim djelom.
http://www.vecernji.ba/da-nisu-koristile-parfeme-zene-iz-njemacke-ne-bi-bile-napadnute-1053425

poštivanje međunarodnih standarda. Naime, isključiva briga o vlastitoj sigurnosti država članica je kontraproduktivna za sveopću sigurnosnu situaciju u EU. Zajednički pristup ovim pitanjima bez skrivenih nacionalnih interesa je preduvjet za uspjeh. Upravo su razjedinjenost europskih zemalja i nedostatak jasnih poruka uzrokovali ovu migracijsku krizu kojoj se ne završetak ne nazire.

Tablica 1: Statistički pokazatelji o nezakonitim migracijama, Izvor: Frontex

FRAN indicatori	**2008**	**2009** procjene	**2010**	**2011**	**2012**	**2013**	**2014**
Nezakoniti prelasci vanjske granice EU izvan graničnih prijelaza	159.881	104.599	104.051	140.980	72.437	107.365	283.532
Nezakonit boravak na teritoriju EU	441.237	412.125	353.077	350.944	344.928	345.098	441.780
Otkriveni pomagači	9.884	9.171	8.629	6.957	7.662	7.252	10.234
Izdate odluke o povratku				231 385	269 949	224 305	252 003
Učinkovit povratak				149 045	158 955	160 418	161 309

3. MIGRACIJE NA PROSTORU REPUBLIKE HRVATSKE

Uslijed svog geostrateškog položaja Republika Hrvatska na samom je putu migracijskih kretanja osoba iz istočnoeuropskih i azijskih zemalja prema razvijenim zemljama EU. Kao i druge europske zemlje i Republika Hrvatska je suočena s porastom broja nezakonitih migracija, posebice zbog svog zemljopisnog položaja, a za pretpostaviti je da će, ukoliko dođe do znatnijeg razvoja gospodarstva, postati privlačna zemlja za ekonomsku migraciju koju neizostavno prati i "crno tržište rada" kao i nezakoniti ulasci i ostanak protivan važećem zakonodavnom okviru.

Aktualna izbjeglička kriza s arapskog poluotoka i sjevera Afrike ne datira samo od 2015. godine već nekoliko godina unatrag. Izbjeglice kontinuirano koriste rute preko Grčke, Italije i manjim dijelom Španjolske, ali nisu bile u ovako izraženom broju. Danas je Republika Turska prva zemlja u svijetu po broju primljenih izbjeglica iz ratom zahvaćenih

područja, ali i ekonomskih migranata. Njihov broj se procjenjuje na oko 1,5 do 2 milijuna i predstavlja polaznu točku glavnine migracija prema RH. Sve procjene i analize europskih agencija, posebno FRONTEX-a (Agencija za kontrolu vanjskih granica EU) ukazivale su na ovaj rastući problem i bilo je samo pitanje dana kada će se izbjeglički val dogoditi i Hrvatskoj koja je bila potpuno nepripremljena za ovu krizu.

Kako se Republika Hrvatska nalazi na vanjskoj granici Europske unije, ali izvan Schengena, za očekivati je da će biti izražen sve veći pritisak na njezinu državnu granicu od strane migranata, ali i krijumčara ljudima. Iako još uvijek nije u Schengenu, korisno je napomenuti da Schengenski pravni sustav jasno definira ulazak na teritorij Europske unije i način na koji izbjeglice mogu regulirati svoj status. Također, Dublinski sustav azila je jasno uredio načine dobivanja statusa azilanta i prava tih osoba. Niti jedan od ovih sustava ne prepoznaje ekonomske migrante i već duže vrijeme traje „zloupotreba sustava azila“ na način da osobe koje su ekonomski migranti traže azil koji je predviđen za osobe koje su u vlastitoj zemlji proganjane na političkoj, rasnoj, vjerskoj ili nekoj drugoj pripadnosti. Republika Hrvatska je tijekom procesa pristupanja punopravnom članstvu uskladila svoje zakone i pripremila administrativne kapacitete za njihovu implementaciju, međutim, ovi mehanizmi nisu mogli odgovoriti ovakvom pritisku. Do siječnja 2016. preko teritorija RH prešlo je oko 600.000 izbjeglica prema zapadnim zemljama uvođenjem tzv. koridora. Kako se u ovom slučaju radilo o masovnom i nekontroliranom dolasku izbjeglica, bilo je pitanje dana kada će Njemačka i druge zemlje članice Schengena uvesti ponovnu graničnu kontrolu na unutarnjim granicama te ojačavati kontrolu zelene granice jer je evidentno da je nekontrolirani priljev izbjeglica postao sigurnosna, ali i ekonomska prijetnja. Ono što posebno uznemiruje javnost jest postavljanje žilet žice na zapadne granice RH koja je kao zemlja Europske unije ostala s druge strane jer nije članica schengenskog prostora. Europa će braniti Schengen, a RH nema odgovor na to pitanje. Uspostava tzv. hot spotova na ruti od Grčke prema EU je dogovorena na sastanku u Briselu, ali to nitko ne želi priznati u našoj javnosti[622]. Izbjeglicama definitivno treba osigurati pomoć, osnovne uvjete za život te moguću integraciju. Međutim, taj proces mora biti kontroliran i koordiniran u okviru šireg sustava.

Republika Hrvatska treba koordinirati svoje aktivnosti sa ostalim zemljama članicama i biti aktivan sugovornik i partner na europskoj razini. Ukoliko smo članica Europske Unije, a jesmo, tako se trebamo i ponašati. RH pripada regiji jugo-istočne Europe i treba biti partner zemljama koje su u procesu pristupanja EU ali usklađivanje politika i stavova treba biti u Bruxellesu sa ostalim zemljama članicama. Situacija u kojoj se na granice između zemalja članica postavlja žičana ograda je sramotno i nedopustivo a upravo to su Slovenija i Mađarska napravile Hrvatskoj.

[622] Leaders' Meeting on refugee flows along the Western Balkans Route Leaders' Statement http://ec.europa.eu/news/2015/docs/leader_statement_final.pdf

4. POLITIKE NA RAZINI EU U SEGMENTU SIGURNOSTI U VEZI PROBLEMA NELEGALNIH MIGRACIJA

Razvoj sigurnosti granica na europskoj razini vidljiv je kroz izmjene europskih osnivačkih ugovora u posljednjih dvadeset godina[623]. Počeci su bili vrlo općeniti, bez jasnih obveza zemalja članica dok je danas to područje potpuno u nadležnosti europskih institucija. Kako rastu globalni sigurnosni izazovi, tako se mogu očekivati razvoj i napredak tog područja na europskoj razini, a tome u prilog govore i znatna financijska sredstva koja EU stavlja na raspolaganje članicama za kontrolu vanjske granice. Također, europske agencije iz nadležnosti unutarnjih poslova dobivaju sve veće ovlasti na teritoriju EU, čime pitanja unutarnje sigurnosti izlaze iz isključive nadležnosti zemlje članice i dobivaju mnogo širu dimenziju[624]. Unatoč javnoj percepciji da su "šengenska pitanja" samo u nadležnosti granične policije, ona potpadaju i pod nadležnost unutarnjih poslova, pravosudnu i carinsku suradnju, zaštitu osobnih podataka, te stoga zemlji nakon ulaska u EU treba neko vrijeme da postane punopravna članica šengenskih sporazuma. Granična kontrola ne može podnijeti teret odgovornosti za sigurnost cijele EU. S druge strane, nedovoljna i neučinkovita kontrola povećava rizik od nezakonitih migracija i svih oblika prekograničnog kriminala. Upravo zato upravljanje granicom u sigurnosnom smislu mora biti sposobno odgovoriti na sve prijetnje koje su povezane s granicom.[625]

Politike u EU od njezinog nastanka[626] početno su se razvijale u političkom i ekonomskom segmentu gdje su nositelji sigurnosti bili vojska i vojno udruživanje unutar NATO saveza te je promišljanje sigurnosti bilo uvjetovano ideološkom blokovskom podjelom. Politike na području zajedničke unutarnje sigurnosti su se počele razvijati kasnije. Kad analiziramo politiku EU po pitanju nezakonitih migracija, potrebno je osvrnuti se na razvoj politika koje su tome prethodile. Politike Europske unije po navedenom pitanju povezane su ili se naslanjaju na dokumente donesene od strane drugih institucija. U tom sislu može se spomenuti Konvencija Ujedinjenih naroda protiv međunarodnog organiziranog kriminaliteta i njezinih protokola iz Palerma iz 2000. godine, Protokola o prevenciji, suzbijanju i kažnjavanju trgovine ljudima, posebno ženama i djecom i Protokola protiv krijumčarenja migranata kopnom, morem i zrakom.[627]

Implementirane su značajne mjere kontroliranja nezakonitih migracij koje su uslijedile tehnološkim napretkom, čvršćom suradnjom policijskih tijela, razmjenom informacija te stvaranjem zajedničkih baza podataka.[628] Između svih raspoloživih mjera žarište se može staviti na razvoj operativnih sposobnosti, osnivanje novih agencija te proširivanje okvira rada

---

[623] Calestini, B. (2007). *European Police Law Handbook*. Rim: Laurus Robufo.
[624] Dragović, F. (2012). Kako čuvati europske granice? Političke analize, 3, 12, 12-17. (Tema broja: Nacionalna i europska sigurnost).
[625] Bertozzi, S. (2008). Schengen: Achievements and Challnges in Mannaging an Area Encompassing 3.6 milion km². CEPS Working Document, 284.
[626] Uključujući preteče EU – Europsku Ekonomsku zajednicu i Europsku zajednicu.
[627] Dragović, F. (2012). Kako čuvati europske granice? Političke analize, 3,12, 12-17.
[628] Bigo D. i Guild E. (2005). Controlling Frontiers: Free Movement into and within Europe. *Ashgate Publishing Limited, UK.*

nezakonitih migracija te unapređenje postojećih sustava i uspostave i kreiranja novih rješenja.[629]

Pod razvojem operativnih sposobnosti podrazumijeva se posebno ključni dio implementiranja strateških ciljeva EU po pitanju nezakonitih migracija. Program razvoja Integriranog upravljanja granicama na razini EU je dugoročan proces koji određuje i unapređuje srednjoročne i dugoročne ciljeve za poboljšanje suradnje unutar službi, međuagencijske i međunarodne suradnje u agencijama uključenima u upravljanje granicama, a sve s namjerom ostvarivanja boljeg sustava upravljanja granicama. Viznim informacijskim sustavom osigurana je efikasna protočnost podataka između zemalja članica EU o vizama. Sustav olakšava provjeru o tražiteljima viza i azila kako na vanjskim granicama EU, tako i unutar zemalja EU te u jednu mrežu uvezuje jedinstveni centralni sustav EU i nacionalne baze podataka. Na taj način doprinosi unutarnjoj sigurnosti zemalja članica i pospješuje borbu protiv nezakonitih migracija. Važne mjere koje služe vraćanju nezakonitih migranata su Ugovori o povratku i Sporazumi o readmisiji. Međunarodni centar za razvoj migracijske politike vjeruje kako su Ugovori o povratku i Sporazumi o readmisiji nelegalnih migranata postali važan alat država po pitanju izazova nezakonitih migracija.[630]

Osnivanje agencija te odbora i proširivanje njihova djelokruga rada po pitanjima nezakonitih migracija predstavlja značajnu komponentu za provođenje sigurnosnih politika EU jer na strateškoj razini uvezuju donositelje odluka, kao što pospješuju i taktičku razinu razmjene svih vrsta podataka. Među najznačajnijima potrebno je izdvojiti neke od njih. Stalni odbor za operativnu suradnju na području unutarnje sigurnosti[631] osnovan je 2010. godine s namjerom razvoja, nadzora i implementacije Unutarnje strategije sigurnosti EU. U tu svrhu pokriva sigurnosne aspekte integriranog upravljanja granicama gdje je potrebna i pravosudna suradnja u kaznenim stvarima. Strateški odbor za migracije, granice i azil[632] je osnovan kao dio novih radnih struktura za pripremu rasprava Vijeća EU-a s obzirom na pitanja migracija, granica i azila. Zadaće odbora koji se sastoji od viših dužnosnika su usklađivanje pitanja strateških smjernica po pitanjima koja se odnose na migracije, granice i azil. Sa sličnim okvirom djelatnosti je osnovan i Koordinacijski odbor za policijsku i pravosudnu suradnje u kaznenim stvarima[633] čija je zadaća usklađivanje strateških smjernica Vijeća po pitanjima policijske i pravosudne suradnje u kaznenim stvarima. Frontex je agencija EU-a sa sjedištem u Varšavi koja je specijalizirana za koordinaciju operativne suradnje između država članica u području granične sigurnosti. Agencija nema operativnu djelatnost već se njezin rad temelji na razmjeni podataka. Europski policijski ured (Europol) bavi se obavještajnom djelatnošću u području kriminalističke suradnje između država članica Unije. Cilj mu je unaprijediti suradnju na sljedećim područjima: krijumčarenje droga, ljudi, ukradenih vozila, radioaktivnih

[629] Dragović, F., Mikac, R. (n.d.). Fenomen nezakonitih migracija kao jedan od ključnih sigurnosnih izazova Europske unije, Ministarstvo unutarnjih poslova Republike Hrvatske.
[630] International Centre for Migration Policy Development (2011). "Yearbook on Illegal Migration, Human Smuggling and Trafficking in Central and Eastern Europe", Vienna.
[631] Standing Committee on operational cooperation on internal security – COSI
[632] Strategic Committee on Immigration, Frontiers and Asylum – SCIFA
[633] The Coordinating Committee in the area of police and judicial cooperation in criminal matters – CATS

i drugih nuklearnih tvari; trgovanja ljudima; dječja pornografija; krivotvorenje novaca i pitanje migracijskih mreža. Za pitanja azila osnovana je EASO agencija sa sjedištem na Malti.

Konstantno unapređenje postojećih sustava, zakonskih rješenja i uspostava novih instrumenata važan je segment u realizaciji strateških planova i vizija. Proces unapređenja Schengenskog aquisa i vanjskih granica stalna je obveza i živa materija unutar Unije. Dodatno treba postrožiti mjere nezakonitog zapošljavanja imigranata jer postojeća siva ekonomija djeluje kao faktor koji privlači brojne migrante.[634] Bolja horizontalna i vertikalna koordinacija svih nadležnih tijela uz intenzivnu suradnju sa zemljama članicama je jedini način koji može dati zadovoljavajući rezultat.

5. ZAKLJUČAK

Područje Slobode, sigurnosti i pravde u okviru Europske unije je nesumnjivo jedno od najvećih postignuća u posljednja dva desetljeća (prvenstveno uspjeh postignut kroz Schengenski sporazum te protokol i kontrolu vanjskih granica). Međutim, Europska unija se danas nalazi pred raskrižjem jer žurno mora uskladiti nekoliko različitih višedimenzionalnih platformi po pitanju migracija poput konherentne migracijske politike prihvatljive svim državama članicama; apsorpcijske mogućnosti prihvata migranata i održivost društvene kohezije unutar europskih država; razvojnih i zdravstvenih aspekata migracija; koncepta multikulturalnosti; poštivanja i zaštite temeljnih ljudskih prava; zajedničkih mehanizama koje su mukotrpno desetljećima gradile članice Unije; problema nezakonitih migracija i pojavnosti kriminalnih aktivnosti vezanih uz nezakonite migracije; prijetnji od terorizma i radikalizacije. Posebnu pozornost će biti potrebno posvetiti regulaciji i kontroli migracijskih pritisaka te zaštiti ljudskih prava ugroženih migranata, a da se pritom ne narušava unutarnja sigurnost Unije i pojedinih zemalja članica te instituti koje su izgradile države članice Unije. Kao poseban izazov javlja se integracija migranata i njihovo prihvaćanje vrijednosti koje su uspostavljene u određenim sredinama, a pri tom je osobito važna integracija i prihvaćanje od strane lokalne zajednice. Nadalje, vidljivo je da teret prihvata nije kvalitetno raspoređen, to djelomice ovisi i o samim izbjeglicama koji uglavnom žele u Njemačku, što dodatno usložnjava situaciju na razini EU. Ukoliko se priljev izbjeglica nastavi u većem opsegu, mnoge države će vjerojatno uvesti ponovne kontrole granica i rješavati ova pitanja na nacionalnoj razini što je veoma loše rješenje. Postoji prijetnja da cijeli sustav zajedničke kontrole vanjske granice Europske unije u najmanju ruku postane upitan ili bude derogiran. Ova kriza je pokazala svu ranjivost Europe i nedostatke kada se radi o migracijskim kretanjima budući da su pojedine države ostavljene da se same nose s krizom.

Izbjeglička kriza i sigurnosni rizici za EU i za Republiku Hrvatsku su evidentni. Stoga je potrebno intenzivirati raspravu u EU kako bi sve članice u konačnici mogle zajednički postupati i i zauzeti zajednički stav. Uslijed aktualne razjedinjenosti postojeći sustav međunarodne pomoći izbjeglicama može biti ozbiljno narušen. Naime, potrebno je pomoći državama koje prve dolaze u dodir s izbjeglicama i to u vidu pružanja materijalne pomoći

[634] Dragović, F., Mikac, R. (n.d.). Fenomen nezakonitih migracija kao jedan od ključnih sigurnosnih izazova Europske unije, Ministarstvo unutarnjih poslova Republike Hrvatske.

koja se odnosi na izgradnju izbjegličkih ili prihvatnih kampova, slanje dodatnog broja policajaca, službenika za prihvat, liječnika i sl. Također, nužno je uputiti jasne i nedvosmislene poruke izbjeglicama u segmentu ostvarivanja njihovih prava putem medija i diplomacije. Potrebno je pojačati aktivnosti na diplomatskom i vojnom planu s ciljem podizanja razine sigurnosti u državama odakle izbjeglice dolaze. Ne bi se smjela zanemariti ni pomoć trećim zemljama koje također primaju izbjeglice (posebno Turska).

Posebno je nužno pojačati borbu protiv krijumčara ljudi i u tom smislu drastično povećati kazne zajedničkim radom europskih agencija, nacionalnih policija zemalja Europske unije, kao i trećih država. U konačnici, potrebno je potaknuti suradnju obavještajnih agencija zemalja EU i trećih država kako bi se prikupile kvalitetne informacije o mogućim pripadnicima organiziranih kriminalnih skupina ili terorističkih organizacija koji pod krinkom statusa izbjeglica pokušavaju ući u Europsku uniju te pojačati mjere na suzbijanju radikalizacije i ekstremizma. Integracija imigranata koji dolaze iz drugih civilizacijskih okruženja je stoga krucijalni problem, a to je područje u kojem su se dogodili najveći propusti s obzirom da je značajan broj osoba iz EU otišao ili kontinuirano odlazi u ratna područja čineći zločine te se posljedično potiču i na počinjenje terorističkih napada na tlu EU.

LITERATURA

Bertozzi, S. (2008). Schengen: Achievements and Challnges in Mannaging an Area Encompassing 3.6 milion km². CEPS Working Document br. 284.

Bigo D. i Guild E. (2005). *Controlling Frontiers: Free Movement into and within Europe*. Ashgate Publishing Limited, *UK*.

Calestini, B. (2007). *European Police Law Handbook*. Rim: Laurus Robufo.

CRS Report for Congress, RL31019, Terrorism: Automated Lookout Systems and Border Security Options and Issues, http://www.fas.org/irp/crs/rl31019.pdf

Dragović, F. (2003). *Nezakonite migracije – sigurnosni fenomen kraja 20. Stoljeća*. Zagreb: ministarstvo unutarnjih poslova republike hrvatske.

Dragović, F. (2012). Kako čuvati europske granice?, *Političke analize*, 3(12), 12-17.

Dragović, F., Mikac, R. (n.d.). Fenomen nezakonitih migracija kao jedan od ključnih sigurnosnih izazova Europske unije, Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske.

EU Schengen Catalogue – External borders control, Removal and readmission: recomendacion and best practices, Council of the European Unuion, General Secreteriat, February 2002. SCH-EVAL 1, COMIX 4, http://ue.eu.int/jai/default.asp?lang=eu.

Gosh, B. (1998). *Social and Economic Consequences of Irregular Migration*, Prezentacija na Konferenciji o migracijama u Beču, 25. do 27. studenog 1998.

Gosh, B. (1999). Irregular Migration, Migration News, 6 (1), January 1999.

Grizold, A. (1998). Međunarodna sigurnost, teorijsko-institucionalni okvir, Zagreb: Fakultet političkih znanosti Sveučilišta u Zagrebu.

Hellenthal, M. (1998). *Granična sigurnost - kamen temeljac unutarnje sigurnosti*, Izbor, 2-3., Zagreb: MUP.

International Centre for Migration Policy Development (2011). Yearbook on Illegal Migration, Human Smuggling and Trafficking in Central and Eastern Europe, Vienna.

Loescher, G. (1995). International security and population movements, The Cambridge Survey of World Migration, edited by Robin Cohen, University of Warwick, Cambridge University Press, 557 – 560.
Strategija nacionalne sigurnosti Republike Hrvatske, "Narodne novine", broj 32/02.
Strategija nacionalne sigurnosti Republike Hrvatske, "Narodne novine", broj 32/02.
Strategija nacionalne sigurnosti Republike Hrvatske, "Narodne novine", broj 32/02.
Strategija nacionalne sigurnosti Republike Hrvatske (2002.) Zbirka propisa i strateških dokumenata iz područja obrane.
Trauner F., Kruse I. (2008.) Visa Facilitation and Readmission Agreements: Implementing a New EU Security Approach in the Neighbourhood'', CEPS Working Document No. 290/April 2008, prikazano na: http://www.ceps.eu/book/ec-visa-facilitation-and-readmission-agreements-implementing-new-eu-security-approach-neighbour (pristupljeno: 26.11.2015.).

Jure Tadić
Filip Dragović
Tonči Tadić

MIGRANT CRISIS AND SECURITY CONCERNS FOR THE EU

Summary

The European Union is facing today the largest uncontrolled influx of migrants and refugees in its history so that term migrant and refugee crisis is well founded. The causes which have led to the explosion of the migrant crisis so to speak in 2015 are diametrically opposed: the escape from the suffering of war, the search for a better life, leaving dysfunctional states and escape from various forms of extremism and terrorism. It is estimated that in 2000 there were about 150 million migrants in the world; ten years later the numbers reached 214 million, assuming an increase to 405 million by 2050. The main migration flows are mostly directed to highly developed countries and areas, whereby the European Union has been the most desirable and most easily attainable destination over the last few years. Other target countries, primarily the United States, Canada and Australia, are unreachable to many migrants due to their distance and increased border controls. Regardless of the measures taken and legal restrictions imposed, the huge and primarily uncontrolled influx of (illegal) migrants into the European Union during 2014 and 2015 has brought both this issue and the issue of border control and security into the focus of protection of national interests of certain countries. Thus, the question of internal security of some countries now is associated with migrants, that is, with their uncontrolled influx and a possible impact on the security, the economic and political situation in the country. It can be stated that the refugee crisis has not only arrived at the door of Croatia and the EU, but that it has also affected this area with all its risks as such. It seems that the refugee crisis has never been more topical than it is today, due to the large influx of both migrants and refugees from the Middle East, whose final destination is the European Union. However, it is evident that the states and EU institutions have recognized too late or more precisely have underestimated the problem of migration as a phenomenon which carries a huge security risk. Besides, stricter controls at external EU

borders, primarily at its southern borders, have been addressed only partially, and have not yielded the expected results. The lack of common procedures of European states and failure to take concrete political views on this issue has been an aggravating circumstance for an efficient solution of this crisis.

Key words: *refugees, migrant and refugee crisis, security risks, migrants, refugees, illegal migration.*

PREGLEDNI ZNANSTVENI RAD

Tunjica Petrašević[635]
Dunja Duić[636]

DIREKTIVA O EVIDENCIJI PODATAKA O PUTNICIMA (PNR) I ZAŠTITA PODATAKA U EU

Sažetak

Cilj je Direktive regulirati prijenos podataka iz evidenciji podataka o putnicima (PNR-a) na međunarodnim letovima od zračnih prijevoznika državama članicama i obradu tih podataka koju obavljaju nadležna tijela. Direktivom se utvrđuje da se prikupljeni podaci iz PNR-a mogu obrađivati samo u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela. Zračni prijevoznici će morati tijelima država članica dostaviti podatke iz evidenciji podataka o putnicima (PNR-a) za letove prema EU-u ili iz EU-a. Svaka država članica morat će uspostaviti takozvani odjel za informacije o putnicima, koji će primati podatke iz PNR-a od zračnih prijevoznika. Nacrt Direktive početkom 2016. godine ide na odlučivanje pri Europskom parlamentu i Vijeću. Nakon što Direktiva bude usvojena, države članice će imati dvije godine vremena da unesu Direktivu u svoje nacionalno zakonodavstvo. Otvorene dileme vezane uz prikupljanje, korištenje i čuvanje podataka u evidenciji podataka o putnicima (PNR): Koliko dugo će se čuvati podaci i u kojem obliku?, Hoće li podaci biti skriveni ili ne?, Hoće li podaci prikazivati identitet ili ne?, Na koji način je garantirano brisanje podataka nakon proteka predviđenog vremena za čuvanje podataka?, Opravdanost količine podatka koja se čuva ?

Ključne riječi: *evidencija podataka o putnicima, PNR, čuvanje podataka, direktive.*

1. UVOD

Na razni EU u tijeku je usvajanje nove direktive o evidenciji podataka o putnicima (tzv. PNR direktiva, skraćeno od ***P****assenger* ***n****ame* ***r****ecor*). *Ratio* PNR direktive je regulirati prijenos podataka iz evidencije podataka o putnicima (PNR-a) na međunarodnim letovima od zračnih prijevoznika državama članicama i obradu tih podataka koju obavljaju nadležna tijela.
Cilj ovog rada jest prikazati nacrt direktive i upozoriti na određene otvorene dileme vezane uz prikupljanje, korištenje i čuvanje podataka u evidenciji podataka o putnicima (PNR).
Direktivom se utvrđuje da se prikupljeni podaci iz PNR-a mogu obrađivati samo u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela. Zračni prijevoznici će morati tijelima država članica dostaviti podatke iz evidenciji podataka o putnicima (PNR-a) za letove prema EU-u ili iz EU-a. Svaka država članica morat

[635] doc. dr. sc. Tunjica Petrašević, prodekan za znanost i posijediplomske studije, Pravni fakultet Osijek, e-mail: tpetrase@pravos.hr
[636] dr. sc. Dunja Duić, poslijedoktorand, Pravni fakultet Osijek, e-mail: dduic@pravos.hr

će uspostaviti takozvani odjel za informacije o putnicima, koji će primati podatke iz PNR-a od zračnih prijevoznika. Nacrt Direktive početkom 2016. godine ide na odlučivanje pri Europskom parlamentu i Vijeću. Nakon što Direktiva bude usvojena, države članice će imati dvije godine da unesu Direktivu u svoje nacionalno zakonodavstvo.
Otvorene dileme vezane uz prikupljanje, korištenje i čuvanje podataka u evidenciji podataka o putnicima (PNR): Koliko dugo će se čuvati podaci i u kojem obliku?, Hoće li podaci biti skriveni ili ne?, Hoće li podaci prikazivati identitet ili ne?, Na koji način je garantirano brisanje podataka nakon proteka predviđenog vremena za čuvanje podataka?, Opravdanost količine podatka koja se čuva ?
Prije nego se upustimo u analizu nacrta Direktive, objasnit ćemo pravnu narav i učinke direktiva kao zakonodavnih akta Unije. Potom ćemo definirati pojam "osobni podatak" te se osvrnuti na europsko i hrvatsko zakonodavstvo o zaštiti osobnih podataka. Nakon toga, a u vidu teme ovog rada važno je prije detaljne analize zakonodavnog prijedloga PNR direktive razjasniti što je prekogranični prijenos podataka. Glavni dio rada je analiza nacrta Direktive. Na kraju se daju određene zaključne napomene i upozorava na određene probleme i u pogledu implementacije direktive i u pogledu njene primjene.
U poglavlju koje slijedi opisat ćemo pravnu narav i učinke direktiva kao zakonodavnih akta Unije.

2. PRAVNA NARAV I UČINCI DIREKTIVA KAO ZAKONODAVNIH AKTA UNIJE

Izvore prava EU možemo podijeliti na primarne i sekundarne. U primarno pravo ulaze Osnivački ugovori, opća načela prava i Povelja o temeljnim pravima EU-a.[637] U sekundarno pravo EU ulaze uredbe, direktive, odluke, preporuke i mišljenja. Nas prije svega zanimaju direktive kao zakonodavni instrument Unije.
Za razliku od Ugovora i uredbi koji su akti izravne primjene u državama članicama, direktive to nisu. Direktive (ili smjernice) definirane su kao akti koji, u pogledu rezultata koji se njima ostvaruje, obvezuju svaku državu članicu kojoj su upućeni, ali ostavljaju nacionalnim vlastima izbor forme i metode.[638] Države su obvezne direktivu prenijeti ili implementirati u svoj nacionalni pravni sustav. Država bira formu u kojoj će to učiniti, primjerice novi zakon, izmjena postojećeg ili podzakonski akt (npr. uredba Vlade), no akt kojim se prenosi direktiva mora imati pravno obvezujuću snagu.
Direktive u pravilu nemaju izravnu primjenu niti izravan učinak u nacionalnim pravnim sustavima. Zamišljeno je da ga one proizvode posredno, posredstvom nacionalnog zakonodavstva. No u slučaju propusta države da pravodobno (u ostavljenom roku) i ispravno (potpuno) implementira direktivu, one mogu biti izravno primijenjene pred nacionalnim institucijama, posebice sudovima i upravnim tijelima, ako su njima predviđena prava za

[637] Osnivački ugovori: Ugovor o funkcioniranju Europske unije (UFEU) i Ugovor o Europskoj uniji (UEU) (dalje: Ugovori) temeljni su dokumenti Europske unije u kojima se utvrđuje kompletna nadležnost Unije te obveze i prava država članica u okviru članstva u EU. Ugovori predstavljaju primarno pravo EU i nadređeni su nacionalnom pravu država članica. Sastavni dio Ugovora su i Povelja o temeljnim pravima, Protokoli i Izjave koji su pridruženi Ugovoru i imaju istu pravni snagu kao i Ugovori.
[638] Vidi čl. 288(3) UFEU.

pojedince (pravne i fizičke osobe). No direktive mogu iznimno proizvoditi samo izravne učinke u vertikalnim pravnim odnosima. U nastavku ćemo ovo objasniti.
Da bi neka direktiva uopće proizvodila izravni učinak, ona mora biti dovoljno jasna, precizna i bezuvjetna.
Vertikalni pravni odnos je odnos države članice i pojedinaca (fizičkih i pravnih osoba). Horizontalni pravni odnos je odnos između pojedinaca međusobno. Ugovori i uredbe imaju izravne vertikalne i horizontalne učinke. Direktive mogu proizvoditi samo vertikalne učinke i to jednosmjerno. Pojedinac može zahtijevati određeno činjenje od države, ali ne i obrnuto.
Sud EU je kako bi zaštitio pojedince u onim državama članicama koje nisu implementirale direktivu predvidio mogućnost izravnog učinka direktiva. Sud je odbio dati (priznati) izravni horizontalni učinak direktivama[639], ali kako bi disciplinirao ("kaznio") nesavjesne države članice, Sud je proširio pojam "države" za potrebe izravnog učinka direktiva. U tome kontekstu treba istaknuti kako je pojam "država" autonoman pravni koncept prava EU i podrazumijeva bilo koju granu vlasti (zakonodavna, izvršna i sudbena), bilo koju razinu vlasti (centralna, regionalna i lokalna) pa čak i privatne kompanije koje nadzire ili kontrolira "država".[640]
Zaključak je sljedeći: da bi se pojedinac mogao pozvati na direktivu koja nije implementirana u nacionalno pravo, druga strana u sporu mora biti država, s time da Sud EU vrlo široko shvaća pojam države.
Osim mogućnosti da proizvede izravni vertikalni učinak, posljedice neimplementacije direktive može biti i odgovornost države članice za štetu, odnosno može uslijediti tužba protiv države članice zbog povrede prava Unije. Tužbu za naknadu štete podiže pred nacionalnom sudom pojedinac koji je pretrpio štetu zbog neimplementacije ili pogrešne implementacije direktive. Postupak protiv države članice zbog povrede prava Unije pokreće se pred Sudom EU (konkretno Sudom) od strane druge države članice ili Europske komisije. U pravilu je Europska komisija ta koja pazi na poštovanje prava EU od strane država članica. U slučaju neimplementacije direktive, povreda je počinjenja nečinjenjem (propustom).

3. ZAŠTITA OSOBNIH PODATAKA U EU

3.1. Europsko i hrvatsko zakonodavstvo o zaštiti osobnih podataka

Iako Europska konvencija za zaštitu ljudskih prava (dalje: EKZLJP ili Konvencija)[641] izričito ne jamči pravo na zaštitu osobnih podataka, u praksi Europskog suda za ljudska prava (ESLJP) ovo pravo smatra se temeljno važnim za uživanje prava koje se jamči člankom 8. Konvencije koji propisuje pravo na poštovanje privatnog i obiteljskog života, doma i dopisivanja te se propisuju uvjeti u kojima su dopuštena ograničenja toga prava, tj. propisuje

[639] Sud odbija priznati horizontalni učinak direktiva uz obrazloženje: *"primijeniti prasku suda o izravnom učinku smjernica i na horizontalne odnose, značilo bi priznati zajednici ovlast da stvara obveze za pojedinca s trenutnim učinkom... koju ovlast ona ima samo kada je ovlaštena usvojiti uredbe"* (par. 24), ali *"nužno je spriječiti državu da iskoristi vlastiti propust da postupi u skladu s pravom zajednice"* (par. 49) – to je tzv. *estoppel doktrina*. Predmet 148/78 Ratti (1979) ECR 1629.
[640] Predmet C-188/89, *Foster v. British Gas* [1990] ECR I-3313. Vidi više u: Rodin, S., Ćapeta, T. (2008). Učinci direktiva Europske unije u nacionalnom pravu. Zagreb: Novi informator.
[641] Iako formalno nije izvor prava Unije, Sud EU štiti ljudska prava kako su ona zajamčena ustavnim tradicija država članica i EKLJP. Sve države članice Unije su ujedno i članice Vijeća Europe, a i sama Unija pregovora o pristupanju Konvenciji.

da se javna vlast neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te radi sprečavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih.[642] Europski sud u za ljudska prava (dalje: ESLJP) razmatrao je brojne slučajeve koji su se ticali zaštite osobnih podataka. Iz praske ESLJP proizlazi ne samo da članak 8 Konvencije obvezuje države na suzdržavanje od radnji kojima bi mogle prekršiti to pravo iz Konvencije, već i ih obvezuje na aktivno promicanje učinkovitog poštovanja privatnog i obiteljskog života.[643] U okviru Vijeća Europe postoji i posebna Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (Konvencija br. 108). Konvencija br. 108 je 1981. godine otvorena za potpisivanje. Sve članice EU su ratificirale Konvenciju, međutim ona je izmijenjena 1999. godine kako bi se omogućilo Europskoj zajednici da pristupi Konvenciji [644] i dodatno je izmijenjena 2001. godine protokolom koji uvodi odredbe o prijenosu podataka nečlanicama Vijeća Europe.[645] Republika Hrvatska ratificirala je Konvenciju 2005. godine i njezina su temeljna načela ugrađena u Zakon o zaštiti osobnih podataka (dalje u tekstu ZZOP).[646]

U zakonodavstvu EU opće pravilo koje definira pravo zaštite osobnih podataka propisano je člankom 16. UFEU (bivši članak 286. UEZ-a) te se navodi da svatko ima pravo na zaštitu svojih osobnih podataka.[647] Posebna pravila o pravu zaštite osobnih podataka nalazimo u glavama Ugovora vezanih uz područje sigurnosti. Tako članak 39. UEU regulira pravila vezana uz zaštitu osobnih podataka u okviru primjene zajedničke vanjske i sigurnosne politike (vanjska sigurnost Unije).[648] S druge strane, članci 87. i 88. UFEU reguliraju pravila veza uz

---

[642] (Europska) Konvencija za zaštitu ljudskih prava i temeljnih sloboda. MU 18/97., 6/99., 14/02., 13/03., 9/05., 1/06., 2/10. Više o EKZLJP vidi u: Omejec, J. (2014). *Konvencija za zaštitu ljudskih prava i temeljnih sloboda u praksi Europskog suda za ljudska prava. Strasbourški acquis*. Zagreb: Novi informator. Harris, D., O'Boyle, M., Warbrick, C. i Bates, E. (2009) *Law of the European Convention on Human Rights*, Oxford: Oxford University Press; Mowbray, A.(2012). *Cases, materials, and commentary on the European Convention on Human Rights*. Oxford: Oxford University Press. White, R. i Ovey, C. (2010). *The European Convention on Human Rights*. Oxford: Oxford University Press.

[643] Vidi: Malone protiv Ujedinjene Kraljevine, br. 8691/79, 2. kolovoza 1984.; Copland protiv Ujedinjene Kraljevine, br. 62617/00, 3. travnja 2007., I. protiv Finske, br. 20511/03, 17. srpnja 2008. K. U. protiv Finske, br. 2872/02, 2. prosinca 2008.

[644] Izmjene Konvencije o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (br. 108) kojima je omogućen pristup Europskim zajednicama, koje je Odbor ministara usvojio u Strasbourgu,15. lipnja 1999.; čl. 23. st. 2. Konvencije br. 108 u izmijenjenom obliku.

[645]Dodatni protokol uz Konvenciju o zaštiti pojedinaca pri automatskoj obradi osobnih podataka, koji se tiče nadzornih tijela i prekograničnih prijenosa podataka, CETS br. 181, 2001. Vidi više u: Priručnik o europskom zakonodavstvu o zaštiti podataka, Luksemburg: Ured za publikacije Europske unije, 2014, str. 1517.

[646] Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi s nadzornih tijela i međunarodne razmjene podataka, Narodne novine, Međunarodni ugovori 4/05. Zakon o zaštiti osobnih podataka, Narodne novine 106/12.

[647] Ugovori imaju prednost u primjeni pred nacionalnim pravnim pravilima. Koncept nadređenosti razvio se u sudskoj praksi Suda EU, gdje je nadređenost prvi put utvrđena u predmetu *Costa v. ENEL*. Sud je u toj presudi odredio da pravo koje proizlazi iz Ugovora ne može zbog svoje posebne i originalne prirode biti zamijenjeno domaćim zakonskim odredbama bez obzira na to kako su one formulirane, a da pri tome ne izgubi svoj karakter prava Zajednice (Unije) te da se pri tome ne dovede u pitanje pravni temelj Zajednice (Unije). Vidi više o nadređenosti EU prava u: Duić, D. (2012). Nadređenost europskog prava nad ukupnim pravnim sustavom država članica: analiza presude Kucukdeveci. *Pravni vjesnik*., 28 (1); 71-87.

[648] Čl. 39 UEU: U skladu s čl. 16. Ugovora o funkcioniranju Europske unije i odstupajući od njegova st. 2., Vijeće usvaja odluku u kojoj se utvrđuju pravila o zaštiti pojedinaca s obzirom na obradu osobnih podataka od

zaštitu osobnih podataka u okviru Područja slobode, sigurnosti i pravde (unutarnja sigurnost Unije), propisujući da su u policijsku suradnju uključena sva nadležna tijela država članica, koja uključuje policiju, carinu i druge službe zadužene za izvršavanje zakona specijalizirane u području sprečavanja, otkrivanja i istrage kaznenih djela. Za te potrebe Europski parlament i Vijeće, odlučujući u skladu s redovnim zakonodavnim postupkom, mogu utvrditi mjere koje se odnose na: prikupljanje, pohranu, obradu, analizu i razmjenu odgovarajućih podataka.[649] U okviru misije Europola čiji cilj je poduprijeti i ojačati djelovanje policijskih i drugih službi zaduženih za izvršavanje zakona država članica i njihovu uzajamnu suradnju u sprečavanju i suzbijanju teškog kriminaliteta koji pogađa dvije države ili više država članica, terorizma i oblika kriminaliteta koji utječu na zajednički interes obuhvaćen politikom Unije, Europski parlament i Vijeće uredbama usvojenima u skladu s redovnim zakonodavnim postupkom utvrđuju ustroj, funkcioniranje, područje djelovanja i zadaće Europola. Te zadaće mogu uključivati i prikupljanje, pohranu, obradu, analizu i razmjenu podataka, osobito onih koje su dostavila tijela država članica, trećih zemalja ili drugih subjekata.[650]

Uz navedeno a u pogledu zaštite temeljnih prava, Povelja o temeljnim pravima Europske unije (dalje: Povelja) u članku 8. regulira zaštitu osobnih podataka. Prema članku 8. Povelje svatko ima pravo na zaštitu svojih osobnih podataka. Takvi podaci moraju se obrađivati pošteno u za to utvrđene svrhe, na temelju pristanka osobe o kojoj je riječ ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom. Uz to, svatko ima pravo na pristup prikupljenim podacima koji se na njega ili nju odnose i pravo na njihovo ispravljanje.[651] Iz sudske prakse Suda EU proizlazi da Povelja jamči pravo zaštitu osobnih podataka, tj. da to pravo uključuje zaštitu svakog podatka koji se odnosi na identificiranog pojedinca ili pojedinca koji može biti identificiran. [652]

Međutim, dvije Izjave koje su dodane Ugovorima ograničavaju pravo na zaštitu podataka u dva slučaja. Izjava (2) o članku 16. UFEU navodi da kad god bi pravila o zaštiti osobnih podataka koja treba donijeti temeljem članka 16. mogla imati izravne posljedice za nacionalnu sigurnost, moraju se uzeti u obzir posebne značajke tog pitanja. Ona podsjeća da trenutno mjerodavno zakonodavstvo (Direktiva 95/46/EZ) sadržava posebna odstupanja u tom pogledu. Dakle riječ je o mogućnosti općeg ograničenja prava na zaštitu osobnih podatak, s obzirom na činjenicu da članak 16. UFEU propisuje opće obveze zaštite osobnih podataka. S druge strane, Izjava (21) specifično se odnosi na zaštitu osobnih podataka u područjima pravosudne suradnje u kaznenim stvarima i policijske suradnje te potvrđuje da se posebna pravila o zaštiti osobnih podataka i slobodnom kretanju takvih podataka u područjima pravosudne suradnje u kaznenim predmetima i policijske suradnje na temelju članka 16. UFEU mogu pokazati potrebnima zbog posebne naravi tih područja. [653]

---

strane država članica pri obavljanju aktivnosti u području primjene ovog poglavlja i pravila o slobodnom kretanju takvih podataka. Poštovanje tih pravila podliježe nadzoru neovisnih tijela.

[649] Čl. 87 (1) (2) UFEU.

[650] Čl. 88 (1) (2) UFEU.

[651] Čl. 8. Povelje o temeljnim pravima Europske unije.

[652] C-92/09 i C-93/09 *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen*, (2010) ECR I-11063. O obveznom zadržavanje podataka i privatnosti vidi više u: Dragičević, D, Gumzej, N. (2014). Obvezno zadržavanje podataka i privatnost. *Zbornik PFZ*. 64 (1), 39-80.

[653] Izjava (20) i Izjava (21)

Možemo zaključiti da temeljno pravo na zaštitu osobnih podataka iz članka 8. Povelje ipak nije apsolutno pravo, već ga treba promatrati s obzirom na njegovu funkciju u društvu. Navedeno je vidljivo iz Izjava koje su pridružene Ugovorima i potvrđeno u sudskoj praksi Suda EU .[654]

Osnovni zakonodavni akt o zaštiti podataka u Europskoj uniji su Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (dalje: Direktiva o zaštiti podataka) kojoj je cilj bio (i jest) uskladiti zaštitu osobnih podataka na nacionalnoj razini, tj. u okviru nacionalnog zakonodavstva država članica [655] i Uredba (EZ) br. 45/2001 o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka (Uredba o zaštiti podataka u institucijama Europske unije) kojom se osigurava zaštita osobnih podataka pri obradi osobnih podataka u institucijama EU.[656] S obzirom na to da jedan od osnovnih dokumenata EU o zaštiti podataka datira iz 1995. godine, a da je od toga doba tehnologija znatno napredovala, Europska komisija je 2012. godine predložila reformu zakonodavstva o zaštiti podataka, to je prije svega Opća uredba o zaštiti podataka koja je trenutno u zakonodavnom postupku prihvaćanja. [657]

U Republici Hrvatskoj pravo na sigurnost i tajnost osobnih podataka jamči se ponajprije Ustavom RH koji je u članku 37. propisano sljedeće: "Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom."[658] Temeljem ustavne odredbe o pravu na zaštitu osobnih podataka donesen je Zakon o zaštiti osobnih podataka. Zakonom se uređuje zaštita osobnih podataka te nadzor nad djelovanjem informatičkih sustava u državi.[659] Zakon o zaštiti osobnih podataka, kao temeljni akt u području zaštite osobnih podataka u RH također je u svim bitnim odredbama u skladu s Direktivom 95/46/EZ o zaštiti podataka. Kako je već navedeno, Republika Hrvatska je ratificirala Konvenciju br. 108 čije su odredbe uključene u ZZO, a i Europsku konvenciju koja je od 1997. godine postala dijelom hrvatskoga pravnog poretka te je u skladu s odredbom članka 141. Ustava RH po pravnoj snazi iznad zakona.[660]

Vezano uz hrvatsko zakonodavstvo o zaštiti osobnih podataka treba napomenuti, primjerice da je Ustavni sud u svoj praksi donio odluku o ukidanju pojedinih odredbi Zakona o kaznenom postupku zbog nesuglasnosti s jamstvima prava na poštovanje i pravnu zaštitu privatnog života te sigurnosti i tajnosti osobnih podataka.[661]

Možemo zaključiti iz navedenog da postoji opsežno zakonodavstvo vezanu uz zaštitu osobnih podataka u Europi. Pravo na zaštitu osobnih podatak treba se smatrati jednim od temeljnih

---

[654] Spojni predmeti C-92/09 i C-93/09, Volker i Markus Schecke GbR i Hartmut Eifert protiv Land Hessen, (2010) ECR I-11063, paragraf 56.

[655] Direktiva o zaštiti podataka, OJ L 1995 L 281, str. 31.

[656] Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka OJ L 2001 L 8.

[657] Prijedlog Uredbe Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (Opća uredba o zaštiti podataka), COM(2012) 11 konačno, Bruxelles, 25. siječnja 2012.

[658] Ustav Republike Hrvatske. Narodne novine 5/14. – pročišćeni tekst.

[659] Zakon o zaštiti osobnih podataka. Narodne novine 106/12.

[660] (Europska) Konvencija za zaštitu ljudskih prava i temeljnih sloboda. MU 18/97., 6/99., 14/02., 13/03., 9/05., 1/06., 2/10. Ustav Republike Hrvatske. Narodne novine 5/14.

[661] Odluka Ustavnog suda Republike Hrvatske br. U-I-448/2009 od 19. srpnja 2012. Narodne novine 91/12.

ljudskih prava. Razvilo se iz članka 8. EKZLJP, tj. iz prava na poštovanje privatnog i obiteljskog života, doma i dopisivanja, međutim u okviru zaštite temeljnih prava u Europskoj uniji postaje samostalno temeljno pravo koje se jamči člankom 8. Povelje. U skladu s navedenim zakonodavstvo Republike Hrvatske se treba smatrati usklađenim s europskim osnovama zaštite i regulacije osobnih podataka. Prije svega, Ustav RH sadrži posebnu odredbu o zaštiti osobnih podataka koja je u skladu s krovnim europskim dokumentima o zaštiti ljudskih prava (EKZLJP i Poveljom), uz to hrvatsko sekundarno zakonodavstvo (Zakon o zaštiti osobnih podataka) usklađeno je s europskim sekundarnim zakonodavstvom (Direktivom o zaštiti podataka). Valja očekivati da će Republika Hrvatska kao i do sada pri budućim izmjenama europskog zakonodavstva (u smislu prijedloga nove Uredbe o zaštiti osobnih podataka) slijediti dosadašnju dobru praksu.

3.2. Definicija pojma osobni podaci

Zakon o zaštiti osobnih podatka definira osobni podatak u članku 2. stavku 1. propisujući da je osobni podatak svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati (u daljnjem tekstu: ispitanik); osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi identifikacijskog broja ili jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet.[662] Ova definicija u skladu je sa zakonodavstvom EU koje definira osobni podatak u članku 2.a Direktive 95/46/EZ.[663] Definicija je važna zbog činjenice da mnoga imena nisu jedinstvena i za utvrđivanje identiteta osobe potrebni su dodatni identifikatori kako bi se osiguralo da se osoba ne zamijeni nekom drugom. Koji su to identifikatori utvrdio je Sud EU u svojoj praksi. U Predmetu C-275/06, *Promusicae*, Sud EU navodi da je neosporno da dostavljanje imena i adresa pojedinaca uključuje stavljanje na raspolaganje osobnih podataka, odnosno informacija koje se tiču identificiranih fizičkih osoba ili fizičkih osoba koje je moguće identificirati, u skladu s definicijom iz članka 2.a Direktive 95/46/EZ. Takvo dostavljanje informacija predstavlja obradu osobnih podataka prema članku 2(1) Direktive 2002/58, u vezi s člankom 2(b) Direktive 95/45/EZ.[664] U Predmetu C-101/01 *Kazneni postupak protiv Bodil Lindqvist* utvrđeno je da navođenje osobnih podataka različitih osoba i njihovih brojeva telefona, podataka o njihovom zaposlenju ili o njihovim hobijima na internetskim stranicama predstavlja obradu osobnih podataka.[665] U Spojenim predmetima *Volker i Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* u kojima je bilo riječ o objavi osobnih podataka o korisnicima poljoprivredne potpore, Sud zaključuje da se pravo na poštovanje privatnog života vezano uz obradu osobnih podataka iz članaka 7. i 8. Povelje tiče se bilo koje

---

[662] Čl. 2. st. 1. t. 1. Zakona o zaštiti osobnih podataka. Narodne novine 106/12.

[663] Čl. 2.a Direktiva 95/46/EZ: "osobni podaci bilo koji podaci koji se odnose na utvrđenu fizičku osobu ili fizičku osobu koju se može utvrditi ("osoba čiji se podaci obrađuju"); osoba koja se može utvrditi je osoba čiji je identitet moguće utvrditi, izravno ili neizravno, a posebno navođenjem identifikacijskog broja ili jednog ili više činitelja značajnih za njegov fizički, fiziološki, mentalni, gospodarski, kulturni ili socijalni identitet". Vidi više o zaštiti osobnih podataka u EU: Kuner, C. (2007). *European data protection law*. Oxford: Oxford University Press.; Rosemary, J.; Hamilton, A. (2012). *Data protection law and practice*. London: Sweet.

[664] C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España* SAU (2008) ECR I-00271, paragraf 45.

[665] C-101/01 *Criminal proceedings against Bodil Lindqvist,* (2003) ECR, I-12971, paragraf 27.

informacije, koja se odnosi na identificiranog pojedinca koji se može identificirati, dakle isključuje pravne osobe. [666]

3.3. Prekogranični prijenos osobnih podataka

U vidu teme ovog rada važno je prije detaljne analize zakonodavnog prijedloga Direktive o evidenciji podataka o putnicima (PNR) razjasniti i što je prekogranični prijenos podataka. Direktiva 95/46/EZ u članku 25(1) propisuje da postoji slobodan prijenos podataka među državama članicama i dozvoljava prijenos osobnih podataka trećim zemljama izvan Europske unije.

S obzirom na spomenute odredbe, već 2004. godine, u skladu s člankom 25(1) Direktive 95/46/EZ potpisan je Sporazuma između Europske unije i Sjedinjenih Američkih Država o obradi i prijenosu podataka iz evidencije podataka o putnicima (PNR) zračnih prijevoznika. Evidencija podataka o putnicima (PNR) uključuje imena, adrese, podatke o kreditnoj kartici i broj sjedala putnika u zračnom prometu. Prema zakonima SAD-a, zračne kompanije dužne su te podatke staviti na raspolaganje Ministarstvu domovinske sigurnosti prije polaska putnika (na letove u SAD ili iz njih).[667]

Međutim, Europski parlament vrlo brzo nakon sklapanja ovog sporazuma pokrenuo je postupak protiv Vijeća EU pred Sudom EU. U Predmetu C-317/04 i 318/04 *Europski parlament protiv Vijeća Europske unije*, Europski parlament traži poništenje Odluke Vijeća 2004/496/EZ, navodeći da Odluka krši temeljna načela Direktive, temeljna ljudska prava i načelo proporcionalnosti. Sud je utvrdio da PNR podatke prikupljaju zrakoplovne kompanije prilikom obavljanje djelatnosti (prodaja avionskih karata) koje spada u slobodu pružanja usluga. Obrada podataka koja je dogovorena u Odluci Vijeća 2004/496/ EZ sasvim je drugačije prirode, tj. odnosi na javnu sigurnost, obranu, nacionalnu sigurnost (uključujući gospodarsku dobrobit države kada se operacija obrade odnosi na pitanja nacionalne sigurnosti) i aktivnosti države u području kaznenog prava. S obzirom na to, Sud EU je utvrdio da Odluka Vijeća 2004/496/ EZ nije u skladu s Direktivom s obzirom na to da članak 3(2) Direktive propisuje da se Direktiva ne primjenjuj u navedenim situacijama. Iz tog razloga Sud EU je poništio Odluku Vijeća 2004/496/.[668] Nakon toga sa SAD-om potpisan je novi Sporazum 2007. godine, koje je revidiran 2012. godine i na snazi je do 2019. godine.[669] Novi sporazum ograničava svrhu korištenja informacija na borbu protiv ozbiljnih transnacionalnih zločina i terorizam i uspostavlja vremensko razdoblje od 6 mjeseci za zadržavanja podataka:

---

[666] Spojni predmeti C-92/09 i C-93/09, *Volker i Markus Schecke GbR i Hartmut Eifert protiv Land Hessen,* (2010) ECR I-11063, para 52.

[667] Odluka Vijeća 2004/496/EZ od 17. svibnja 2004., o potpisivanju sporazuma između Europske unije i Sjedinjenih Američkih Država o obradi i prijenosu podataka iz evidencije podataka o putnicima (PNR) zračnih prijevoznika Ministarstvu za domovinsku sigurnost Sjedinjenih Američkih Država, Uredu za carinsku i graničnu zaštitu, OL 2004 L183, str. 83, i Odluka Komisije 2004/535/EZ od 14. svibnja 2004. o adekvatnoj razini zaštite osobnih podataka sadržanih u Evidenciji imena putnika, putnika u zračnom prijevozu, dostavljenih Uredu za carinsku i graničnu zaštitu SAD-a, OL 2004 L 235, str. 11- 22.

[668] Spojeni predmeti C-317/04 i 318/04, *Europski parlament protiv Vijeća Europske unije (*2006) ECR I-04721, paragraf 57., 58. i 59.

[669] Odluka Vijeća 2012/472/EU od 26. travnja 2012. o sklapanju Sporazuma između Sjedinjenih Američkih Država i Europske unije o uporabi i prijenosu evidencije imena putnika Ministarstvu domovinske sigurnosti SAD-a, SL 2012 L 215/4., st. 5.-14.

nakon proteka šest mjeseci podaci se moraju maskirati i depersonalizirati.[670] Osim sa SAD-om, sporazumi o prijenosu i obradi podataka iz evidencija podataka o putnicima sklopljeni su s Kanadom 2006. godine i s Australijom 2011. godine. [671]

4. DIREKTIVA O EVIDENCIJI PODATAKA O PUTNICIMA (PNR)

Kako navodi Komisija: "Cilj je Europske unije osigurati da stanovnici žive u području slobode, sigurnosti i pravde, bez unutarnjih granica. Europljani moraju biti sigurni da je, kuda god se kretali unutar Europe, njihova sloboda i sigurnost dobro zaštićena, čime se u potpunosti poštuju vrijednosti Unije, uključujući vladavinu prava i temeljna prava."[672] Kako je Unija suočena s prijetnjom terorizma i prekograničnim kriminalom, nužna je snažnija suradnja država članica. Za te je prijetnje potreban učinkovit i usklađen odgovor na europskoj razini. Europski program sigurnosti stoga mora biti zajednički program Unije i država članica, rezultat čega bi trebalo biti područje unutarnje sigurnosti EU-a, gdje su ljudi potpuno zaštićeni u skladu s temeljnim pravima. Program bi trebao potaknuti, između ostalog, bolju razmjenu informacija, povećati operativnu suradnju i uzajamno povjerenje. Nas prije svega zanima razmjena informacija. Unija već ima niz instrumenata za olakšavanje razmjene informacija među nacionalnom tijelima za provedbu zakona ali oni nisu dovoljno iskorišteni.
Jedan od instrumenata je i tzv. Registar osobnih podatka putnika – PNR ("**P**assenger **n**ame **r**ecord"). Analizom informacija iz PNR-a koje se daju prilikom rezervacije karata i prijave za let olakšava se identifikacija putnika koji predstavljaju velik rizik, a ranije nisu bili poznati tijelima nadležnima za provedbu zakona. Podaci iz PNR-a pokazali su se nužnima za identifikaciju putnika koji predstavljaju velik rizik u kontekstu borbe protiv terorizma, trgovanja drogom, trgovanja ljudima, seksualnog iskorištavanja djece i drugih teških kaznenih djela.[673]
Podaci iz registra putnika (PNR) u naravi su neprovjerene informacije koje pružaju putnici, a sakupljaju i čuvaju zračni prijevoznici. U tzv. Stockholmskom programu Vijeće je pozvalo Komisiju da predstavi prijedlog uporabe tih podataka za sprečavanje, otkrivanje, istragu i kazneni progon kaznenih djela terorizma i teških kaznenih djela, na temelju kojeg je Komisija još 6. studenoga 2007. godine izradila nacrt Okvirne odluke Vijeća o korištenju podataka iz registra putnika (PNR) za svrhe za provedbu zakona. Ovaj prijedlog je bio predmet rasprave u radnim skupinama u Vijeću, međutim nakon stupanja na snagu Ugovora o funkcioniranju Europske unije (UFEU) 1. prosinca 2009. godine, ovaj nacrt je zastario.[674]

---

[670] Priručnik o europskom zakonodavstvu o zaštiti podataka. Luksemburg: Ured za publikacije Europske unije, 2014, str. 138.
[671] Vidi više: Reguliranje uporabe podataka iz registra putnika http://www.consilium.europa.eu/hr/policies/fight-against-terrorism/passenger-name-record/, (15. veljače 2016.)
[672] Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i odboru, regija, Europski program sigurnosti, Strassbourg, 28.04.2015., COM (2015) 185 final, str. 2.
[673] Ibid. str. 7.
[674] Nacrt Okvirne odluke Vijeća o korištenju podataka iz registra putnika (PNR) za svrhe za provedbu zakona, COM(2007) 654 final; Od stupanja na snagu Lisabonskog ugovora, Ugovor o Europskoj zajednici (UEZ) zamijenjen je Ugovorom o funkcioniranju Europske unije. Okvirne odluke kao pravni instrumenti više se ne koriste, tj. u nekadašnjem "trećem stupu" (policijska i pravosudna suradnja u kaznenim stvarima) europske institucije dobivaju supranacionalne zakonodavne ovlasti, što znači da EU institucije pravne akte (uredbe, direktive,odluke) u ovom području izmjenama Ugovora u Lisabonu donose u redovitom zakonodavnom postupku. O izmjenama koje donio Lisabonski ugovor vezano uz područje policijske i pravosudne suradnja u

Komisija je tako, na temelju članaka 82 (1)(d) i 87 (2)(a) UFEU, izradila nacrt Direktive Europskog parlamenta i Vijeća o uporabi podataka iz PNR-a za sprečavanje, otkrivanje, istragu i progon terorističkih kaznenih djela i ozbiljnog zločina (Direktiva o evidenciji podataka o putnicima (PNR) [675]

Članak 1. nacrta Direktive predviđa prenošenje podataka iz evidencije podataka o putnicima (PNR) zračnih prijevoznika i gospodarskih subjekata koji nisu zračni prijevoznici o putnicima na međunarodnim letovima s odredištem i polazištem u državama članicama te obradu tih podataka, uključujući njihovo prikupljanje, uporabu i čuvanje u državama članicama kao i razmjenu podataka među državama članicama te između država članica i Europola. Podaci iz PNR-a prikupljeni u skladu s ovom Direktivom mogu se obrađivati samo u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i određenih teških transnacionalnih kaznenih djela ili u svrhu sprečavanja neposredne i ozbiljne prijetnje javnoj sigurnosti. [676]

Prema prijedlogu Direktive zračni prijevoznici tijelima država članica morat će dostaviti podatke iz PNR-a za letove prema EU-u ili iz EU-a (međunarodni letovi). Njome će se također državama članicama omogućiti, ali ih se neće obvezati, da prikupljaju podatke iz PNR-a u vezi s odabranim letovima unutar EU-a. O tome će pojedina država dati izjavu Komisiji, a izjava će biti objavljena u Službenom listu EU.[677]

Direktiva predviđa da će države članice uspostaviti tzv. odjel za informacije o putnicima – tijelo nadležno za sprečavanje, otkrivanje, istragu ili kazneni progon kaznenih djela terorizma i teških kaznenih djela ili odjel takvog tijela da djeluje kao "Odjel informacija o putnicima" koji će primati podatke iz PNR-a od zračnih prijevoznika.[678] Pri tom odjelu (jedinici) mora se imenovati službenik za zaštitu podataka u Odjelu informacija o putnicima (engl. *Data Protection Officer*).[679] Prema prijedlogu direktive, svaka država članica donosi popis nadležnih tijela koja su ovlaštena za traženje ili primanje skrivenih podataka iz PNR-a ili rezultata sustavne obrade podataka iz PNR-a od strane Odjela informacija o putnicima s ciljem daljnjeg ispitivanja tih informacija ili poduzimanja odgovarajućih mjera isključivo u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških transnacionalnih kaznenih djela ili sprečavanja neposredne i ozbiljne prijetnje javnoj sigurnosti. [680]

Proces prihvaćanja nacrta direktive dio je redovitog zakonodavnog postupka. Ovaj postupak pretpostavlja suodlučivanje pri donošenju EU zakonodavstva u kojem sudjeluju Europski parlament i Vijeće EU, koji na prvom ili drugom čitanju prihvaćaju ili ne prihvaćaju zakonodavni prijedlog Europske komisije. Postupak suodlučivanja dio je EU zakonodavstva od 1982. godine, a izmjenama iz Lisabonskog ugovora je preimenovano

---

kaznenim stvarima vidi više u: Đurđević, Z. (2008). Lisabonski ugovor – prekretnica u razvoju kaznenog prava u Europi. Hrvatski ljetopis za kazneno pravo i praksu, 15 (2), 1077-1127.

[675] Nacrt direktive Europskog parlamenta i Vijeća o uporabi podataka iz PNR-a za sprečavanje, otkrivanje, istragu i progon terorističkih kaznenih djela i ozbiljnog zločina (Direktiva o evidenciji podataka o putnicima (PNR), COM(2011) 32 završno, Bruxelles, 2. veljače 2011.

[676] Vidi čl. 1. nacrta Direktive.

[677] Vidi čl. 1.a.

[678] Vidi čl. 3.

[679] Vidi čl. 3.a (Amandman 35. Odbora za građanske slobode, pravosuđe i unutarnje poslove Europskog parlamenta).

[680] Vidi čl. 5.

u redovni zakonodavni postupak i postalo je osnovni postupak za donošenje odluka (primjenjuje se u otprilike 85 politika EU).[681]

Nacrt Direktive datira iz 2011. godine i nekoliko je puta njegovo prihvaćanje bilo blokirano pri Odboru za građanske slobode, pravosuđe i unutarnje poslove Europskog parlamenta čiji su članovi iznosili prigovore vezane uz zaštitu temeljnih prava na zaštitu osobnih podataka, privatnost i nediskriminaciju. Međutim, s obzirom na političku situaciju u Europskoj uniji (migracijsku krizu i terorističke napade koji su se dogodili u Parizu u 2015. godini), krajem 2015. godine održani su međuinstitucionalni pregovori između Europskog parlamenta, Vijeća EU-a i Komisije (trijalog), gdje je končano postignut kompromis u spornim pitanjima vezanih uz nacrt Direktive. Utvrđeno je da podaci iz PNR-a uključuju ime, datume putovanja, plan putovanja, informacije o karti, podatke za kontakt, putničku agenciju preko koje je let rezerviran, sredstvo plaćanja, broj sjedala i podatke o prtljazi.

Dodatno su razjašnjene postojeće dileme vezane uz prikupljanje, korištenje i čuvanje podataka u evidenciji podataka o putnicima (PNR) koje su još uvijek predmet rasprava u okviru EU institucija: Koliko dugo će se čuvati podaci i u kojem obliku?, Hoće li podaci biti skriveni ili neće?, Hoće li podaci prikazivati identitet ili ne?, Na koji način je garantirano brisanje podataka nakon proteka predviđenog vremena za čuvanje podataka?, Opravdanost količine podatka koja se čuva? Redom ćemo odgovoriti na postavljena pitanja.

Europski parlament predlagao je da se podaci iz PNR-a čuvaju u bazi podataka Odjela informacija o putnicima u razdoblju od 30 dana od njihovog dostavljanja. Međutim prihvaćen je kompromisni prijedlog o pohranjivanju: podaci će se na početku pohranjivati šest mjeseci, nakon čega će biti prikriveni(skriveni) i pohranjeni na dodatno razdoblje od četiri i pol godine, pri čemu će za pristup potpunim podacima postojati strog postupak. Države članice se obvezuju brisati podatke iz PNR-a po isteku roka od 5 godina, osim onih podataka koji su već ustupljeni nadležnim tijelima u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona, u kom slučaju je zadržavanje takvih podataka regulirano relevantnim nacionalnim zakonima.[682]

Vijeće je 4. prosinca 2015. godine odobrilo kompromisni tekst dogovoren s Europskim parlamentom o prijedlogu direktive. Nakon toga Odbor za građanske slobode, pravosuđe i unutarnje poslove Europskog parlamenta je 10. prosinca 2015. godine usvojio tekst sa 38 glasova za, 19 protiv i 2 suzdržana. Direktiva trenutno čeka na glasovanje u prvom čitanju na Europskom parlamentu, ako bude prihvaćena ide Vijeću na donošenje. Nakon donošenja direktive države članice će imati dvije godine da donesu zakone i druge propise koji su potrebni da se usklade s njome.[683]

---

[681] Čl. 289. i 294. UFEU.

[682] Drugo izvješće Odbora za građanske slobode, pravosuđe i unutarnje poslove. Izvjestitelj: Timothy Kirkhope http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2015-0248+0+DOC+XML+V0//HR; Direktiva o evidenciji podataka o putnicima (PNR) EU-a Vijeće potvrdilo dogovor s Europskim parlamentom http://www.consilium.europa.eu/hr/press/press-releases/2015/12/04-eu-passenger-name-record-directive/ (20. veljače 2016.)

[683] http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=&reference=2011/0023%28COD%29#tab-0 (20 veljače 2016.)

5. ZAKLJUČNE NAPOMENE

U prvome djelu rada su analizirane direktive kao zakonodavni akti Unije i njihovi učinci u nacionalnom pravu. Saga o direktivama je već dobro poznata. One u pravilu nemaju izravne učinke u nacionalnom pravu, već posredne, putem nacionalnih implementacijskih propisa. U slučaju propusta implementacije ili pogrešne ili nepotpune implementacije, direktiva može proizvesti izravni učinak, ali samo vertikalni i to jednostrani, tako da pojedinac nešto može zahtijevati od države, ali ne i obrnuto. Kao posljedica propusta implementacije može uslijediti i tužba pojedinaca pred nacionalnom sudom kojom oni potražuju naknadu štete koju su pretrpjeli. S druge strane, Komisija može tužiti državu pred Sudom EU i ako se utvrdi povreda, mogu uslijediti vrlo visoke novčane sankcije.

Kako je PNR direktiva još uvijek u fazi prijedloga i tek treba proći zakonodavnu proceduru, isključeni su bilo kakvi izravni učinci. No ako direktiva bude usvojena, od njena stupanja na snagu obvezni smo poduzeti sve mjere kako bi ispravno implementirali direktivu. Direktiva nameće obveze zračnim prijevoznicima, ali i nadležnim vlastima koje će prikupljati i obrađivati podatke. Pretpostavka je da će to kod nas biti Ministarstvo unutarnjih poslova. U tom smislu potrebno je uspostaviti odjel informacija o putnicima koji će primati podatke iz PNR-a od zračnih prijevoznika. Pri tome odjelu mora se imenovati službenik za zaštitu podataka.

U drugome djelu rad se bavi zaštitom osobnih podataka u EU. Na prvome mjestu smo se osvrnuli na Europsku konvenciju za zaštitu ljudskih prava. Iako nema izričitu referencu na zaštitu osobnih podatka, ovo pravo je od temeljne važnosti za uživanje prava koje se jamči člankom 8. Konvencije koji propisuje pravo na poštovanje privatnog i obiteljskog života, doma i dopisivanja, a Europski sud u za ljudska prava razvio je bogatu sudsku praksu. Dalje treba istaknuti kako je pod okriljem Vijeća Europe usvojena posebna Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (Konvencija br. 108) i njezina su temeljna načela ugrađena u Zakon o zaštiti osobnih podataka (dalje u tekstu ZZOP).

U primarnom pravu EU-a, opće pravilo koje definira pravo zaštita osobnih podataka propisano je u članku 16. UFEU gdje se navodi da svatko ima pravo na zaštitu svojih osobnih podataka. Posebna pravila o pravu zaštite osobnih podataka sadržana su u članku 39. UEU te člancima 87. i 88. UFEU. Posebno treba izdvojiti Povelju o temeljnim pravima gdje se u članku 8. izrijekom jamči pravo na zaštitu osobnih podataka. Iz sudske prakse Suda EU proizlazi da Povelja jamči pravo zaštitu osobnih podataka, tj. da to pravo uključuje zaštitu svakog podatka koji se odnosi na identificiranog pojedinca ili pojedinca koji može biti identificiran. No, može se zaključiti da temeljno pravo na zaštitu osobnih podataka iz članka 8. Povelje nije apsolutno pravo, već ga treba promatrati s obzirom na njegovu funkciju u društvu. Navedeno je vidljivo iz Izjava koje su pridružene Ugovorima i potvrđeno u sudskoj praksi Suda EU .

Osnovni sekundarni pravni akti o zaštiti (osobnih) podataka su Direktiva 95/46/EZ o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka i Uredba (EZ) br. 45/2001 o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka kojom se osigurava zaštita osobnih podataka pri obradi osobnih podataka u institucijama EU. Kako jedan od osnovnih dokumenata EU o zaštiti podataka datira iz 1995. godine, a od toga doba tehnologija

je znatno napredovala, Europska komisija 2012. predložila je reformu zakonodavstva o zaštiti podataka, prije svega to je Opća uredba o zaštiti podataka koja je trenutno u zakonodavnoj proceduri. Što se tiče hrvatskog zakonodavstva, pravo na sigurnost i tajnost osobnih podataka jamči se ponajprije Ustavom RH (čl. 37.) i Zakonom o zaštiti osobnih podataka. No tomu treba pridodati Konvenciju br. 108 čije su odredbe uključene u ZZOP te EKZLJP.
Možemo zaključiti iz navedenog da postoji opsežno zakonodavstvo vezanu uz zaštitu osobnih podataka u Europi. Pravo na zaštitu osobnih podatak treba se smatrati jednim od temeljnih ljudskih prava. No što je uopće "osobni podatak"? Zakon o zaštiti osobnih podatka definira osobni podatak u članku 2. stavku 1. propisujući da je osobni podatak svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati (u daljnjem tekstu: ispitanik); osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi identifikacijskog broja ili jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet. Ova definicija u skladu je sa zakonodavstvom EU.
U trećem dijelu rad analizira nacrt PNR direktive. Direktiva bi trebala pridonijeti boljoj razmjeni informacija između država članica i tako doprinijeti povećanju sigurnosti što je iznimno važno u doba kada je Unija suočena s prijetnjom terorizma i prekograničnim kriminalom. No PNR direktiva još nije niti usvojena, a izazvala je veliku pozornost i brojne kontroverze, ponajprije zato što će njena primjena izravno zadirati u temeljno ljudsko pravo na zaštitu osobnih podataka, privatnost i nediskriminaciju.

U tom smislu nužno je osigurati određene garancije:

- s obzirom na svrhu za koje se podaci iz PNR-a mogu obrađivati (procjena putnika prije dolaska prema prethodno utvrđenim kriterijima rizika ili kako bi se identificirale određene osobe; upotreba u posebnim istragama/kaznenim progonima; doprinos razvoju kriterija za procjenu rizika)
- s obzirom na razmjenu takvih podataka među državama članicama i između država članica i trećih zemalja
- s obzirom na pohranjivanje (podaci će se na početku pohranjivati šest mjeseci, nakon čega će biti prikriveni i pohranjeni na dodatno razdoblje od četiri i pol godine, pri čemu će za pristup potpunim podacima postojati strog postupak)
- osigurati zajedničke protokole i formate podataka za prijenos podataka iz PNR-a od zračnih prijevoznika tzv. odjelima za informacije o putnicima država članica te
- osigurati jake zaštitne mjere u pogledu zaštite privatnosti i osobnih podataka, uključujući ulogu nacionalnih nadzornih tijela i obvezno imenovanje službenika (ili povjerenika) za zaštitu podataka.

LITERATURA

Duić, D. (2012). Nadređenost europskog prava nad ukupnim pravnim sustavom država članica: analiza presude Kucukdeveci. *Pravni vjesnik*, 28 (1), 71-87.
Dragičević, D; Gumzej, N. (2014). Obvezno zadržavanje podataka i privatnost. *Zbornik PFZ*. 64 (1), 39-80.
Đurđević, Z. (2008). Lisabonski ugovor – prekretnica u razvoju kaznenog prava u Europi. *Hrvatski ljetopis za kazneno pravo i praksu*, 15 (2), 1077-1127.
Kuner, C. (2007). *European data protection law*. Oxford :Oxford University Press.
Harris, D., O'Boyle, M., Warbrick, C. i Bates, E. (2009). *Law of the European Convention on Human Rights*, Oxford . Oxford University Press.
Mowbray, A. (2012). *Cases, materials, and commentary on the European Convention on Human Rights*. Oxford: Oxford University Press.
Omejec, J. (2014). *Konvencija za zaštitu ljudskih prava i temeljnih sloboda u praksi Europskog suda za ljudska prava. Strasbourški acquis*. Zagreb: Novi informator.
Priručnik o europskom zakonodavstvu o zaštiti podataka. (2014). Luksemburg: Ured za publikacije Europske unije.
Rodin, S., Ćapeta, T. (2008). *Učinci direktiva Europske unije u nacionalnom pravu*. Zagreb: Novi informatior.
Rosemary, J.; Hamilton, A. (2012). *Data protection law and practice*. London: Sweet.
White, R. i Ovey, C. (2010). *The European Convention on Human Rights*. Oxford: Oxford University Press.

Zakonodavstvo

*(Europska) Konvencija za zaštitu ljudskih prava i temeljnih slobod*a. MU 18/97., 6/99., 14/02., 13/03., 9/05., 1/06., 2/10.
Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka. Narodne novine, Međunarodni ugovori 4/05.
Ustav Republike Hrvatske. Narodne novine 5/14. – pročišćeni tekst.
Zakon o zaštiti osobnih podataka. Narodne novine 106/12.
Direktiva o zaštiti podataka. OJ L 1995 L 281.
Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka. OJ L 2001 L 8.
Odluka Vijeća 2004/496/EZ od 17. svibnja 2004. o potpisivanju Sporazuma između Europske unije i Sjedinjenih Američkih Država o obradi i prijenosu podataka iz evidencije podataka o putnicima (PNR) zračnih prijevoznika Ministarstvu za domovinsku sigurnost Sjedinjenih Američkih Država, Uredu za carinsku i graničnu zaštitu. OL 2004 L183.
Odluka Komisije 2004/535/EZ od 14. svibnja 2004. o adekvatnoj razini zaštite osobnih podataka sadržanih u Evidenciji imena putnika, putnika u zračnom prijevozu, dostavljenih Uredu za carinsku i graničnu zaštitu SAD-a. OL 2004 L 235.
Odluka Vijeća 2012/472/EU od 26. travnja 2012. o sklapanju Sporazuma između Sjedinjenih Američkih Država i Europske unije o uporabi i prijenosu evidencije imena putnika Ministarstvu domovinske sigurnosti SAD-a. SL 2012 L 215/4.

Sudska praksa

Europski sud za ljudska prava

Malone protiv Ujedinjene Kraljevine, br. 8691/79, 2. kolovoza 1984.
Copland protiv Ujedinjene Kraljevine, br. 62617/00, 3. travnja 2007.
I. protiv Finske, br. 20511/03, 17. srpnja 2008.
K. U. protiv Finske, br. 2872/02, 2. prosinca 2008.
Sud EU
Predmet C-188/89, *Foster v. British Gas* [1990] ECR I-3313.
Predmet C-101/01 *Criminal proceedings against Bodil Lindqvist*, (2003) ECR, I-12971.
Predmet C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU* (2008) ECR I-00271.
Spojeni predmeti C-317/04 i 318/04, *Europski parlament protiv Vijeća Europske unije* (2006) ECR I-04721.
Spojeni predmet C-92/09 i C-93/09 *Volker i Markus Schecke GbR i Hartmut Eifert protiv Land Hessen*, (2010) ECR I-11063.

Tunjica Petrašević
Dunja Duić

DIRECTIVE ON THE USE OF PASSENGER NAME RECORD (PNR) DATA AND DATA PROTECTION IN THE EU

Summary

The aim of the draft Directive is to regulate the transfer of PNR data from airlines to national authorities, as well as their processing of such data. The draft Directive will allow, but not oblige, Member States to collect PRN data concerning selected intra-EU flights. The Directive stipulates that the information collected from the PNR can be processed only for the prevention, detection, investigation and prosecution of terrorist offenses and serious crimes. According to the draft Directive each Member State shall set up or designate a competent authority for the prevention, detection, investigation or prosecution of terrorist offences and serious crime to act as its Passenger Information Unit responsible for collecting PNR data from air carriers, storing and analysing them and transmitting the result of the analysis to the competent authorities. In early 2016 the European Parliament and the Council will formally adopt the text. From the day of its entry into force, Member States will have two years to transpose the Directive into national law. Open dilemmas regarding the collection, usage and storage of Passenger Name Record (PNR) data: how long will data be stored and in what form? Will the data be hidden or not? Will the data show identity or not? Are there guarantees that data will be deleted after the expiry of the stipulated time for storage? What is the justification for the amount of stored data?

Key words: *Passenger Name Record (PNR), data retention, Directive.*

PREGLEDNI ZNANSTVENI RAD

Dubravko Derk[684]
Barbara Prprović[685]
Nikolina Nemec[686]**.**

UTJECAJ AKTUALNIH MIGRACIJA NA EUROPSKU SIGURNOST KROZ PRIZMU STANJA I KRETANJA KRIMINALITETA

Sažetak

Ovaj rad temelji se na analizi aktualnih migracijskih procesa s ciljem utvrđivanja generatora migracija te uloge migranata kao dijela nekonvencionalnih sigurnosnih prijetnji kroz njihov mogući utjecaj na europsku sigurnost, posebno u kontekstu sekuritizacije migrantske krize i migranata kao sigurnosne prijetnje. Rad također problematizira i ukazuje na određene deficite institucija Europske unije, nedovoljno razvijene mehanizme i alate na institucionalnoj razini te s tim u vezi različitih gledišta i interesa unutar pojedinih država Europske unije glede migracijskih politika i zaštite vanjskih granica EU, kao i ukupne zaštite nacionalnih interesa država članica. U tom smislu kroz rad je izraženo traženje korelacija sigurnosnih, političkih i socioekonomskih odnosa ključnih aktera i njihova utjecaja kako na opću sigurnost s jedne strane građana i imigranata, tako i na ukupnu europsku sigurnost. Dosadašnja istraživanja migracija i njihovog utjecaja na sigurnost pokazala su da direktna veza između imigranata i povećanja kriminaliteta ne postoji, te da je uloga imigranata kao uzročnika kriminala ograničena. Rezultat razmatranja aktualnog stanja u EU pokazuje da se usljed ovih migracija u određenoj mjeri pojavljuju sigurnosne prijetnje i rizici posebno vezano uz terористički čin u Parizu, a u određenoj mjeri i drugim kaznenim djelima s elementima nasilja, što u ukupnosti na subjektivnoj razini kod građana EU ostavljaju dojam latentne nesigurnosti.

***Ključne riječi**: imigranti, sigurnost, nasilje, terorizam, kriminalitet, akulturacija.*

1. Uvod

Posljednja događanja posebno u gradovima s većim brojem novo pridošlih imigranata ukazuju da u srazu različitosti postoje ozbiljni sigurnosni rizici koji streme ka nasilju, izazivanju nereda i općoj socijalnoj nesigurnosti. Urbana getoizacija migranata kao posljedica promašenog projekta multikulturalizma u predgrađima velikih europskih konglomeracija, gospodarskih i političkih središta EU proizvodi novu prije svega socijalnu, a zatim i kulturnu i

[684] Dubravko Derk, Zagrebački holding, Maksimirska 71, 10000 Zagreb, dubravko.derk9@gmail.com
[685]Barbara Prprović, Sveučilište u Zagrebu, Hrvatski studiji, Borongajska 83d, 10000 Zagreb, prprovic.barbara@gmail.com
[686] Nikolina Nemec, Sveučilište u Zagrebu, Hrvatski studiji, Borongajska 83d, 10000 Zagreb, nemec.nikolina2@gmail.com

religijsku subkulturu koja je izvan društvene kontrole. S tim u vezi možemo postaviti pitanje proizlazi li propast projekta multikulturalnog modela integracije u Europi dijelom i zbog odsutnosti osjećaja tih imigranata pripadnosti zemlji u kojoj su rođeni, u kojoj žive i rade.

Legitimno je pitanje za utvrđivanje jesu li, a ukoliko jesu pod kojim uvjetima aktualne migracije i sigurnosna prijetnja. Okolnosti i posljedice terorističkog napada u Parizu iz studenog 2015. godine upućuju na zaključak kako migracijski procesi i migracije pogotovo ovakvih masovnih razmjera pod određenim uvjetima mogu biti i postati sigurnosno pitanje, a u širem smislu oni su nedvojbeno prijetnja sigurnosti i institucijama Europske unije i njezinim stanovnicima. Sukladno tome, države provode sve restriktivniju politiku te stvaratelji javnih politika i šira javnost migrante počinju percipirati kao sigurnosnu prijetnju što rezultira aktiviranjem sigurnosnih diskursa, tehnika i tehnologija nadzora te pojačanom represijom prema migrantima (Bigo, 2002, 2007; Tirman, 2004; Huysmans, 2006, Pozniak i Petrović, 2014). Na to ukazuju brojni sigurnosni indikatori s obzirom na prostor s kojeg imigranti dolaze te s obzirom na samu trasu njihova putovanja, dakako i događanja u državama primateljicama. Naime, na sve tri spomenute razine zabilježeni su ozbiljni sigurnosni događaji.

Predmet ovog rada je utjecaj aktualne migracijske krize i samih migranata na europsku sigurnost s obzirom na potencijalne sigurnosne prijetnje koje sa sobom nosi toliko široko kretanje ljudi. U prvom dijelu rada sagledavaju se migracije iz perspektive sigurnosnih prijetnji. Zatim se razmatraju aktualne teorije o utjecaju migracija na kriminal. U trećem dijelu istražen je utjecaj imigracija na kriminal, dok se četvrti dio odnosi na zaključke do kojih se došlo predmetnim razmatranjem.

Svrha rada je pregled ključnih teorija socijalne kontrole i njihova primjena u objašnjenju kriminalnog ponašanja imigranata s ciljem sagledavanja eventualne povezanosti imigracija i promjena u trendovima kretanja kriminala.

Pregled dostupne literature i podataka izvršen je korištenjem službene statistike i podataka Statističkog ureda Europske unije (EUROSTAT), Agencije Ujedinjenih naroda za pomoć izbjeglicama (UNHCR), Međunarodne organizacije za migracije (IOM) kao i drugih podataka dostupnih iz javnih izvora informiranja, portala i dnevnih novina, što ima brojna ograničenja pri donošenju zaključaka.

Praktična korisnost rada očituje se u pojašnjenju u javnosti stvorenog uvjerenja o utjecaju imigranata na porast kriminaliteta i s tim u vezi i stvorenog dojma o porastu nesigurnosti građana Unije.

2. Migracije kao sigurnosna prijetnja

United Nations Department of Economic and Social Affairs i Visoko povjerenstvo Ujedinjenih naroda za izbjeglice u svom izvješću Global Trends Forced Displacement in 2014. objavilo je podatak da imigranti danas čine oko 3% svjetske populacije što je oko 230 milijuna ljudi. Od toga oko 20%, dakle njih oko četrdesetak milijuna su ilegalni imigranti. Istovremeno prema njihovim podacima više od 60 milijuna ljudi prisilno su napustili svoje

domove najviše iz sigurnosnih razloga. Devedesetih godina prošlog stoljeća sigurnosni sustavi prepoznaju nove nekonvencionalne sigurnosne prijetnje državama: terorizam, migracije, proliferaciju, organizirani kriminal te ekološki kriminal. Tatalović i Lacović (2012) drže da sigurnosne ugroze kao što su terorizam, proliferacija oružja za masovno uništenje, transnacionalni organizirani kriminal, ekološki kriminal te ilegalne migracije zahtijevaju brz, koordiniran i sveobuhvatan odgovor. Kicinger (2004) polazi od pretpostavke da migracije postaju jedna od nekonvencionalnih sigurnosnih prijetnji i to zbog neviđenih razmjera ovog fenomena, budući su sve europske zemlje suočene s izazovima koji proizlaze iz migracijskih kretanja. Također, smatra da migracije mogu biti rizik za unutarnju sigurnost država gdje su kriminalne razine među imigrantima više nego među domaćom populacijom, posebno naglašavajući činjenicu da teroristi koriste migracijske kanale za prodore u pojedine države. U tom smislu, zbog svoje masovnosti i ekstremnih razmjera, aktualni migracijski procesi stavljaju na kušnju institucije EU i njihovu organiziranost da upravljaju ovakvim krizama, posebno što stavljaju na kušnju „male“ države u njihovu nastojanju da se nose s krizom. Da aktualna migracijska kriza nije smjela biti iznenađenje za EU i njezine institucije, jasno proizlazi iz Europske strategije sigurnosti iz 2003. godine koja naglašava kako Unija neće biti izložena vojnim tradicionalnim rizicima, već da su nove prijetnje odnosno sigurnosni izazovi vezani uz migracije, energiju i pitanja okoliša. Istovremeno ista strategija iz 2015. godine inzistira na efektivnoj suradnji i povjerenju između svih involviranih faktora, institucija i agencija EU, država članica kao i nacionalnih vlasti. Jedan od glavnih ciljeva strategije je razbijanje kriminalne mreže koja se bavi krijumčarenjem imigranata.

U svom teorijskom pristupu odnosa imigracija i sigurnosti Koser (2011) smatra kako se javne rasprave o povezanosti migracija i sigurnosti nastoje fokusirati na različite aspekte povezane s nacionalnom sigurnosti, razumijevane kao zaštita i promocija dobrostojećih građana i legalnih stanovnika države i teritorija. Percepcija migracija kao prijetnje za nacionalnu sigurnost porasla je u nedavnim godinama dijelom i kao odgovor na brzi porast međunarodnih imigranata pri čemu se posebno ističu neregularni ili ilegalni migranti. Također, smatra da su realne ili imaginarne veze prema terorizmu, organiziranom kriminalu ili zdravstvenim prijetnjama glavne percepcije ilegalnih migracija kao sigurnosne prijetnje. Kerwin (2014) ukazuje na činjenicu da okvir ljudske sigurnosti pomiče raspravu o migracijama izvan nacionalnih vrijednosti u prostor kriminalizacije migranata što uvjetuje kod svih aktera posebno imigranata i njihovu dodatnu nesigurnost.

Balkanska ruta obzirom na nove okolnosti dobiva i novu definiciju budući da je ovim kolektivnim imigracijama stavljena u funkciju globalnog organiziranog kriminala, krijumčarenja i terorizma. Balkanska ruta postaje alat koji su organizirane kriminalne grupe stavile na dispoziciju migrantima te ga dobro unovčile. Futo, Jandl i Karsakova (2005) smatraju kako prema nekim istraživanjima većina nezakonitih migranata danas pribjegava pomoći organiziranih krijumčara ljudi. Istražujući fenomen imigracija, Morehouse i Blomfield (2011) drže da su prema mišljenju mnogih upravo snaga gospodarstva i dostupnost poslova za neovlaštene migrante ključni čimbenici koji određuju koliko će migranata neovlašteno pokušati ući u europske zemlje.

3. Teorije o odnosu između imigracija i kriminala

Dosadašnja istraživanja utjecaja imigracija i imigranata na sigurnost i stanje kriminaliteta koja su provedena u Sjedinjenim Američkim Državama, Velikoj Britaniji i Njemačkoj kroz duži niz godina ukazuju na činjenicu da nema bitnih odstupanja u odnosu na porast kriminaliteta ili povećanje nesigurnosti građana u lokalnim zajednicama u kojima žive imigranti. Nekoliko je ključnih teorija koje upućuju i služe objašnjenju odnosa između migracija, imigranata i kriminala te objašnjenju obrazaca kriminalnog ponašanja u različitim imigrantskim skupinama i generacijama. Ove teorije usredotočuju se na različite čimbenike koje smatraju važnima u oblikovanju individualnog ponašanja i iskustva migracija.

Teorija samostalnog izbora

Bui (2009) ukratko opisuje kako su niske razine kriminala među prvim doseljenicima u SAD dovele su do pretpostavke da su ti doseljenici bili samoizabrani ekonomski pojedinci koji su imali nisku tendenciju prema kriminalu. To je poznato kao teorija samostalnog izbora čiji zagovornici tvrde da zbog činjenice kako su doseljenici napustili svoju domovinu i došli u SAD zbog ekonomskih prilika, većina ih je u SAD-u teško radila. Naravno, zbog njihovog interesa za dugoročni napredak, ponašali su se pristojno i izbjegavali su nevolje sa zakonom. Butcher i Piehl (2005) koristili su model ishoda na tržištu rada kako bi objasnili niske razine kriminala među imigrantima koji su došli u SAD nakon 1965. godine i podržali hipotezu samostalnog izbora. Kada je to moguće, imigranti izabiru preseljenje u zemlju u kojoj će njihova zarada biti veća, a takvi ekonomski rezultati mogu poslužiti kao zaštita protiv kriminalne aktivnosti.

Teorija socijalne strukture

Prema teoriji strukturalnog pritiska, razvijenoj od strane Mertona, materijalni uspjeh ovisi o obrazovanju i mogućnostima zaposlenja, koji nisu jednako dostupni svima, a kad legitimne mogućnosti nisu dostupne, zločin može biti inovativna alternativa postizanja materijalnih ciljeva. Zbog toga što su mnogi novi imigranti nekvalificirani i slabo obrazovani, a gospodarske mogućnosti ne prodiru u urbana geta gdje se mnogi novi doseljenici nastanjuju, zločin postaje vjerojatna opcija (Sellin, 1938). Teorija socijalne neorganiziranosti, koju su razvili Shaw i McKay (1942), naglašava nepovoljne društvene uvjete u urbanim getima koji olakšavaju slom ustanova zajednice i mehanizama društvene kontrole. Prema toj teoriji, siromaštvo, visoke razine prometa stanovništva, kulturna heterogenost i prisutnost velikog broja odraslih kriminalaca oslabljuju društveni nadzor i potiču delikvenciju. Jonjić (1985) napominje kako migracije stvaraju strukturalnu napetost koja izaziva individualnu i grupnu anomiju zbog nemogućnosti integriranja u društvenu strukturu većinskog stanovništva. Prema tome, imigracija povećava razinu zločina jer uzrokuje društvene promjene i stvara socijalnu neorganiziranost koja rezultira manje učinkovitim društvenim nadzorom (Bui, 2009).

Teorije utemeljene na kulturi

U objašnjenju migracijskih procesa važnu ulogu zauzima i teorija subkulture nasilja koja ispituje ponašanje i akcije različitih grupa unutar društva koje odbijaju ili se odvajaju od

tradicionalnih normi i svjetonazora većine (Nwalozie, 2015). Teoriju subkulture nasilja razvili su Wolfgang i Ferracuti (prema: Bui, 2009), a ona sugerira da isto kao što se siromašni prilagođavaju svojim strukturalnim uvjetima, nasilje može postati normalno i očekivano sredstvo rješavanja sporova u depriviranim i neorganiziranim zajednicama. Kulturna teorija sukoba, s druge strane, naglašava razliku između američkih zakona i kulturnih tradicija koje imigranti donose iz svojih matičnih zemalja. Sellin (1938) smatra kako kazneno pravo odražava vrijednosti i interese dominantnih skupina, dok sustav vrijednosti i normi među useljenicima može biti sasvim drugačiji. Kad su kulturni kodovi imigranata u sukobu s onima u društvu domaćina, ponašanje imigranata će biti označeno kao devijantno ili kriminalno.

Ekonomska teorija

Prema tradicionalnom ekonomskom modelu i teoriji kriminala koju su razvili Becker (1968) i Ehrlich (1973) postoje pojedinci koji racionalno odabiru između kriminala i ilegalnih aktivnosti usporedbom neto koristi od svake aktivnosti Pojedinci s lošim šansama na tržištu rada češće će biti uključeni u kriminalne aktivnosti što se može objasniti nedostatkom ekonomske i socijalne integracije etničkih manjina u društvo (Junger-Tas, 2001), dok kulturalna izolacija uzrokuje sumnje, nesporazume, mitove i neznanje (Champion i Rush, 1997). Na primjer, mlađi muškarci koji su napustili školu bez kvalifikacija vjerojatno imaju različite kriminalne sklonosti od onih iskusnih profesionalaca s diplomskim stupnjem. Zamislimo pretpostavku prema kojoj imigranti misle da je vjerojatnost njihova uhićenja puno veća nego počinitelja rođenih u Velikoj Britaniji, i još to povezano sa strahom da će biti deportirani. To će u svakom slučaju imigrante dijelom odvratiti od kriminalnog ponašanja jednako kao i otežan pristup tržištu rada i njihove niže plaće od rođenih u Velikoj Britaniji. No, McCarthy i Hagan (1995, 2001) smatraju da kriminalni uspjeh snažno ovisi o specifičnim kompetencijama koje oni nazivaju kriminalnim kapitalom. To znači da migranti neće razvijati kriminalnu karijeru u državi u koju emigriraju unatoč nezaposlenosti i teškim životnim uvjetima ukoliko ne posjeduju kriminalni kapital.

Perspektive akulturacije i asimilacije

Akulturacija ili kulturna asimilacija odnosi se na promjene u stavovima i/ili ponašanjima, koje nastaju kao rezultat kontakata s drugim kulturama. Imigrantima i njihovoj djeci kulturne promjene događaju se na brojnim dimenzijama, uključujući jezik, kulturna uvjerenja, vrijednosti, ponašanja, odanost i osjećaj pripadnosti kulturi domaćina, ali i predanosti kulturi podrijetla. Model klasične asimilacije koji predlaže Gordon tvrdi da su akulturacija i prihvaćanje od strane društva domaćina uvjeti za društvenu i gospodarsku mobilnost. Nedostatak akulturacije smatra se čimbenikom koji doprinosi kriminalu i delikvenciji među useljenicima koji nemaju znanja o novim zakonskim normama, a time niti sposobnost da se prilagode novoj ekonomiji. (Bui, 2009)

Bui (2009) isto tako opisuje kako su otkrića istraživanja o niskim razinama kriminala i delikvencije među strancima izazov klasičnom modelu asimilacije i sugeriraju da akulturacija također ima negativne posljedice. Nedavna literatura pokazuje da što duže imigranti i njihova djeca žive u SAD-u, oni više postaju predmetom gospodarskih i društvenih snaga kao što su visoke stope raspadanja obitelji i upotrebe različitih supstanca, ponašanja koja su među

autohtonim narodom povezanima s kriminalnim ponašanjem. Osim toga, dužim vremenom i socijalizacijom u američkim ustanovama, susjedstvu i kulturi mladih, djeca imigranata sve bolje usvajaju norme ponašanja u društvu domaćina, uključujući dobra i rizična ponašanja.

Perspektiva segmentiranih asimilacija

Perspektiva segmentiranih asimilacija razvijena je s naglaskom na promjene u američkom gospodarstvu i na tržištu rada i na to kako oni utječu na iskustvo nedavnih useljenika koji su došli uglavnom iz Azije i Latinske Amerike. Portes i Zhou (prema: Bui, 2009), novi imigranti i njihova djeca doživljavaju različite procese prilagodbe na temelju karakteristika populacije SAD-a u koju su integrirani. Prema tome, veća izloženost američkoj kulturi može biti povezana s mješovitim adaptacijskim ishodima. Ovisno o vrsti ljudskog kapitala (obrazovanja i vještina) i društvenog kapitala (društvenih resursa i mogućnosti podrške) koje različite doseljeničke skupine posjeduju, jedan put će dovesti do asimilacije doseljenika i njihove djece srednjoj klasi većine. Suprotan tip prilagodbe uzrokovan siromaštvom i rasnom segregacijom dovest će do silazne mobilnosti te asimilacije imigranata i njihove djece u gradsku podklasu. Pridržavanje tradicionalnih vrijednosti i zadržavanje etničkog identiteta dovest će do trećeg puta prilagodbe, s brzim gospodarskim napretkom i očuvanjem vrijednosti i solidarnosti među useljenicima. (Bui, 2009)

4. Istraživanje utjecaja imigracijskih procesa na kriminal

Bui (2009) nadalje opisuje kako je veza između imigracije i kriminala postala predmet istraživanja na prijelazu iz 20. stoljeća, nakon što su useljenici iz Europe u velikom broju došli u SAD. Odnos imigracije i zločina nije bio glavni predmet istraživanja prije toga jer je trend imigracije bio spor u tom periodu i zato što se vjerovalo da su se većina europskih useljenika koji su došlo početkom 20. stoljeća već asimilirali u društvo SAD-a.

Imigracijski val poslije 1965. godine, kroz politiku otvorenih vrata koji je uključivao velik broj azijata, afro-karibijanaca i dr., obnovio je istraživački interes za temu, dijelom zbog povećanih javnih rasprava o troškovima i koristima imigracije, a dijelom zbog podudarnosti dvaju društvenih fenomena: (1) dolazak novih useljenika i (2) porast stope kriminala 1970-ih i 1980-ih. Bilo je i zabrinutosti o niskim razinama vještina na tržištu rada kod novih doseljenika, posebno onih koji su stigli preko tajnih kanala i zakonskih rupa. Rana i nedavna istraživanja proizvela su različite rezultate, ali ne pokazuju jake dokaze o kauzalnim učincima imigracije na zločin. Umjesto toga, istraživanja su pokazala učinke različitih socioekonomskih čimbenika na kriminalno ponašanje među useljenicima. (Bui, 2009)

Ne postoje negativni učinci imigracije na kriminal

Nekoliko ranih i nedavnih studija nisu pronašle dokaze o negativnom utjecaju doseljavanja na problem kriminala. Nalazi iz tri rane studije, uključujući i one Industrijske komisije (1901), Imigracijske komisije (1911) i Nacionalnog povjerenstva za provedbu i poštivanje zakona (također popularno poznato kao Wickersham komisija, 1931-1932), pokazali su da, na makro razini, gradovi s visokim udjelom stranaca nemaju nužno veće stope kriminala od gradova s nižim udjelom stranaca. Na mikro razini, bijelci rođeni u inozemstvu promatrani su

kao manje kriminalni nego bijelci rođeni u SAD-u jer su imali niže stope zatvaranja u zatvor. Sudski zapisi također pokazuju da su ljudi rođeni u inozemstvu imaju manju vjerojatnost da budu proglašeni krivima za zločin. Istraživanja u posljednjih nekoliko godina pružila su slične rezultate - pokazuju da četvrti s velikim koncentracijama stranaca imaju niže razine nasilja od onih s manjim udjelima stranih stanovnika. (Bui, 2009)

Iako većina istraživanja o kojima se upravo raspravljalo nije objasnila razlog niskih razina uhićenja i osuda među imigrantima, nedavna studija provedena od strane Butchera i Piehla predlaže da samo izabrana priroda imigranata objašnjava njihove niske razine zločinstva. Otkrili su da su nedavni doseljenici iz svih rasnih i etničkih skupina imali nižu razinu obrazovanja, ali da su imali značajno niže razine zatvora od domorodaca, još u razdoblju kada se institucionalizacija proširivala. U 2000. godini, među ljudima u dobi od 18 do 39 godina, grupa od koje se sastoji velika većina zatvorske populacije, stranci su imali stopu zatvaranja (0,7%), koja je 5 puta manja nego u domorodaca (3,5%). Nakon što nisu našli potporu za druga objašnjenja (npr. povećana deportacija i odvraćanje), Butcher i Piehl zaključili su da su imigranti samostalno odabrani između onih s niskom kaznenom sklonosti. (Butcher i Piehl, 2005)

Mežnarić (prema: Perić, 2015) sagledava problem migranata u kontekstu svojevrsne moralne panike Europljana te stereotipu o porastu kriminala koji je uvjetovan dolaskom migranata kroz tzv. uvoz kriminogenih faktora gdje se ide linijom manjeg otpora i za sve loše što se dogodi okrivljuju se migranti. Dugotrajna longitudinalna istraživanja koja su proučavala kriminalitet paralelno s povećanjem raznolikosti zajednice pokazala su da se u velikim zajednicama koje stalno bilježe priljeve novih ljudi u periodu od trideset godina u Velikoj Britaniji, posebice Londonu određena stopa kriminaliteta pojavljuje neovisno o migrantima odnosno da njihov dolazak ne utječe na povećanu stopu kriminaliteta (Mežnarić, prema: Perić, 2015). U tom smislu posebno naglašava takozvani VDD kompleks (viktimizacija-demonizacija-diskriminacija) u kojem se viktimizacija odnosi na određene stereotipe o kriminalu, odnosno o tome kako dolazi do porasta kriminaliteta s dolaskom migranata. Demonizacija označava istinsko nepoznavanje i posljedično okrivljavanje migranata za destruktivne procese, uključujući i kriminalitet, dok diskriminacija uključuje negativna razmišljanja i stavove o migrantima. Na društvenoj razini, stereotipi imaju funkciju pokazivanja dominantnih vrijednosti, čije prihvaćanje s jedne strane pojedincu donosi društveno prihvaćanje (Bowker, Carrier, 1976; prema: Bulat, 1995), dok s druge strane dovodi imigrante u situaciju viktimizacije. Percepcije o imigrantima i kriminalu pokazuju kako valovi imigranata koji obično žive u socijalno ugroženim zajednicama bivaju percipirani kao „drugačiji“ od strane većinskog bijelog stanovništva (Godfrey, Williams i Lawrence, 2008). Prema Keppeler i Gaines (2009), etničke manjine drže se zajedno zbog kulture, naslijeđa, jezika te odbacivanja i opresije od strane većinskog stanovništva što je zauzvrat percipirano kao dokaz tajnovitog i klanskog ponašanja koje, prema mišljenju većinskog stanovništva, opravdava zlostavljanje manjina. Nasilje nad etničkim manjinama motivirano predrasudama i stereotipima u znanosti je poznato kao ekstremističko nasilje, odnosno kao kazneno djelo protiv života i tijela, opće sigurnosti ljudi i imovine te ostala kaznena djela u kojima su žrtve pripadnici određenih, najčešće manjinskih grupa (Radetić-Paić i sur., 2012;

Smiljanic, 2002; Spalek, 2002). Radetić-Paić i sur. (2012) navode kako je počiniteljima ekstremističkog nasilja cilj odaslati poruku pripadnicima grupe iz koje žrtva dolazi, a da se kao generator ove vrste nasilja prepoznaje diskriminacija po etnicitetu, rasi, spolu, religiji, a u novije doba i diskriminacija prema osobama s posebnim potrebama. No, relevantna istraživanja provedena u Velikoj Britaniji, Americi i dijelom u Njemačkoj govore upravo suprotno, odnosno, da prisutnost migranata ne utječu na porast kriminaliteta.

Istraživanja koja su rađena u Velikoj Britaniji naime pokazuju da kada je u pitanju nasilnički kriminalitet populacija koja je rođena u inozemstvu nije povezana s nasilničkim kriminalitetom u Velikoj Britaniji. Kada je u pitanju imovinski kriminalitet istraživanje pokazuje kontinuirano smanjenje imovinskih kaznenih djela u periodu od 1983. do 2002. godine u Engleskoj i Walesu. U isto vrijeme u tim je zemljama prisutan kontinuirani porast broja stanovnika koji tamo nisu rođeni. Istraživanje dakle pokazuje negativnu korelaciju između stope imovinskog kriminaliteta i imigranata. Ono što je važno je da detaljnije studije na ovu temu nisu pronašle dokaze da bi porast broja imigranata uzrokovao pad stopa kriminaliteta (Imigration and Crime: Evidence for the UK and Other Countries).

Bell (2014) u svom istraživanju koje je provedeno u Velikoj Britaniji u periodu od 1999. do 2002. godine ukazuje na činjenicu različitog utjecaja na kriminalitet na primjeru dvije vrste imigranata. Prvo su dislocirani imigranti iz bivše Jugoslavije te imigranti tražitelji azila iz ratom zahvaćenih država, kao što su Irak i Afganistan, te s druge strane imigranti zemalja država A8 (države istočne Europe), posebno državljani Poljske, koji su došli u Veliku Britaniju tragajući za poslom. Prema rezultatima istraživanja, procjena učinka na povećanje ili smanjenje kriminala može ležati u i biti rezultat razlike u mogućnostima pristupa tržištu rada. Naime, imigranti iz zemalja A8 imaju veće stope zaposlenosti od imigranata tražitelja azila koji ne smiju po dolasku u Veliku Britaniju raditi te im je smanjen pristup socijalnim povlasticama, a proces odlučivanja o zahtjevu za azil je dugotrajan. Ova ograničenja kod tražitelja azila uvjetuju neznatno povećanje imovinskog kriminala za 1%, dok je kod imigranata zemalja A8 niža za 0,4% upravo zbog dostupnosti tržištu rada, stopa kriminala.

U odnosu na aktualnu migracijsku krizu i boravak migranata u Njemačkoj, ministar unutarnjih poslova, Holger Muench izjavio je kako nekontrolirani ulazak migranata u Njemačku predstavlja prijetnju za nacionalnu sigurnost Njemačke, a posljedice bi se mogle ogledati u jačanju radikalne desnice koji su uglavnom i počinitelji napada na imigrante s elementima nasilja. Broj tih napada se od početka godine do kraja listopada utrostručio na brojku od 600 napada, dok je 2014. godine zabilježeno svega 198 takvih napada. Analiza njemačkog Saveznog ureda za suzbijanje kriminala (BKA) pokazala je također da se dolaskom velikog broja izbjeglica u Njemačku stopa kriminala nije povećala, ali se po kriminalu ističu imigranti iz Srbije, Kosova i Makedonije. Istodobno broj počinitelja kaznenih djela koji dolaze iz Sirije i Iraka je ispod prosjeka. Podaci pokazuju da se migranti kao počinitelji kaznenih djela pojavljuju jednako često kao i ostalo stanovništvo (Analiza saveznog ureda za suzbijanje kriminala).

Iako sva dosadašnja istraživanja ukazuju da nema povezanosti između porasta kriminala i migranata, zanimljiv je primjer Švedske kada je u pitanju nasilnički kriminalitet pri čemu se

specifičnim pokazuje kazneno djelo silovanja. Istraživanja koja su tamo provedena prema podacima Eurostata objavljenih i na portalu Narod.hr, potvrdila su povezanost značajnog porasta stope kaznenih djela silovanja sa useljeničkom populacijom kao počiniteljima. Naime, u posljednjih 40 godina od kada je Švedski parlament odlučio promijeniti homogenu Švedsku u multikulturnu zemlju nasilnički kriminalitet porastao je za 300%. Usmjerimo li pozornost na broj silovanja, povećanje je još i drastičnije. Naime, 1975. godine policiji je prijavljen 421 slučaj silovanja, a 2014. godine 6620 silovanja što je porast od 1.472%. Prema izvješću Nacionalnog vijeća za prevenciju kriminala iz 2012. godine, 2011. godine 29.000 švedskih žena bilo je silovano, a manje od 25% silovanih žena odlučilo je prijaviti silovanje. Među osamnaest istraživanja o kriminalu u Švedskoj koja su provedena krajem devedesetih godina, 11 ih se bavilo slučajevima silovanja. Od toga, dva izvješća bavila su se vezom između slučajeva silovanja i imigracija te su oba izvješća potvrdila korelaciju tih varijabli. Nadalje, utvrđeno je da je 2002. godine 85% osuđenih na žalbenom sudu Svea Hovratt na najmanje dvije godine zatvora zbog silovanja, što je zanimljivo zbog činjenice kako je tih 85% osuđenih rođeno u stranoj zemlji ili pripadaju drugoj generaciji imigranata.

Iz izvješća Švedskog Nacionalnog vijeća za prevenciju kriminala iz 1996. godine dolazi se do zaključka da kod imigranata iz sjeverne Afrike postoji 23 puta veća vjerojatnost da će počiniti silovanje, nego kod muškaraca iz Švedske, kod muškaraca iz Iraka ta je vjerojatnost 20 puta veća, a kod muškaraca iz Bugarske i Rumunjske 18 puta. Muškarci iz ostalih dijelova Afrike imaju 16 puta veću vjerojatnost za počinjenje silovanja, a muškarci iz Irana, Perua, Bolivije imaju 10 puta veću vjerojatnost od švedskih muškaraca (Carlgvist i Hadegard, 2015). Ono što je signifikantno u svim izviješćima vijeća, a zabrinjava različite nevladine udruge u Švedskoj, je činjenica da se druga generacija imigranata u službenim statistikama vode kao Šveđani što po njima ne prikazuje stvarno stanje jer prikriva imigrantsko porijeklo počinitelja silovanja.

Istovremeno iz podataka Eurostata na primjeru Danske može se vidjeti kako je u državi slične kaznenopravne regulative na 100 000 stanovnika prijavljeno 7,3 slučaja silovanja, dok je u Švedskoj to 53,2 slučaja na isti broj stanovnika, a u Africi ta brojka iznosi 91,6 silovanja na 100 000 stanovnika. Nadalje, u 2011. godini policiji u Švedskoj je prijavljeno 6 509 slučajeva silovanja, a u Danskoj 392 slučaja silovanja. Bez obzira na razliku u broju stanovnika (Švedska 9 743 087, Danska 5 614 000) ta diskrepancija je svakako značajna. Može se naime postaviti pitanje jesu li žene u Danskoj manje spremne prijavljivati silovanje od žena u Švedskoj? Službeni ured za statistiku u Danskoj 2010. godine otkriva signifikantne rezultate kako je više od polovice osuđenih silovatelja imalo imigrantsko porijeklo, dok vlasti u Švedskoj čine sve da prikriju porijeklo počinitelja silovanja.

5. Zaključak

Dosadašnja istraživanja migracijskih procesa i njihova utjecaja na sigurnost i kriminalitet nisu pokazala značajna odstupanja od uobičajenih pokazatelja porasta kriminaliteta. Naime, studije rađene u Americi, Velikoj Britaniji i Njemačkoj ne potvrđuju tvrdnju o negativnim utjecajima imigranata na porast kriminaliteta u smislu potvrde uloge imigranata kao potencijalnih

počinitelja kaznenih djela. Umjesto toga, rezultati istraživanja pokazuju ograničenu ulogu imigracija i imigranata u uzrokovanju problema kriminala.

S druge strane, na primjeru Švedske i Danske vidljivo je da su posljednjih godina kada su u pitanju nasilni prijestupi, posebno silovanja ta kaznena djela u iznimnom porastu, a imigranti se pojavljuju kao počinitelji u više od polovice presuđenih slučajeva. Upravo iz tog razloga, kao i činjenice da je tamna brojka i stopa neprijavljivanja ovih zločina visoka, ovi podaci upućuju na potrebu novih relevantnih istraživanja u području sudjelovanja imigranata u izvršenju kaznenih djela posebno onih s elementima nasilja.

Procesi akulturacije, kroz koje imigranti zadržavaju pozitivne aspekte svojih kultura kao i olakšana integracija useljenika, može smanjiti kriminal i delinkvenciju. Eliminiranjem socijalnih razlika imigranata i domicilnog stanovništva kroz širenje politike degetoizacije migranata, politike socijalne uključivosti, boljem pristupu tržištu rada te politike aktivne društvene kontrole, potencijalni sigurnosni rizici za građane EU, posebice u dijelu njihova utjecaja na stanje i kretanje kriminaliteta biti će svedeni u prihvatljive okvire.

Opravdana zabrinutost građana Unije od terorizma i nasilnog kriminala s druge strane, više je nego dovoljna osnova za racionalan pristup institucija EU u sagledavanju imigracijskih procesa kao dijela kompleksa sigurnosnih problema s kojima je Unija suočena te definiranja proaktivnih politika prema imigrantima koje ostvaruju preduvjete za rješavanje tih problema.

LITERATURA

Becker, G. (1968). Crime and Punisment: An Economic Approach. Journal of Political Economy. Preuzeto s: http://econpapers.repec.org./bookchap/nbrnberch/3625.html, pristupljeno: 21.1.2016.

Bell, B. (2014). Crime and imigration. Do poor labor market opportunity lead to migrate crime. University of Oxford UK. Preuzeto s: http://wol.iza.org./articles/crime-and-imigration.pdf., pristupljeno: 21.1.2016.

Bigo, D. (2002). Security and Immigration: Toward a Critique of the Governmentality of Unease. Alternatives, 27:63–92.

Bigo, D. (2007). Detention of Foreigners, States of Exception, and the Social Practices of Control of the Banopticon. University of Minnesota Press, 3–34.

Bui, H. N. (2009). Immigration and Criminal. U: 21st century criminology: a reference handbook, ur. J. Mitchell Miller

Bulat, N. (1995). Dimenzije stereotipova i predrasuda u odnosu na raseljene osobe i izbjeglice iz Bosne i Hercegovine. Migracijske teme, 11(2): 151-171

Butcher, K., Piehl, A. M. (2005). Immigration and self-reported delinquency: The interplay of immigration status, gender, race and ethnicity. Yournal of Crime and Justice, 28: 79-100

Carlgvist,I. Hadegaard L. (2015) Sweden: Rape Capital oft he West. Institut Gatestone International Policy Council. Preuzeto s: http://www.gatestoneinstitut.org/5195/sweden-rape, pristupljeno: 29.1.2016.

Champion, D. J., Rush, G. E. (1997). Policing in the community, New Jersay: Simon & Shuster.

Ehrlich, I. (1973). Participation in illegitimate activities: a theoretical and empirical investigation. Journal of Political Economy, 81 (3):521-565

Futo, P., Jandl, M., Karsakova, L. (2005). Illegal Migration and Humman Smuggling in Central and Eastern Europe. Migracije i etničke teme 21(1-2): 35-54.
Godfrey, B.S., Williams, C.A., Lawrence, P. (2008). Immigration, Ethnicity, Race and Crime. History and Crime.
Huysmans, J. (2006). The Politics of Insecurity: Fear, Migration and Asylum in the EU. London – New York: Routledge.
Jonjić, P. (1984). Teorijski aspekti proučavanja migracije: kritički pregled literature. Migracijske teme 1: 63-76
Junger-Tas, J. (2001). Ethnic minorities, social integration and crime. European Journal od Criminal Policy and Research, 9: 5-29
Keppeler, V. E., Gaines, L. K. (2009). Community Policing: A Contemporary Perspective, Fifth Edition, Newark: LexisNexis Group.
Kicinger, A. (2004) Internation Migration as a Non-Traditional security Threat and the EU Respones to This Phenomen, CEFMR Working paper 2/2004. http//:www.cefmr.pan.pl/docs/cefmr_wp_2004_02.pdf
Koser, K.. (2011). When is Migration a Security Issue? Preuzeto s: http//:www.brookings.edu/reserch/opinions/2011/03/31-libya-migration-koser, pristupljeno: 17.12.2015.
Kerwin, D. 82014) Human Security, Civil Society and Migration. Center for Migration Studies of New York. Preuzeto s: https://docs.unocha.org/sites/dms/HSU/Kerwin%20statement.pdf, pristupljeno: 16.11.2015.
McCarthy, B., Hagan J. (1995). Getting into street crime: the structure and process of criminal embeddedness. Social Science Research, 24: 63-95.
McCarthy, B., Hagan, J. (2001). When crime pays: capital, competence and criminal success. Social Forces, 79 (3): 1035-1059
Morehouse, C., Blomfield, M. (2011) Irregular Migration in Europe. Washington DC: Migration Policy Institute
Nwalozie, C. J. (2015). Rethinking Subculture and Subcultural Theory in the Study of Youth Crime – A Theoretical Discourse. Journal of Theoretical and Philosophical Criminology, 7(1):1-16
Perić, I. (2015) Imigracija po policijskim kriterijima portal H-alter. Preuzeto s: http://www.h-alter.org/vijesti/imigracija-po-policijskim-kriterijima, pristupljeno: 29.1.2016.
Pozniak, R., Petrović, D. (2014.) Tražitelji azila kao prijetnja. Studia ethnologica Croatica., 26: 47-72
Radetić-Paić, M., Opašić, V., Kostešić, I. (2012). Police procedure as a possible indicator od institutional exstremism. Metodički obzori, 16/7: 25-36.
Sellin, T. (1938). Culture Conflict and Crime. New York: Social Science Research Council
Shaw, C., McKay, H. (1942). Juvenile Delinquency in Urban Areas. Chicago: University of Chicago Press
Smiljanic, N. (2002) Human rights and Muslims in Britain. U: Islam, Crime and Criminal Justice, Spalek. B. (ur.), Collumpton: Willan
Spalek, B. (2002) Muslim women's safety talk and their experiences of victimisation: a study exploring specificity and difference. U: Islam, Crime and Criminal Justice, Spalek. B. (ur.), Collumpton: Willan
Tatalović, S., Lacović, T. (2012) Političke analize br.12. Nacionalna i europska sigurnost Fakultet političkih znanosti Zagreb. Preuzeto s: http//:www.fpzg.hr/images/50016358/pa-12.pdf, pristupljeno: 6.4.2016.
Tirman, J. (2004). The Maze of Fear: Security and Migration after 9/11. New York: New Press

Internetski izvori

EUROSTAT – podaci preuzeti s: http://ec.europa.eu/eurostat, pristupljeno: 26.1.2016.
Portal Narod.hr. Posljedice imigrantskog vala. O tome se šuti. Preuzeto s: http//:narod.hr./eu/o-tome-se-šuti-broj-silovanja-u-švedskoj-povečan-za-deset-puta, pristupljeno: 23.12.2015.
The Migration Observatory. Imigration and Crime: Evidence for the UK and Other Countries. Preuzeto s: http://migrationobservatory.ox.ac.uk/briefings/imigration-and-crime-evide, pristupljeno: 21.1.2016.
The Swedis National Council for Crime Prevention. Rape and sexual offences. Preuzeto s: https://www.bra.se./bra/bra/-in-english/home/crim-and... pristupljeno:18.12.2015.
United Nation Department of Ekonomic and Social Affairs – podaci preuzeti s: http//:unchr.org/556725e69.html, pristupljeno 28.1.2016. godine.

Dubravko Derk
Barbara Prprović
Nikolina Nemec

IMPACT OF RECENT MIGRATIONS ON THE EUROPEAN SECURITY

Summary

This work is based on a review of current migration processes, the role of migrants as part of non-conventional security threats through their possible impact on European security. In this sense, the paper deals with correlations of security and socio-economic relations between the key players and their impact on both the general safety of citizens and immigrants on the one hand, as well as the overall European security on the other hand. Previous migration studies and its impact on safety have shown a limited direct relationship between immigrants and the increase in crime and the role of immigrants as crime causes. The results show, considering the current situation in the EU, that these migrations occur as a result of security threats and risks associated with terrorist acts in Paris, and to some degree to other criminal acts with elements of violence, especially expressed in some member states such as Sweden and Denmark, that as a whole subjectively leave EU citizens with an impression of latent insecurity.

Key words: *migrants, security, violence, terrorism, crime, acculturation.*

REVIEW PAPER

Tatjana Gerginova[687]

THE ROLE OF PRIVATE INSTITUTIONS FOR SECURITY IN THE NATIONAL SECURITY SYSTEM

Summary

The 90s of the 20th century are globally characterized by the appearance of new and modern challenges, risks and threats, that led to the appearance of a new phenomenon known as the privatization of security. In completion of the national security, private security institutions emerged in addition to the police.

It is indisputable that a country's job is to make sure that every citizen enjoys a decent amount of safety. However, people, no matter if for subjective or objective reasons, often search for a higher level of protection than the one given by their country; this imposes the need to establish a legal definition for these new forms of protection, the type of the legal form and the service they will provide. Hence the need to determinate the proper legal framework in the field of physical and technical security services for life and property as well as in the field of private detective agencies work which will contribute to improve the safety of life and property.

The police are in charge of providing public peace and order while the private security services are in charge of protecting people and their property.

The author of the paper will specify the role of private security institutions and the main tasks they carry out in the Republic of Macedonia. The author will differentiate between the main function and the police work done by the police and the main services that are given by private security institutions. In conclusion, the author will give arguments why private security institutions should continue evolving and be a part of the society.

Key words: *physical security, private security, private security institutions, technical security.*

1. INTRODUCTION

Opening the doors of the private security sector, the countries on the territory of former Yugoslavia, found themselves as other countries in transition before the actual challenges: high profitability of the private security sector and initial legally unsettled situation in that area in which the sector began its life. They have to be brought into conformity with the requirements of the rule of law and simultaneous reforms in the public security sector. There was the need for harmonization of the domestic legislation with the international legal standards related to the functioning of the private security sector. Moreover, there is the need to establish the adequate legislation in the field of physical and technical securing people and

[687] Assist. Prof. Tatjana Gerginova, Faculty of Security, University of Bitola, e-mail: tanjagerginova@gmail.com

property, as well as in the area of hiring private detective agencies, that will contribute to improving certain aspects of the safety of citizens and property.

The aim of the adoption of legislation in the private security sector is the need to make a functional distinction in relation to the competence in performing certain safety measures in tasks. Therefore, all segments can be different compared with the action of the country or the police sector and it is necessary to establish appropriate standards and professionalism in all forms of private security.[688] The number of threats and challenges mainly occurred due to the sudden technological and scientific development, which is used for unwanted objectives. Based on a detailed analysis of the legal, economic and security environment and assessment of the level of threat to vital interests in the modern World, the most important risks and security threats can be identified. These are, as follows: organized crime and corruption, terrorism, major armed conflicts, regional disputes and conflicts, armed rebellions, national and religious extremism, natural, technical and industrial disasters, epidemics of larger scale, the proliferation of nuclear and conventional weapons, lack of strategic energy resources, abuse of new technologies, scientific achievements in the field of informatics, genetic engineering, ethnic tensions, illegal migration, etc. The main characteristics of these risks and threats are mostly of non-military nature, and the existing capacity is difficult to identify, detect and prevent (Gerginova, 2015: 141).

2. CONCEPT, OBJECTIVES AND TYPES OF PRIVATE SECURITY

In the Republic of Macedonia in 1991 occurred changes in property relations, leaving the social ownership and the establishment of private property as the dominant form, on the one hand, and establishing a new system of values, on the other hand, which eligible to establishing a kind of trinity - government, non-government and civil sector (Spaseski, Aslimovski & Gerasimoski, 2008: 30-33).

Services of the private security sector in the modern world are increasingly becoming an alternative to the state security sector, in achieving the protection of private as well as public (the state), international and global interests and values. Hence, the demands for the development of the private security sector, as well as to establish a serious partnership with the state security sector, are growing. Today, the private security sector becomes a real need, because the state is no longer able to meet equally and effectively all increased security needs of the society and the reality.

In order for the new and complex security system to function successfully, it is necessary to regulate legally mutual relations regarding the rights, duties and responsibilities on the one hand, and consistency between practices, on the other hand. In determining the powers of the state police (which belongs to the public sector) and private security agencies (that belong to the private sector), the main difference consists in a facility that is protected from performing criminal acts of his detriment. As the primary interest of protecting the public sector, the

[688] Gerginova T., "*The need for private security institutions",* Faculty of Security – Skopje - INTERNATIONAL YEARBOOK – 2014. see more detailed: Bošković, Mićo: *Fundamentals of detective activity*, Faculty of Legal and Business Studies, New Sad, 2006, page 18

emphasis is placed on the facility to serve the interests of society. The police belong to the public sector, where the object of protecting is the interests of society and the state.
Employees of private security belong to the private sector, where the object of protection is the interests of the organization or individual who requested the provision, not the interests of society as a whole. While for the civil sector, the primary care is prevention, for these three dominant sectors, there are differences in terms their authorizations. Within the public sector, authorizations of the police are based on the rights and duties of the state, to prosecute and punish perpetrators of illegal behavior.

Out of the private sector, the authorizations relating to the individual's right of self-protection, which he/she delegates, are defined with a contract with the organization for securing or a detective. Civil sector bases its authority on the right of citizens to be protected from preventive destructions in society as well as from other threats (Spaseski, Aslimovski & Gerasimoski, 2008: 30-33).
Under the Law on private security, the private security is an activity of public interest (Law on private security 'Official Gazette' of the Republic of Macedonia, No. 166/ 2012, art. 2). It is performed by legal entities that are licensed for private security. The private security shall undertake activities established by this Law for the prevention and detection of harmful occurrences and illegal actions, which threaten the physical integrity and dignity of the person and property which is protected (Law on private security 'Official Gazette' of the Republic of Macedonia, No. 166/ 2012, art. 3).

Private security is the protection of persons and property, which is carried out by legal entities that are licensed for private security, and the legal entities performing private security in the form of provision of services for individual requirements (Law on private security 'Official Gazette' of the Republic of Macedonia, No. 166/ 2012, art. 8).

"Private security in the form of providing services" is to protect people and property based on a contract that does the legal entity, which has made registering their activity in the Central Registry of the Republic of Macedonia and has obtained a license for private security in the form of providing services. This provision legal entity is performed as physical security and technical security. Physical security is performed as physical protection; monitoring patrol security; providing transport and transfer of money and other valuable items and provision of public gatherings and other events.

"Private security for own needs" is the protection of property and persons in the legal entity. It is performed by private security workers employed in the legal entity, holding a license for private security for their own needs, and performed as physical security (as physical protection and monitoring security) (Law on private security 'Official Gazette' of the Republic of Macedonia, No. 166/ 2012, art. 9).

Main services provided by legal entities that are licensed for private security are as follows:[689]
- Protecting people and property from all forms of corruption, organized crime, terrorist activities, various forms of abuse, misappropriation, fraud and other methods of alienation and appropriation of its property; political crime, general crime and economic crime (political crime, terrorism, sabotage, sabotage, espionage, general crime - theft, severe and armed robbery, robbery, deprivation of motor vehicle, fraud, extortion, hijacking, fire, economic crime - corruption, reckless operation, misuse of official position or powers, embezzlement, receiving and giving bribes, indulgence of official secrets);

- Physical security, as a collateral of persons (life, physical integrity) which are carried for personal protection of persons and provision of assets of such persons from access to uninvited persons, destruction, damage, illegal seizure and other forms of harmful activities. Employees of private security perform physical security;

- Technical security, as a collateral of persons and property by using technical tools and devices, the design, installation and maintenance;

-Body protection, which presents an appearance of physical security, which directly provides the protection of persons and property by employees for private security;

-Provision monitoring, as a form of physical security carried out as constant physical supervision of technical systems and embedded devices for securing people and property and telecommunication transmission of alarm signals in the center of security and surveillance;

-Monitoring patrol security, as a form of physical security that is performed as a constant physical supervision of integrated technical systems and devices, for securing people, property and telecommunication transmission of alarm signals, in the center and provision supervision and hiring workers for private provision; vehicle security is used to prevent damaging activities for persons and property that are provided; the security of persons and property is performed by alarm signal, received by the public security and surveillance;

-Providing transportation and transfer of money and other valuable items as a form of physical security of transport and transfer of money, gold, precious stones, works of art, and other valuable items with workers for private security and special vehicles;

-Provision of public gatherings and other events as a form of physical security for workers with private security and the use of technical means for the maintenance of public order at public gatherings, sporting events, cultural, entertainment, religious, humanitarian, social, political, economic and other events.

[689] More details see: Gerginova. T., *Tactics and technique of provision*, material for students, 2012

Legal entities that are licensed for private security must not protect persons and property based on special regulations provided by competent state authorities for example the police. In addition, these legal entities may not perform activities related to debt collection and must not use operational methods and means which by law are not allowed or whose application based on special regulations are authorized only competent state authorities. However, the Law on Private Security has not determined the operational methods and tools. Only use the competent national authorities not listed and not narrowly defined their content (Law on private security 'Official Gazette' of the Republic of Macedonia, No. 166/2012). It is characteristic that the private security contract for private security is given between the two parties: legal entity (holding a license for private security) and a person (as a user of the service). "Employees of private security" is a person who holds a valid license for private security and private security identification card, who is employed in legal entities and duties to protect people and property, or performs tasks based on the powers established by this law. "Border space of providing" is a line that includes real estate and areas that are part of the property that is to be provided. "Authorized Officer" is an employee of the Ministry of Interior, according to the Law on Internal Affairs and the Police Law.

The Law on Police (Law on Police, "Official Gazette" of the Republic of Macedonia No. 41/2014, art. 1) regulates police affairs, the organization of the police, police powers and the rights and obligations arising from the employment of police officers in the Ministry of Interior (which are not regulated by the Law on Internal Affairs). Under this law, the police are determined as part of the Ministry which perform police work by police officers. By this Act, a police officer shall be determined as an authorized officer, under the provisions of the Law on Internal Affairs, uniformed and plainclothes member of the police with police authorizations, performing police duties in accordance with law (Law on Police, "Official Gazette" of the Republic of Macedonia No. 41/2014, art. 2). The main function of the police is to protect and respect the fundamental rights and freedoms of man and citizen guaranteed by the Constitution, laws and ratified international agreements; the protection of the legal order; the prevention and detection of offenses; taking measures to prosecute the perpetrators of such crimes; to maintain public order and peace in the society (Law on Police, "Official Gazette" of the Republic of Macedonia No. 41/2014, art. 3).

Police officers in achieving the main function, which perform police duties under this act, shall be actions of the police officers concerning (Law on Police, "Official Gazette" of the Republic of Macedonia No. 41/2014, art. 5):

-protection of life, personal safety and property of citizens;
-protection of rights and freedoms of man and citizen guaranteed by the Constitution, laws and ratified international agreements;
-prevention of criminal acts and offenses, detection and apprehension of the perpetrators and taking other measures provided by law for the prosecution of offenders;
-identifying and looking for direct and indirect proceeds obtained by committing a felony;
-maintaining public order;
-regulation and control of traffic;
-control of movement and stay of foreigners;

-border checks and border surveillance;
-pointing out assistance and protection of citizens in case of necessity;
-securing specific persons and objects and
-other duties prescribed by law.

Police provides assistance to state authorities, municipalities and the City of Skopje, to legal and physical entities in the rescue of people and material goods from natural and other disasters (Law on Police, "Official Gazette" of the Republic of Macedonia No. 41/2014, art. 6). For the prevention or detection of crimes and offenses, the police cooperate with citizens, state bodies, NGOs and other entities, for the prevention or detection of crimes and misdemeanors. Police cooperates with the bodies of the municipalities and the City of Skopje on issues relating to public safety and road traffic (Law on Police, "Official Gazette" of the Republic of Macedonia No. 41/2014, art.11).

2.1. Monitoring - monitoring and patrol security

2.1.1. *Center for security and surveillance*

For the purpose of monitoring and security monitoring patrol security, private security agencies have established a center for security and surveillance (Law on private security "Official Gazette" of the Republic of Macedonia, No. 166/2012, art. 33). Centre for providing and monitoring a separate room equipped with technical devices for automatic reception and processing of alarm signals and other information arriving from devices and installations in buildings or vehicles installed for that purpose. The Center for providing the security and surveillance mandatory has employees on duty 24 hours a day. After receiving an alarm signal in the center providing the supervision and legal person performing private security in the form of providing services to hire a patrol guards. Providing employee (operator) in the center for security and providing the supervision are obliged to immediately inform the police if the information received indicates that committing a crime prosecuted ex officio.

2.1.2. *Patrol security*

Patrol to provide a legal entity performing private security type
The provision of services used preventively in order to prevent damaging activities over persons and property that are provided, as well as for the intervention in alarm arrive signal center for security and surveillance. Patrol consists of one vehicle and worker security (Law on private security 'Official Gazette' of the Republic of Macedonia, No. 166/ 2012, art. 34).
Providing transport and transfer of money and other valuable items

- *Providing transportation of money and other valuable items with specially equipped vehicle*

Legal entities engaged in private security in the form of provision of services may duties to protect the transport of money and other valuable items, especially if equipped vehicle for transportation must have (Law on private security 'Official Gazette' of the Republic of Macedonia, No. 166/ 2012, art. 35):

- armored bodywork, glass and tires;
- built-in mechanical security safe;
- embedded mobile video surveillance system of the vehicle is done by the staff of the vehicle;
- two-way relationship with the center for security and surveillance workers and ensuring that they leave the vehicle when receiving or delivery note (Global System for Mobile communications - GSM network or radio);
- built-in global positioning system (GPS) for satellite tracking and remote monitoring center and providing supervision and built-in panic button with the automatic sending of an alert signal at the center of security and surveillance.

Special build vehicle for transportation, except main elements, can have built-in electrochemical protection for the money during the transportation.

➢ *Workers for providing transport of money and other valuable items*

The staff of the vehicle composed of at least three workers for providing one of which is a driver. All staff members must have identification cards for security. In performing providing transport of money and other valuable items, all members of staff the vehicle must be properly armed with firearms and be equipped with protective equipment (ballistic vest - a bulletproof vest and helmet) (Law on private security 'Official Gazette' of the Republic of Macedonia, No. 166/ 2012, art. 36).

➢ *Providing transfer of money and other valuable items without special equipped vehicle*

Legal entities engaged in private security, in the form of provision of services may have duties to protect the transfer of money and other valuable items without special equipped vehicle. A seat holds suitcase whose construction is constructed, in a manner to allow to prevent violent opening and transferring of content, as well as to attempt forcibly opening alerts or occurrences, using sound, light or other signal. Jobs related to ensuring, perform at least two workers to provide ballistic vest-armor, while at least one employee is armed with the appropriate firearms and equipped with a mobile phone, or a portable radio system for his/her own needs. Safety suitcase in which transfers money or other valuable items, should not be mechanically fastened to the person who wears it (Law on private security “Official Gazette” of the Republic of Macedonia, No. 166/ 2012, art. 37).

2.1.3. Provision of public gatherings and other events

Doing the provision of public gatherings and other events

Legal entities engaged in private security in the form of provision of services, may perform the maintenance of public order at public gatherings, sporting events, cultural and entertainment, religious, humanitarian, social, political, economic and other events, to provide workers with using technical means and devices, in accordance with regulations for public gatherings and prevent violence at sports competitions. Employee wear work clothes that have vests fluorescent bands that are labeled "Security". During the execution of the maintenance of public order to ensure public gatherings and other events, employees are not allowed to

regulate traffic. Work to ensure employees perform without firearms (Law on private security "Official Gazette" of the Republic of Macedonia, No. 166/ 2012, art. 38).

Plan to ensure

When the legal person maintaining public order at a public gathering or event, there is the need for committed more than five workers to ensure the responsible person. Then, in the legal entity, a plan for securing the area where it is held the public gathering or event, shall be developed and submitted to the Ministry of Interior no later than 48 hours before the meeting or event. This plan has to include: the place and time of the public gathering or event provided; number and arrangement of hired workers for security; the data about the person who will manage workers security during the public gathering or event and a means to communicate with this person (Law on private security "Official Gazette" of the Republic of Macedonia, No. 166/ 2012, art. 39).

3. TECHNICAL SECURITY

3.1. Conducting technical security

Technical security is done by using technical means and devices for preventing illegal actions directed at persons and property, especially for protection against (Law on private security "Official Gazette" of the Republic of Macedonia, No. 166/ 2012, art. 40):

- unauthorized access to buildings and facilities that are provided;
- unauthorized use and dispose of items that are provided;
- unauthorized entry of firearms, explosives, radioactive, flammable and toxic substances;
- burglary, sabotage or violent attack on object being provided;
- unauthorized access to data and documentation;
- attacking vehicles which are transporting money and other valuable items.

Things are only performed in house providing, or to limit the space that is provided during the transport and transfer of money (and other valuable items), as well as while performing physical protection of individuals. Aids and devices can be connected to a system of technical protection.

3.2. Privacy and reporting on performance of video surveillance

Aids and devices must be used in a way that, outside the building providing or beyond the limit of the space that is provided, these aids don't violate the privacy of other people. When providing a facility or premises used for the public use, it is carried out by technical means and equipment for video surveillance. The legal entity which carries on a security is obliged to visibly emphasize reporting that video surveillance is conducted in accordance with regulations of the protection of personal data (Law on private security 'Official Gazette' of the Republic of Macedonia, No. 166/ 2012, art. 41).

Private security worker may conduct Physical security with firearms in order to provide:

- persons provided with physical protection;
- legal entities operating with money and other valuables, especially banks, post offices, savings banks and exchange offices;
- transport and transfer of money and other valuable items and
- Buildings and property provided under this Act.

3.3. Use of firearms for physical security

Employee security in the performance of private security guards may use only firearms that are owned by the legal entity, which is employed. There is an explicit legal prohibition - Employee security during the execution of physical security must not take their own firearms that own the rules of the weapons (Law on private security “Official Gazette” of the Republic of Macedonia, 166/2012. art. 30).

The responsible person in the legal entity shall have an order to carry firearms for providing workers, who are authorized to carry weapons issued according to the regulations on weapons. Workers providing mandatorily, have the order to carry firearms, permit to carry a weapon, and at the request of authorized official of the Ministry of Interior, they have to provide the insight about their permissions. Private security employee is obliged to have the order to carry a firearm and license to carry weapons pursuant to the Private Security Act, the weapons and the laws that regulate this matter. Non-compliance of the legal framework, the employee is providing corresponding criminal, misdemeanor, disciplinary and material for violations (Guidelines on the application of force, "Official Gazette” of the Republic of Macedonia No. 86/2013). Regular supervision over the work of the Chamber and legal persons of private security is performed by the Ministry of Interior, at least once per calendar year (Law on private security 'Official Gazette' of the Republic of Macedonia, No. 166/2012, art. 66).

The authorized officials of the Ministry of Interior shall perform the following activities of supervision (Act on Private Security “Official Gazette” of the Republic of Macedonia, No. 166/2012, art. 67):

- checking the manner of keeping and carrying of firearms, as well as the ability of handling and use of firearms, and
- verification of the application of the powers of workers for security.
- The provisions of the Law on private security are provided for criminal liability for the responsible person in the legal entity if:
- It envisages a fine of 1 200 to 1 500 euros in dinars, if the responsible person in the legal person issued a warrant for carrying some firearm workers to provide under art. 29(2) of the Law on Private Security "Official Gazette” of the Republic of Macedonia, No. 166/2012, ch. 74, par. 1.
- A fine of 600 to 700 euros in dinars will be sentenced for offense to a natural person if: the request of an authorized official of the Ministry of Interior did not make available to order for carrying a firearm license to carry weapons and firearms bearing (art. 29(3) of the Law on private security (“Official Gazette” of the Republic of Macedonia, No.166/2012, ch. l75, par. 2).

In accordance with the Law on Private Security, it is specified exactly when the employee security can be armed with firearms. For example, while performing providing transport of money and other valuable items, workers security must be armed with appropriate firearms, which have to be equipped with protective equipment (ballistic vest - a bulletproof vest and helmet) (Law on Private Security "Official Gazette" of the Republic of Macedonia, No.166/2012, art. 36). On the other hand, while working on securing public gatherings and other events providing workers employed in the legal entity have to be performed with the use of firearms (Law on private security “Official Gazette2 of the Republic of Macedonia, No. 166/2012, art. 36). As mentioned before, violations of the provisions of the Law on Private Security, the Law on Weapons and laws that regulate this matter, while the employee is providing corresponding criminal, misdemeanor, material and discipline for violations (Guidelines on the application of force “Official Gazette” of the Republic of Macedonia No. 86/2013).

Workers performing providing physical security can carry firearms and ammunition only in the building that provide, or to limit the space provided (Law on private security “Official Gazette” of the Republic of Macedonia, No. 166/ 2012, art. 29).

An exception when the order to carry firearms exactly set the place and the period will carry firearms and ammunition, providing workers who perform physical security can carry firearms and ammunition outside the building who provide or beyond the limit of space that is provided when:

- perform transport and transfer of money and other valuable items just in time and direction of the development of transport, transfer;
- improving physical protection;
- monitor - patrol security.

3.4. Prohibition to carry private firearms

Worker security during the execution of physical security must not carry private firearms that own the rules of the weapon (Law on private security 'Official Gazette' of the Republic of Macedonia, No. 166/ 2012, art.30).

Worker security is obliged to act on the orders of an authorized official of the Ministry of Interior, but the employee may not execute an order from an authorized official of the Ministry of Interior, and the orders of their superior worker if he would be committing a criminal case (Law on private security 'Official Gazette' of the Republic of Macedonia, No. 166/ 2012, art.47).

4. CONCLUSIONS

Today, private security agencies are part of the security system of the Republic of Macedonia and perform meaningful service in achieving the national security of the state and in achieving security of citizens, property, facilities, key infrastructure and so on.

The justification for the existence and further development of the private security sector can be argued as follows:
-*efficiency (real and potential)*, resulting from the best material and technical equipment of private sector entities for security;
-*economic* because the private security sector with their activities "as easing" (reduces duties) the police and other security entities, which creates significant budgetary savings;
-*economic usefulness* because the private security sector employs labor, and over fulfillment of tax obligations strengthens the state budget;
- *rationalization of the public sector*, as national forces are dedicated to solving the most serious security problems, which leads to their professional development and reducing the number of public employees;
- *Improvemen*t of the overall security of citizens and the state by establishing a partnership between government and the private security sector.
- *Services provided by private security* today cover a wide range of activities, from protection of property and capital to private storage services airports, banks and individuals.

The basic level of service include providing persons for the security of the: buildings, apartments, providing shopping malls and small gatherings, maintenance of public order at public gatherings, sporting events, cultural, entertainment, religious, humanitarian, social, political, economic and other events, services supervisory, investigative services, comprehensive risk assessment and services for risk reduction given to private businesses, providing banks (providing the transport of money and other valuable items, gold, precious stones, works of art, securities and other valuable items), etc.

REFERENCES

Gerginova, T. (2015). *Globule security.* Skopje: Faculty for security.
Gerginova, T. (2012). *Police and human rights in the security system of the Republic of Macedonia.* Doctoral dissertation. Skopje: Faculty of Security.
Gerginova, T. (2014). *The need for private security institutions.* International Yearbook. Skopje: Faculty of Security.
Law for police. *Official Gazette of Republic of Macedonia*, No. 41/2014.
Law on Internal Affairs. *Official Gazette of Republic of Macedonia*, No. 42/03.03.2014.
Law on private security. *Official Gazette of Republic of Macedonia*, No. 166/26.12.2012.
Regulation on the use of force and firearms, and instruction on the behavior and interrelationships of the police officers. *Official Gazette of Republic of Macedonia*, No. 65/30.05.2007
Spaseski, J., Aslimovski, P., Gerasimoski, S. (2008). *Private Security.* Skopje, Ohrid: Faculty for security.