Editorial

This last issue of the Journal of Criminal Justice and Security for this year consists of five quite diverse scientific analyses of important aspects of the field of criminal justice. In-depth studies in the areas of providing security in future smart cities, the impact of the EU General Data Protection Regulation on mobile devices, an analysis of the legal aspects of illegal asset recovery, the formal boundaries of law, and violence against employees in old people's homes are presented.

In the first paper *Analysis of the Relationship between Smart Cities, Policing and Criminal Investigation,* **Kaja Prislan** and **Boštjan Slak** present the symbiosis between smart cities, policing, criminal investigation and criminal intelligence and critically address the underlying privacy concerns arising from smart city designs. The authors emphasise it is evident that smart city technologies and services can influence policing styles and police effectiveness since smart city technologies and services hold great potential for criminal investigations and criminal intelligence by providing information upon which police can develop investigations or crime-control strategies.

In the second paper *The Impact of the EU General Data Protection Regulation (GDPR) on Mobile Devices,* **Domen Hribar, Miha Dvojmoč** and **Blaž Markelj** examine novelties introduced by the European Regulation on the protection of natural persons with regard to the processing of personal data (GDPR) and its key impacts on mobile device users. The paper presents some of the biggest changes affecting both natural persons and legal entities. Further, certain issues that might occur while implementing the Regulation are raised together with the degree of individuals' awareness of the need to protect the personal data stored on their mobile devices. The research findings show that individuals are relatively well aware of the concept of personal data; however, the scope of their knowledge shrinks as this concept becomes increasingly complex.

In the third paper *An Analysis of the Legal Aspects of Illegal Assets Recovery in Slovenia,* **Katja Rejec Longar** presents an analysis of legal aspects of asset recovery in Slovenia through the five-stage process of asset recovery: financial investigation, freezing or seizure of assets, confiscation, enforcement of the confiscation order and asset disposal. The author concludes that the Slovenian legal order provides the competent authorities with several avenues for recovering proceeds and illegally acquired assets. There is the traditional confiscation of proceeds, *in personam* confiscation in criminal proceedings, extended confiscation in criminal proceedings and civil forfeiture after the Forfeiture of Assets of Illegal Origin Act. One problem is that provisions for asset recovery are dispersed across both substantive and procedural law. Another problem is that some provisions are formulated in such a way that they are impossible to implement in practice. The author concludes it would be necessary to define financial investigation in criminal proceedings.

In the next paper *Formal Boundaries of Slovenian Law,* **Bojan Tičar** describes how the field of criminal justice and security in Slovenia is regulated. The paper deals with an analysis of the formal boundaries of Slovenian law mostly from the aspect of the Slovenian legal order in force. The reader will learn how the

Slovenian legal order functions, which general acts are adopted by the state and which by local bodies, the rules governing their application, and the relationships between them, as well as how EU law is applied in Slovenia.

The final paper in this issue of the Journal of Criminal Justice and Security is the work of **Katarina Cesar, Liljana Rihter, Špela Selak** and **Branko Gabrovec** and discusses *User violence against employees in nursing homes.* The purpose of their study was to complement the research gap in investigating violence within social care and determine the types and extent of workplace violence among all employees in a social care institution, the influence of users' aggressive behaviour on the well-being of employees, and the need for education on dealing with the violence to which employees are exposed. The authors find that in a case study of one nursing home that employees encounter some user violence. The most common form of violence against employees was verbal abuse and the least was unwanted conduct of a sexual nature. The authors conclude that when an employee meets an aggressive user the most likely emotions are fear, helplessness, uncertainty, feeling under threat, and the least likely a lack of understanding from fellow employees.

The Editorial Board hopes you find all of this edition's articles interesting and a good source of new ideas. And, since this is the last issue for 2018, we wish you the very best in 2019.

Assoc. Prof. Branko Lobnikar, PhD
Editor of English Issues

Uvodnik

Zadnjo številko revije Varstvoslovje v tem letu predstavlja pet raznolikih člankov, ki pa vsak zase in vsi skupaj analizirajo pomembne vsebine s področja varnosti. Bralci se bodo seznanili s poglobljeno študijo o zagotavljanju varnosti v pametnih mestih, predstavljen je vpliv uredbe EU o varstvu podatkov pri uporabi mobilnih naprav, predstavljena je analiza pravne ureditve odvzema premoženja nezakonitega izvora v Sloveniji, analizirane so formalne meje zakonov s področja zagotavljanja varnosti v Sloveniji, številko pa zaključujemo z analizo izpostavljenosti zaposlenih nasilju uporabnikov v domovih za starejše občane v Sloveniji.

V prvem članku z naslovom *Analysis of the Relationship between Smart Cities, Policing and Criminal Investigation* **Kaja Prislan** in **Boštjan Slak** predstavljata poglobljeno analizo soodvisnosti procesov zagotavljanja varnosti v pametnih mestih z vidika preiskovanja kaznivih dejanj, kriminalistične obveščevalne dejavnosti in zagotavljanja zasebnosti prebivalcev ter obiskovalcev pametnih mest. Avtorja poudarjata, da lahko sodobne tehnologije in storitve pametnega mesta vplivajo na načine izvajanja policijske dejavnosti in na učinkovitost policije, saj imajo lahko sodobne tehnologije in storitve pametnega mesta velik potencial za kriminalistične preiskave in kriminalističnoobveščevalno dejavnost preko informacij v realnem času. To lahko policiji pomaga, da razvije nove preiskave ali strategije za nadzor kaznivih dejanj.

V drugem članku *The Impact of the EU General Data Protection Regulation (GDPR) on Mobile Devices* **Domen Hribar, Miha Dvojmoč** in **Blaž Markelj** analizirajo novosti evropske direktive s področja uporabe osebnih podatkov (GDPR) s posebnim poudarkom na uporabo mobilnih naprav. Članek predstavlja nekatere največje spremembe, ki vplivajo tako na fizične kot na pravne osebe. Avtorji poudarjajo potrebo po razjasnitvi nekaterih vprašanj pri izvajanju uredbe skupaj s potrebo po večjem zavedanju primerne zaščite varstva osebnih podatkov, shranjenih na njihovih mobilnih napravah. Rezultati raziskave kažejo, da se posamezniki relativno dobro zavedajo koncepta varstva osebnih podatkov, kljub temu, da uredba pred njih postavlja nove izzive.

V tretjem prispevku z naslovom *An Analysis of the Legal Aspects of Illegal Assets Recovery in Slovenia* **Katja Rejec Longar** predstavlja pravno analizo odvzema premoženja nezakonitega izvora v Sloveniji skozi prizmo petstopenjskega procesa odvzema nezakonitega premoženja – finančne preiskave, zamrznitve oziroma zavarovanja premoženja, odvzema premoženja, izvršitve odločbe o odvzemu ter upravljanja z odvzetim premoženjem. Avtorica ugotavlja, da slovenski pravni red pristojnim organom ponuja več možnosti odvzema premoženja nezakonitega izvora. Uporabijo lahko klasični odvzem premoženjskih koristi v okviru kazenskega postopka, razširjeni odvzem po kazenski zakonodaji ter civilni odvzem preko tožbe v skladu z zakonom o odvzemu premoženja nezakonitega izvora. V analizi ugotavlja, da bi bilo nujno opredeliti finančno preiskavo v okviru kazenske zakonodaje, saj ni primerno, da se finančna preiskava izvaja po določbah civilnega prava.

V prispevku *Formal Boundaries of Slovenian Law* **Bojan Tičar** predstavlja formalne meje slovenskega prava predvsem z vidika veljavnega slovenskega pravnega reda. V prispevku so na pregledni način prikazani temeljni pravni instituti. Avtor s pomočjo rimskopravnega pogleda na pravne pojme opisuje, kakšen je odnos piscev s področja teorije prava pa tudi s področja kritičnega prava na definiranje ključnih pravnih pojmov in pojavov.

V zadnjem članku *User Violence against Employees in Nursing Homes* **Katarina Cesar, Liljana Rihter, Špela Selak** in **Branko Gabrovec** analizirajo vrste in razširjenost nasilja na delovnem mestu med zaposlenimi v socialnovarstvenem zavodu. Ugotovili so, da so zaposleni najpogosteje izpostavljeni verbalnemu nasilju, najmanj pogosto pa doživljajo neželeno vedenje spolne narave. Z nasiljem uporabnikov se pogosteje srečujejo zaposleni na področju zdravstvene nege kot zaposleni na drugih področjih. Ugotovili so tudi, da ob tem zaposleni občutijo strah, nemoč in negotovost.

Uredniški odbor revije Varstvoslovje upa, da bodo izbrani članki za bralce zanimivi in vir novih idej. Ker je pričujoča izdaja revije zadnja v letu 2018, vam celotna ekipa revije želi vse dobro v letu 2019.

Izr. prof. dr. Branko Lobnikar
Urednik številk v angleškem jeziku

VARSTVOSLOVJE,
Journal of Criminal
Justice and Security,
year 20
no. 4
pp. 389–413

Analysis of the Relationship Between Smart Cities, Policing and Criminal Investigation

Kaja Prislan, Boštjan Slak

A gunshot rings out in a high-crime section of a large city. A car speeds away. A victim lies on the sidewalk. An audio sensor embedded in a nearby streetlamp detects the sound of gunfire, identifies where it came from and, through a high-speed backhaul to the nearest real-time crime center, alerts dispatchers to the situation. As police and emergency medical technicians race to the scene, the streetlight brightens to its full capacity, making it easier for first responders to see what's going on. Behind the scenes, the feeds collected by the surveillance cameras automatically are run through databases housing fingerprint, DNA and mugshot information. Real-time license plate and facial recognition technologies are applied, and a data analytics engine kicks in to correlate the data and provide actionable intelligence. The result? The perpetrators can be more quickly captured by law enforcement.

(Pillaipakkam, 2017, pp. 33–34)

Purpose:

The main objective is to present the symbiosis between smart cities, policing, criminal investigation and criminal intelligence. Moreover, another purpose is to critically address the underlying privacy concerns arising from smart city designs.

Design/Methods/Approach:

The paper is theoretical in scope and utilises a literature review as the basic method. Correlations between smart cities, policing and criminal investigations are identified by analysing the applicability of core smart city technologies and services [SCTS].

Findings:

It is evident that SCTS can influence policing styles and police effectiveness. SCTS hold great potential for criminal investigations and criminal intelligence as they provide information upon which police can develop investigations or crime-control strategies. Vice-versa, criminal investigations and criminal intelligence can provide guidelines for SCTS developers and the governance of smart cities. However, privacy concerns and the slowly developing regulatory framework remain the biggest issues when it comes to SCTS adoption, thus making measures to safeguard privacy a key factor for the legitimacy of smart cities and smart policing.

Practical Implications:

The paper introduces practical knowledge about the implications of smart cities for policing and crime investigation. Some research ideas are presented as

well as suggestions for legislators, developers and others whose work area falls in the scope of (smart) city governance.

Originality/Value:

A comprehensive study of the symbiosis between smart cities and policing must not only consider the potential of SCTS but the related need to develop regulation and skillsets of human resources. Only a handful of papers address the connectivity of smart cities, criminal investigations and criminal intelligence from such a multidisciplinary scope. Therefore, the paper represents a contribution to works discussing these concepts.

UDC: 351.78:004.7

Keywords: smart cities, safety and security provision, policing, criminal investigation, criminal intelligence

Analiza povezanosti pametnih mest s policijsko in kriminalistično dejavnostjo

Namen prispevka:

Namen prispevka je predstaviti simbiozo med pametnimi mesti, policijsko dejavnostjo, kriminalističnim preiskovanjem in kriminalističnoobveščevalno dejavnostjo. V tem kontekstu je podan tudi kritični razmislek o izzivih in dilemah, povezanih z varstvom zasebnosti.

Metode:

Prispevek je teoretične narave in temelji na pregledu literature. Korelacije med temeljnimi pojmi (pametna mesta, policijska in kriminalistična dejavnost) smo identificirali z analizo temeljnih tehnologij, sistemov in storitev, ki podpirajo delovanje pametnih mest.

Ugotovitve:

Tehnologije pametnih mest omogočajo razvoj novih oblik policijskega dela in imajo potencial za izboljšanje policijske učinkovitosti. Funkcionalnost tehnologij je razvidna tudi na področju kriminalistične dejavnosti, ki lahko z obdelovanjem podatkov in njihovo uporabo bolje načrtuje kriminalistične preiskave in razvija strategije preprečevanja kriminalitete. Simbioza je opazna tudi z nasprotnega vidika – s podajanjem smernic lahko kriminalistična in policijska dejavnost pomagata upravljavcem pametnih mest in razvojnikom tehnologij ter rešitev. Glavni izziv predstavlja varovanje zasebnosti in osebnih podatkov prebivalcev, zato so mehanizmi za preprečevanje zlorab ključni faktor legitimnosti pametnih mest in policijske dejavnosti.

Praktična uporabnost:

V prispevku so predstavljena uporabna znanja glede potencialov pametnih mest za izvajanje policijske in kriminalistične dejavnosti, prav tako tudi predlogi za raziskovalce in oblikovalce politik, razvojnike in druge, ki delujejo na področju upravljanja (pametnih) mest.

Izvirnost/pomembnost prispevka:

Če želimo razumeti sistem dejavnikov, ki vplivajo na simbiozo med policijsko dejavnostjo in pametnimi mesti, je treba upoštevati ne samo potenciale različnih tehnologij in rešitev, temveč tudi potrebe in dileme, ki se pojavijo sočasno s tehnološkim razvojem, primarno na področju razvoja kadrovskih kompetenc in prilagoditve normativnih okvirjev. Pregled literature pokaže, da obstajajo redke znanstvene objave, ki multidimenzionalno proučujejo simbiozo pametnih mest in policijske dejavnosti. Prispevek zato dopolnjuje obstoječa dela in znanja na tem področju.

UDK: 351.78:004.7

Ključne besede: pametna mesta, zagotavljanje varnosti, policijska dejavnost, kriminalistično preiskovanje, kriminalističnoobveščevalna dejavnost

1 INTRODUCTION

Technological development undoubtedly had and continues to have such an immense impact on human lives that modern societies are developing with evolutionary dynamics. According to Ramaprasad, Sánchez-Ortiz and Syn (2017), the technological development of societies also led to the transformation of cities. In the earliest days, human beings lived in groups since they improved the chances of their survival. The settlements that developed from this coherent style of living led to the development of urbane environments. It is today estimated that 55% of the world's population lives in urban settlements. By 2030, urban areas are projected to house 68% of people globally (United Nations, 2018). In Europe, for instance, "urban areas are home to over two-thirds of the EU's population, and they account for about 80% of energy use and generate up to 85% of Europe's GDP" (European Commission, n. d. b). The first settlements formed in response to certain challenges (i.e. dangers arising from the natural elements, animals and/or dangerous groups). Yet, the growing number of people demanding miscellaneous infrastructure, in a social and physical sense, led to the creation of complex cities, where "the rapid urban growth that brings traffic congestion, pollution, and increasing social inequality may turn the city into a point of convergence of many risks (economic, demographic, social, and environmental)" (Ramaprasad et al., 2017, pp. 13–14). In a way, the city itself is becoming a threat to human beings, entailing the culmination of different threats, among which physical and social threats dominate. Physical threats come from traffic, malfunctioning infrastructure (damaged power lines, collapsing buildings, fires etc.), poor air, water etc. quality, or the occurrence of transmittable diseases. 'Social' dangers are reflected in criminality, and they usually grow with the size of a city. With population growth crimes and criminals are becoming more sophisticated (FICCI-E&Y, 2015). In recent years, new and complex threats have emerged, highlighting the need for closer and more efficient cooperation at all levels. Terrorism, organised crime and cybercrime are today considered the top modern threats and defined as priorities by the European Commission (2015) in its European Agenda on Security.

Nevertheless, cities have a rising number of tools available to combat these problems and acts of crime, where modern technology is one of them (The

Economist Intelligence Unit, 2017). Therefore, we can see cities as both a source *of* and *a solution to* today's economic, environmental and social challenges. By integrating modern information and communications technology [ICT] into cities' infrastructure, we can support their development, management and overall governance. Modern ICT can be used to address various issues and problems related to living and working in urban cities, including security and feelings of safety. A 'smart city' refers to the situation when a city's operations and basic functions are supported by smart solutions and modern ICT. Accordingly, global market trends show significant growth in user demands and investments in so-called smart security solutions. In several developed countries, security stakeholders' awareness has also increased and thus (public and private) security organisations are already adapting to these trends and employing new technologies to improve their responsiveness, legitimacy and overall efficiency. The vision of smart security, which is a sub-system of a smart city, is to help address common security problems and, above all, contribute to the more efficient operations of security organisations.

Two main trends encourage the development of smart security solutions:

- The de-etatisation and decentralisation of security responsibilities and policing activities, which includes plural policing (Modic, Lobnikar, & Dvojmoč, 2014; Sotlar, 2015),[1] the segregation of duties between different public and private, national and local security stakeholders, which in turn requires a multi-stakeholder approach to ensuring safety and security (Boels & Verhage, 2016; Sotlar, 2015). This leads to a stronger need for improved coordination, information management, data sharing and communication systems.
- The evolution of security risks, which refers to the fact that security threats and events are becoming more unpredictable, organised and hybrid, making them more unpredictable and harder to manage (European Commission, 2016). This stimulates a stakeholders' consideration of the potential of modern ICT, and higher investments in research and development, especially smart detection solutions.[2]

Yet while smart city technologies can bring substantial advances to the overall quality of life, they also (by)produce a substantial quantity of data (i.e. big data)[3]

1 *The main challenge of plural policing relates to co-operation between the various organisations. Intra-city traffic violations, maintaining public law and order in the cities and similar tasks are for example more and more performed by municipal wardens. However, the most serious offences and crime-related issues certainly continue to be a task for the police and other law enforcement agencies [LEAs].*

2 *Market growth (the CAGR approximately 10%) of the security industry is predicted to stay stable, which is related to the rising popularity of smart security products (Grand View Research, 2018; Stratistics Market Research Consulting, 2017). The global market in physical security is expected to grow by 100% between 2017 and 2023 (Allied Market Research, 2018).*

3 *Završnik (2018a) states that we can speak of big data if six characteristics are present, namely: I) there is big volume of data; II) data is processed very quickly; III) there is a high variety of data; IV) there is a strong veracity of data; V) the value of the data is high; and VI) there is a certain vulnerability of such data.*

that can be used either positively (predictive analyses, scientific research etc.)[4] or negatively, where the most noticeable are privacy violations (Galdon-Clavell, 2013; Talari et al., 2017; van Zoonen, 2016). This paper addresses some of these concerns, with a specific look at the use of different SCTS and the data of smart cities for police and criminal investigative work. The purpose of the paper is to introduce the relationship of two trending topics which are developing alongside each other but are often separately researched. The possible symbiosis of these two concepts – policing and smart cities – is presented, together with use cases and global forecasts.

The paper may be useful for national and local security organisations and other users wishing to monitor global trends in the area of policing smart cities. It is particularly relevant for the shareholders operating in the security domain seeking to become actively involved in its development. The paper is structured as follows: the first section introduces the concepts of smart city, the second provides a more detailed description of the smart cities concept, the third considers the connection between smart technologies and policing, with subchapters more narrowly focusing on the symbiosis between smart cities, criminal intelligence and criminal investigation. The fourth section discusses privacy concerns in relation to SCTS. The last, fifth section summarises the findings and discusses a set of issues in need of research to support further discussion on the issues of usability and matters of smart cities.

2 SMART CITIES

Smart cities (also known as cyberville, digital city, electronic community, flexicity, information city, intelligent city, knowledge-based city, MESH city, telecity, teletopia, ubiquitous city, wired city; (Eremia, Toma, & Sanduleac, 2017; Komninos, 2008)) are a relatively new concept and thus no standard definition has been developed yet, although varying explanations and interpretations are available:

- A smart city is a place where traditional networks and services are made more efficient with the use of digital and telecommunication technologies for the benefit of its inhabitants and business. (European Commission, n. d. a)
- A smart city uses information and communication technology to enhance its livability, workability and sustainability. It collects information about itself using sensors, devices or other systems, and sends the data to an analytics system to understand what's happening now and what's likely to happen next. (Berst & Logsdon, 2016)
- A place where traditional networks and services are made more flexible, efficient, and sustainable with the use of information, digital

4 *Since the amount of data is so vast and diverse, big data is in a way a "theories generator" and not only an empirical pool used for theory testing (Završnik, 2018b). This implies the natural usefulness of big data for a grounded theory methodological approach (Glaser & Strauss, 2009). Frequently connected to smart cities is the so-called living lab 'approach' where research projects use the city sensors and the (big) data they accumulate to research various aspects of human behaviour. There are numerous such labs (for a list, see The European Network of Living Labs (ENoLL), n. d.), although the such use of city sensors and their data is not to be considered as being without dangers (Galič, 2018).*

and telecommunication technologies, to improve [city'] operations for the benefit of its inhabitants. Smart cities are greener, safer, faster and friendlier. (Mohanty, Choppali, & Kougianos, 2016, p. 60)

- 'Smart cities' is a term denoting the effective integration of physical, digital and human systems in the built environment to deliver sustainable, prosperous and inclusive future for its citizens. (The British Standards Institution, 2014, p. 3)
- A smart city uses digital technology to connect, protect, and enhance the lives of citizens. IoT (Internet of Things) sensors, video cameras, social media, and other inputs act as a nervous system, providing the city operator and citizens with constant feedback so they can make informed decisions. (CISCO, n. d.)
- There is no doubt that a Smart City is a multidisciplinary concept that embodies not only its information technology infrastructure but also its capacity to manage the information and resources to improve the quality of lives of its people. (Ramaprasad et al., 2017, p. 15)
- … an intelligent city is a multi-layer territorial system of innovation. It brings together knowledge-intensive activities, cooperation-based institutions for distributed problem-solving, and digital communication spaces to maximise this problem solving capability. (Komninos, 2008, pp. 123–124)
- Smart cities are an endeavour to make cities more efficient, sustainable and liveable. In other words, a smart city is a city that can monitor and integrate functionality of all the critical infrastructure like roads, tunnels, airways, waterways, railways, communication power supply, etc., control maintenance activities and can help in optimizing the resources while keeping an eye on the security issues as well. (Joshi, Saxena, Godbole, & Shreya, 2016, p. 902)

The common theme of these smart city interpretations is the use of ICT and other technologies to improve public services in combination with personnel and innovative developers. Since this approach generates a substantial amount of data (Mohammadi & Al-Fuqaha, 2018; Mohanty et al., 2016; van Zoonen, 2016; Završnik, 2018b), it influences the relationship between residents, data and governance (Powell, 2014).

We propose a summary definition that encompasses the notions listed above and thus, in our view, smart cities can generally be described as complex ecosystems and living organisms that are aware and constantly evolving. They may be seen as a learning places that, with the help of modern technology, collect and analyse various data, and adapt their services to the needs of the community and their problems. The smart city ecosystem has three main pillars: People/ Technology/Skills and competencies.

The purpose of merging these elements is to create synergy in the form of innovations that solve the problems of a certain community. The main goal is to develop products or solutions that help improve the quality of services, reduce current costs and negative environmental impacts, and increase the public sector's response to solving communities' problems.

Among the several characteristics that define a smart city (Eremia et al., 2017), one of the main ones often stressed in existing smart city frameworks is its multidimensionality. Often referred to, the Giffinger et al. (2007) model describes six pillars of smart cities:

- Smart economy: improving the local economy's competitiveness through innovation and entrepreneurship;
- Smart environment: greater energy efficiency, a green economy, sustainable resource management;
- Smart governance: digitisation of public administration and open data;
- Smart living: improved quality of life supported by technology and advanced solutions in the fields of health, safety and culture;
- Smart mobility: better logistics in transport and traffic management;
- Smart people: incentives with the aim of developing new skills, improving competences, creativity, level of qualification and participation of people in public life (also see Joshi et al., 2016).

Considering the diversity of smart city sub-systems, it is crucial for the various stakeholders, primarily residents, to be involved as a source of information in the development process. Here, we mean a co-innovation process with reference to the triple helix approach, which states that, in addition to the public, three core groups of stakeholders should be involved: policymakers, researchers and industry that can, by sharing views and ideas, achieve real synergy (Leydesdorff & Deakin, 2011).

Smart technologies have many purposes and possible applications. One of the smart city's sub-systems is a safe city supported by smart security that covers all safety aspects of the city. A safe city in a smart city is a city that by integrating technology into the natural environment increases the effectiveness of safety-related processes in order to reduce crime and terror threats, to allow its citizens to live in a healthy environment, have simple access to healthcare, and achieve readiness to be able to quickly respond to threatening emergencies (Lacinák & Ristvej, 2017). Here the question appears of how the policing of smart cities should be organised and how these two systems can mutually benefit each other.

3 SMART CITIES AND THEIR POLICING IMPLICATIONS

Apart from the mentioned trend of plural policing, authors (e.g. Newburn, 2007; Willis, 2014) also note that while reactive and routine-based policing remains the principal policing style, there is a great demand to change the style of policing to become more proactively focused (Newburn, 2007). Consequently, policing styles are emerging that rely on analytical and/or data driven, informed policing related decision-making. Most prominent are evidence-based policing [EB], intelligence-led policing [ILP] (Ratcliffe, 2008), problem-oriented policing [POP] (Braga, 2014) and the type most affected by smart and innovative technologies – predictive policing [PP] (Završnik, 2018b). While all forms of policing take

advantage of advances in ICT (SeaSkate, 1998) and policing research,[5] PP is the type that utilises it the most. By using computerised analysis of mass data on past crime, local environment, temperature and other seemingly unimportant information, state security entities can predict and prevent crime or improve LEAs' responses since predictive algorithms can indicate where they will be possibly needed. It should also be noted that prediction methods are not sufficient for the arrest of a suspect because the predictions are generated by statistical processing as part of the analysis of past criminal data and other data. They only produce rough estimates and probabilities of events in the future so this information must be considered as merely giving support for other more traditional policework forms (Perry, McInnis, Price, Smith, & Hollywood, 2013). Such use of ICT for safety and security reasons has triggered discussion of the implications of big data analysis for policing and crime preventions. Despite the undeniable potential held by big data for such purposes, certain core issues remain:

- the data are actually subjective (the data are among other sources generated from police statistics that are racially biased) (Završnik, 2018b); and
- big data is extensive, thereby bringing with it the issues of proper analytics and data management (Baig et al., 2017; Mohammadi & Al-Fuqaha, 2018).

However, while its applicability must still be tested for these two core issues, examples of the application of PP in Chicago[6] (Douglas, 2018) or Santa Cruz (California)[7] (Rich, 2011) are seen as promising.

Data for police use may be generated by using digitised records of criminals, CCTV, unmanned (aerial, (under)water, ground) vehicles, body-worn cameras, social media feeds and data analytics,[8] application of Artificial Intelligence

5 *Nowadays, ICT is used in almost every aspect of police work. From dispatch calls, patrol tracking and for communicating to various improvements in crime scene investigations, to report writing and analysing (SeaSkate, 1998).*

6 *As Douglas (2018) writes "…//using the latest in IT, including video surveillance and computer analysis of incidents, is reducing violent crime in the city". With regard to statistics "Citywide, shootings dropped 21 percent in 2017 compared to 2016, … //… and in districts No. 7 and 11, on the city's southern and western sides — home to the first two [Strategic Decision Support Centers] — shootings are down 33 percent."*

7 *The pilot project can be described as successful. Software uses specially designed algorithms to calculate and predict crime hotspots and then suggest where police patrolling should take place. "In the nearly two months of use, the pilot has garnered positive results. Since the pilot's deployment, the model has correctly predicted 40 percent of the crimes that it was aiming to predict, and the Santa Cruz Police Department has seen a reduction in the types of crime that it's been addressing. In addition, the Police Department saw a 27 percent decrease in the number of reported burglaries in July compared with July 2010." (Rich, 2011)*

8 *A report by FICCIJA and Ernst&Young (FICCI-E&Y, 2015, p. 16) gives an example of the Los Angeles Police Department's (LAPD) usage of "social media to help guide department operations during major events such as the NBA All Star Game in 2011 and the Stanley Cup playoffs in 2012. During these events, the department tracked large-scale parties and other gatherings throughout the city, and deployed teams of building inspectors, police officers, and fire department officials to ensure the events were legal and safe. The department also monitored social media to keep a tab on 'trending' topics, such as whether large crowds of people planned to head downtown, and adjusted deployment plans accordingly. The LAPD has fully integrated its social media branch into the command post structure for major events. The social media branch is responsible for briefing the incident commander about relevant activities on social media."*

[AI] etc. as well as via the traditional police officer–citizen relationship.[9] Police departments create large volumes of digitised data which may improve officers' decision-making (FICCI-E&Y, 2015). In essence, this relationship between smart cities and ICT technology in policing would entail so-called smart policing. Smart policing may be defined by the use of modern technology and processes that increases police officers' efficiency and effectiveness in the field. It should include real-time data, social media communication, field tablets, predictive policing tools, and several other options (FICCI-E&Y, 2015).

While smart technology is presently used to prevent and/or to react to (respond, sanitise, investigate) an incident deriving from human behaviour, the latest trend is moving strongly in the direction of attempts to modify human behaviour. One example is China's Social Credit System that ranks residents (they 'collect' or 'lose' points) for their adherence to (in)formal social rules and their overall diligence (paying bills on time, committing traffic violations etc.) (Larson, 2018). This may be seen as an extreme form of (Pavlov) conditioning where technology plays the role of a stringent ever-present watchman. In line with routine activity theory, such technology for monitoring can deter crime since the third factor (the absence of a capable guardian) does not apply – the guardian is 'always' present. Going a step further, social media – an important part of the smart city by connecting the city with its inhabitants – is a tool of unprecedented usability. There are indications that, for example, voting behaviour and actual candidate choices have been affected by such (ab)use of social media (Završnik, 2018a). Undoubtedly, this holds substantial implications for the threat landscape and thus for policing. The questions regarding smart cities and policing have focused primarily on the increased surveillance capacity a highly networked urban setting provides for law enforcement. SCTS can trigger the response of criminal investigative apparatus with the proactive or real-time detection of criminal acts and security incidents.

3.1 (Criminal) Investigation and smart cities

Criminal investigation can be defined as "the process of discovering, collecting, preparing, identifying and presenting evidence to determine what happened and who is responsible" (Hess & Orthmann, 2010, p. 6). Palmiotto (2013, p. 4) explains "[C]riminal investigation is a thinking and reasoning process. The modern investigator's primary objective is to gather facts about a criminal situation. This objective is accomplished by collecting all the accurate information pertaining to a specific act or crime". In essence, this usually pertains to an array of activities – depending on the form of the criminal justice system – by the police, prosecutors and judicial branch (Maver et al., 2004). A criminal investigation typically starts upon the discovery of an event or its consequences that have signs of a crime. It is not always necessary that an investigation will confirm a crime was conducted

9 *In a more critical view, the option that citizens with their smart devices report acts of deviant behaviours to the police is what Završnik, (2018a, p. 48) denotes as "community policing 3.0", marking citizens as "walking sensors" and an actual part of the smart grid sensor system.*

(Dvoršek, 2008); therefore, some authors (e.g. Bryant, 2010) contend the main goal of a criminal investigation is to know the *truth*. A crucial element in explaining the subject events is information (Gottschalk, 2010) and other data upon which criminal investigators can build while reconstructing the timeline causality of events. That is why it is perhaps easy to see criminal investigations as a reactive activity. However, they can also be proactive when investigators with informational analytics, criminal intelligence[10] or informants and other sources predict criminal behaviours. This short definitional narrative shows that *information* is absolutely crucial for an effective criminal investigation. This is also the core reason we can assert that there is a natural symbiosis of smart cities, criminal investigations and/or criminal intelligence.

3.2 The Benefits of SCTS for Criminal Investigation and Intelligence

While gunshot,[11] scream or glass-shattering sensors, traffic accidents alert systems etc. are chiefly used to expedite faster responses from first-line responders, they can also be used in criminal investigations. Some examples are given in the following use cases.

The log files of sensors give very precise information for specifying the time of an event. This information is probably far more accurate than eyewitness accounts. Log data generated by smart vehicles that 'communicate' with smart city infrastructure in order to give drivers and passengers the most up-to-date information on one hand or to adjust city traffic systems on the other (Baig et al., 2017) can in criminal investigations be retrieved from either the vehicles or the city system and used to establish alibis, traveling routes etc.

Weather-monitoring systems data can be used to more easily or more properly interpret crime scene traces. Environmental factors and the weather situation must always be documented at crime scenes (Maver et al., 2004; Palmiotto, 2013) and later considered in the investigation (e.g. air temperature, precipitation data can be used to more accurately determine the time of death; wind speed and direction can be used for ballistic reconstructions etc.).

Smart cities (or neighbourhoods) also use Wi-Fi systems to first provide free Internet access and/or provide information to those entering a certain area. This, in turn, means data are created concerning mobile phones that have entered a particular space (Galič, 2018). Such data can be used in criminal investigations when we are interested in the movement of a given person, or when a certain timeline must be established. It can also be used to transmit crucial information such as Amber alerts or information on missing or wanted persons.

One may presume that the good sensor grid systems established and utilised for monitoring air or water quality (Talari et al., 2017) could detect illegal waste

10 *Ratcliffe (2008, p. 7) uses the term crime intelligence in his book »as a collective term to describe the result of the analysis of not only covert information from surveillance, offender interviews and confidential human sources (informants), but also crime patterns and police data sources as well as socio-demographic data and other non-police data«.*

11 *Gunshot sensors are acoustic sensors that can be used to detect firearms use and localise the shooter (Khalid, Babar, Zafar, & Zuhairi, 2013).*

dumping. Similarly, smart meters for electric consumption that ease the reporting of electricity consumption to the supplier (Galdon-Clavell, 2013) could also be used to identify possible locations for indoor growing of cannabis (Baig et al., 2017).

Platforms that enable citizens to submit initiatives to improve the quality of life in a city or to report issues they encounter in their lives could also be used as portals for reporting and helping to discover crimes. Such communication with a citizen, usually via social media, is recognised as critical tool for smart cities (Joshi et al., 2016) and thus also useful for various policing tasks. The accumulated data from platforms that allow citizens to submit initiatives for improving the quality of life in the city or to report issues they encounter in their lives is a basis for criminal intelligence to more efficiently build its analytical and intelligence products. This, in turn, can be used to detect emerging crime issues and trends or to influence decision-makers to adapt/change the policing style in a certain area.

In cases of tactical intelligence, namely, where intelligence is used for a specific event (Peterson, 2005), data from SCTS can also be relied on. Pereira, Macadar, Luciano and Testa (2017) in a paper for which they interviewed several personnel working with(in) the Centre of Operations Rio de Janeiro (a form of smart city control and analytics centre) report how good cooperation between the developers of a traffic application and the city administration facilitated better work and overall handling of the situations during the Pope's visit to Brazil.

Citizen participation (e.g. crowdsourcing) platforms in a way also enable citizens to become more empowered and included in the city governance, especially if platforms also include feedback from the city leadership or an agency to which a comment or criticism was intended. Such communication channels, if effective, can reduce dissatisfaction with the city or public administration (Pereira et al., 2017). This could thereby also be a form of crime prevention since communicational feedback gives a person the feeling of having been heard and in some cases prevents negative attention seeking/retributive behaviour (e.g. sending envelopes with white dust to administration offices, threats to public officials etc.).

3.3 The Benefit of Criminal Intelligence and/or Criminal Investigations for Smart Cities

In contrast to the criminal intelligence contribution to smart city systems, due to their focus and the specificity of an individual event, criminal investigations inputs are somewhat limited. The greatest benefit is observed when a smart city system infrastructure is under attack or a crime has been committed against the city itself (e.g. intrusions in various systems that run city power lines, traffic systems etc.) and where digital forensics is used to investigate the event. The data derived from such investigations represent a form of system vulnerability test and can be used to improve the security of the mentioned systems (Baig et al., 2017).

On the other side, strategic intelligence, which deals with information with regard to crime trends and among others develops crime-control strategies (Peterson, 2005), can be used to pinpoint the locations where SCTS can/should be applied. Alternatively, to determine what sort of technology is needed to tackle a

given form of crime in a specific area, e.g. smart lights and aroma diffusers can be used in a particular area at a defined time. The selection of the area, time and form of technology can be based on crime statistics, criminology scholarship as well as a range of other data (mobile phone data, social media analysis etc.) (Meijer & Thaens, 2018). This implies that 'smart' technology is an element of situational prevention.

The broad array of the underlying relationship between smart cities and different policing forms is summarised in Figure 1 below.

Figure 1: Graphic illustration of relationships between smart cities, policing, criminal intelligence and criminal investigations

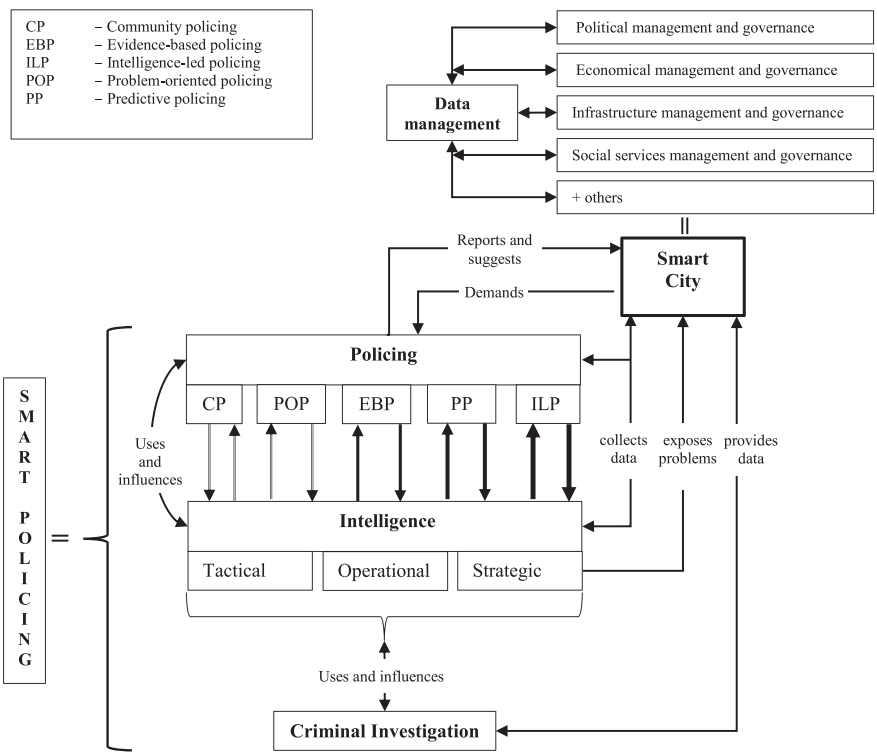

Figure 1 shows a model of correlations between smart cities, policing, criminal intelligence and criminal investigation. Technologies that support smart city functions enable more effective and efficient data management in governing political, economic, infrastructure and social divisions. The information produced by smart cities is usable in all areas related to public security provision, and also for different types of policing. The model also reflects that smart city data management can support the development of smart policing.

While the above figure shows the relationship between different actors and functions that (or at least should) work together to provide security, the technologies that (could) provide data and support policing activities take many different forms. Table 1 below summarises some of the most common core smart city technologies and their possible use for policing, criminal intelligence and criminal investigations.

Table 1: Technology used in smart cities and most easily used in policing, criminal intelligence and criminal investigations

Technology/ system	Primary use	Potential for policing	Potential for Criminal Investigations and/or Criminal Intelligence*
4G / 5G networks	Broadband mobile communications (cellular wireless networks) with high speed, reliability and coverage.	Improved data communications between officer(s), control centres, patrols etc. Networks that enable more (not just voice) and better data to be communicated.	Such networks that enable data (voice, imagery, diagnostics etc.) from various personnel to be recorded or transferred. This in turn eases investigators' work by providing data (evidence) for their cases or real-time information search. If the data recorded or transferred via such networks is analysed more coherently, it can be used for strategic, tactical or operational intelligence, e.g. data mining.
Body-worn cameras and devices	Provide a feed from human operators to control/support centres to obtain information on the psychological or psychical status of the operators, to give support staff enough data to provide support to operators, provide imagery for further analysis (used by army, astronauts, police, in a way also surgeons, divers etc.).	Wearing body cameras by patrolling police officers influences their own behaviour and of persons in police procedures.	Imagery from police officers' body cameras provide data for criminal investigations and can also give evidence of use in investigations. If data is analysed in a more coherent way it can be used for tactical or operational intelligence (can provide info on suspects and locations for breaching actions).
Advanced CCTV	Active video surveillance of locations connected to monitoring systems that include recognition and alarm capabilities and retrospective analytics.	Monitoring locations, events and disruption identification. For example, detecting potentially malicious behaviour, followed by further real-time, pro-active investigative techniques.	Gathering and reviewing information for a specific location/event/ person(s). Can provide evidence useful for investigating crimes already committed. Such technology can from the point of criminal intelligence be used for targeted monitoring of persons of interest. It also has the potential for tactical or operational intelligence.
Geographic information systems (GIS)	Various analytical, research and diagnostic usage. Pollution, traffic, geological etc. monitoring.	Mapping of crime 'hot spots'.	Provides data/information to criminal investigators and/or assists with the development of timelines, mapping locations of crucial events. If data is analysed more coherently, it can be used for strategic planning or tactical and operational intelligence, e.g. suspect movement analysis etc.

Table 1: Continuation

Technology/ system	Primary use	Potential for policing	Potential for Criminal Investigations and/or Criminal Intelligence*
IoT	Collection and storage of various data. Connectivity among devices enables better usability, monitoring, controlling and diagnostics of devices connected with each other (long-distance management of electronic grids, reduced electricity consumption etc.).	Crime analytics, predictive policing, crime mapping.	Provides data that can be used in investigations (e.g. electricity consumption and illegal laboratories). The IoT promises extreme usefulness for criminal intelligence – in a strategic, operational and tactical sense, e.g. building a portfolio of places, people and behaviours – used to plan proper actions or responses.
Sound sensors for screams or gunshots or breaking glass	To activate first responders or automatically notify security personnel in the near proximity that an incident might be developing.	Faster detection of events and lower police response time.	Data logs from such a sensor provide precise information as to when a specific sound was detected – helping to establish an event timeline. If data is analysed in a more coherent way, it can be used for strategic, tactical or operational intelligence, e.g. analysing criminal behaviour patterns at a certain location.
Smart public lightning system	Improved management and effectiveness of the public lighting system and sensors installed on light posts can all be used for monitoring traffic, pollution etc. levels.	Adapting the brightness level to various situations influences crime prevention or officer safety (e.g. brightening to provide greater security or an overview of some location).	Crime scenes can be better examined at night if the brightness can be adjusted, sensors on light posts can provide data for crime investigations.
Smart grids (of any kind)	Provide a better user experience and easier control of the matter (electricity, water, gas, Internet, traffic etc.) transmitted in the grid. Smart grids could also be used for research and predictive analysis. E.g. smart electricity consumption monitoring technology could be used for other purposes such as determining the size of the informal economy by monitoring electricity consumption.	Some grids (traffic-related) provide more safety than non-smart grids. For example, the usage of AI makes traffic flows more fluid.	Crimes can be more easily detected. Some data generated from the smart grid log systems can be used in investigations. If data is analysed more coherently, it can be used for tactical or operational intelligence, e.g. detecting criminal behaviour related to consumption of what is transmitted through the grid.

Table 1: Continuation

Technology/ system	Primary use	Potential for policing	Potential for Criminal Investigations and/or Criminal Intelligence*
Social media monitoring tools and crowdsourcing platforms	Gathering intelligence with advanced analytics performed on social media content, gathering information from the public.	Planning activities, detecting societal problems, public communication.	Social media contributions by suspects, witnesses or other sources can be useful for investigators as they can post information about a particular event, person or location. Such data can be used as evidence in proper circumstances. Gathering data from user posts and communication on events, locations and people monitoring. As part of OSINT, the value is diverse.
Unmanned aerial vehicles ('drones')	Various monitoring of situations and scanning locations or objects (geographical scanning, aerial photography); delivery of products; general consumerism (hobby, DIY development etc.); multimedia (movie making) and more.	Monitoring of events, locations and people.	Crime scene investigations (aerial photography), covert surveillance etc. If data is analysed in a more coherent way, it can be used for strategic, tactical or operational intelligence. Analysing criminal behaviour, gathering intel for breaching actions or high-profile arrests etc.

* Since police investigators use products of criminal intelligence, the primary users and in fact the form of technology use cannot be always clearly abstracted, we therefore jointly provide examples for criminal intelligence and criminal investigation use of the most common technologies. The Criminal Intelligence segments build heavily on the work of Peterson (2005).

4 PRIVACY CONCERNS

As indicated, smart cities amass enormous volumes of data and the opening up of this data for application creates different, legitimate privacy concerns (Galdon-Clavell, 2013; Galič, 2018; Kanduč, 2018; Talari et al., 2017; van Zoonen, 2016; Završnik, 2018b). As Fujs and Markelj (2018) observed, smart technologies give people a certain degree of leisure in return for lower privacy. The concern is not just that the government will utilise the technology to spy on people, but the technologies and data can also be hacked by criminals (Baig et al., 2017) for use in an array of criminal acts or misused by businesses (Galič, 2018; Kanduč, 2018; Završnik, 2018a). The latter might occur intentionally or unintentionally as the mishap of Amazon's Echo system revealed when the system erroneously recorded and made private conversations public (Chokshi, 2018).[12] Although

12 *Due to the sheer number of these systems sold and installed and the manner of how they work and what they do – the system hibernates and waits for speech commands from the users, when commands are given, they are recorded and executed by the system. In turn, systems store a variety of data (speech recordings, usage logs, device cache as well as other data such as calendars or to-do list) on the Amazon cloud service and/or devices themselves. This data promises great usability for criminal investigations (Orr & Sanchez, 2018), either from the point of criminal intelligence where investigators can gather data on a person of interest or perhaps even use these systems for undercover surveillance. In less intrusive purposes, criminal investigators can use data for establishing timelines, alibies etc.*

people are willing to accept constant monitoring and are self-motivated to share their private data with private businesses in order to obtain better services or some loyalty points and discounts (for example, numerous loyalty clubs, cards and lists promise different benefits in return for data on our purchase, viewing, communicating, driving, sleeping, recreating etc. habits), they also lawfully, albeit naively, expect the information will not be compromised or misused. In democratic countries scoring high on the human freedom index, people often see these rights as self-evident and generally take them for granted – customer expectations arise from given regulatory safeguards and beliefs that the system works, and that organisations are properly monitored. However, in reality, when using different services and applications people's privacy depends strongly on the integrity and ethics of (service) providers since users have a very limited insight into the security and protection of the data, while how effective control mechanisms are depends on various factors (customers' reports, staff workload, varying regulations in different states etc). Nevertheless, the new Regulation (EU) 2016/679 of the European Parliament and of the Council (2016) (EU General Data Protection Regulation [GDPR]) recently implemented across the EU looks promising and might also encourage the greater social responsibility of service providers and data collectors. Thus, concerns remain that everyday elements that are carried/worn (smartphones, smartwatches, and accessories, NFC key rings, wallets, even clothes) that have built-in systems or chips (NFC, RFID tags etc.) will be turned into a targeted person-monitoring tool. The same concerns also relate to the use of SCTS. For example, there is a perceived danger that LEAs could utilise the smart city grid of sensors to track and monitor individuals. Consideration and caution are clearly necessary, yet if there is a sufficient burden of proof or if an intelligence agency does not need one it is far simpler to just directly install Trojan-type software on a suspect's electronic device (Abel, 2009) or wearable accessory and use that to track and monitor them, without relying on the smart city grid of sensors.[13] In any case, the proper regulative framework must be developed and enforced to prevent unlawful access to and distribution of data generated by SCTS. By this, we refer mainly to the legal loopholes which are very common due to fast pace of technological development. Spencer (2017), for example, points to the framework in the United States of America which, for instance, states that while privacy (and thereby data) against unlawful searches is protected by Fourth Amendment, this protection does not apply to third parties. This means that data is only protected from LEAs and not from businesses, which could be (ab)used by LEAs to 'outsource' data gathering.

Van Zoonen (2016) notes that discussions of privacy concerns in connection with smart cities should consider types of data, the purpose of the data, and their collectors. There is a complex diversity of factors influencing levels of risk for privacy violations. In our view, the risk level depends on the combination of three factors connected to data generated by SCTS. Namely: 1) users (*who uses the data?*); 2) purposes (*for what is the data being used?*) and 3) form (*what sorts of data?*):

13 *For example, several media reported that Germany's Federal Criminal Police Office (BKA) is using a Trojan virus as a tool to access data of suspected individuals on their smartphones before the information becomes encrypted by apps such as Telegram and WhatsApp (Burack, 2018).*

1. Users (*who*): While studies show that big data promise great positive usability for improving the quality of citizens' lives (Pereira et al., 2017), there is a difference if such data is analysed by an LEA or an agency whose task does not include potential prosecution. Actors operating with data generated for and/or by SCTS can be divided into three groups: the civil sphere (developers and maintainers of SCTS); the plural policing sphere (municipality wardens, private security); and the LEA sphere (police, certain intelligence agencies etc.). Of course, a certain liaison line can be established between them, e.g. when electricity suppliers use smart grids to monitor the residents' electricity consumption and then report anomalies to the LEA. Depending on the protocol that dictates how to screen the grid for such anomalies and how (under which level of suspicion should the electricity supplier report/alert the LEA or how often), the risk for privacy violations can also be diverse.
2. Purposes (*why*). Considering the above-mentioned wide list of actors, the data may have a range of uses. While the civil sphere will use data generated by SCTS to maintain the smart city and its further development, the actors of plural policing can use data for maintaining public law and order, improving the quality of their services etc. Actors from the LEA could take advantage of the data for strategic criminal intelligence (crime prevention aims) or specific criminal investigative purposes (investigation of a particular crime and prosecution of a certain person(s)).
3. Form (*what sorts of data*): We have recognised three different sets of data, namely: 1) "raw" data from diagnostic logs of systems (runtime, auto diagnostic, system checks, system incidents diagnostics etc.) – this data does not hold strong individualisation and identification markers; 2) mass data from sensors (vehicle licence plates in a certain area, phone/tablet data used to communicate with a system etc.) – data is individualised yet additional data is needed to properly identify a subject (e.g. you need access to the database of vehicle registration information to identify a vehicle's owner, but you still do not know who actually drove that vehicle to that location at that time); and 3) strongly individualised data (biometric data, data from fingerprint locks, photographs and other visual data etc.). All three data categories demand different sharing rights and safeguards. For instance, data from the first category are not a threat to privacy since they are not connected to persons or individuals and can thus be undisputedly used by SCTS developers and maintenance teams in their daily work, while the same data could be provided to the LEA, but only in connection with a specific investigation or for crime-prevention measures (here special contracts between data providers and LEAs must be established in advance and detail how data must be protected and how it may be used). Data from the second and third categories should be provided to the LEA only upon judicial demand. If the LEA is the one gathering data, a special access protocol must be developed that tracks who, when and why the

data was accessed. Analysis of these data for other purposes is possible as well, but they must be anonymised to exempt them from personal data confidentiality and privacy related restrictions.

A mix of the aforementioned narratives (who, why and what) influences the emergence of different levels of risk for privacy violations. It may be considered that the risk of privacy violations is low if SCTS maintenance teams use depersonalised diagnostic data logs. In contrast, with strongly individualised data, for instance CCTV recordings used by LEA to monitor person(s) behaviours, the risk for privacy violations can be high (for a similar discussion, see van Zoonen, 2016). Ensuring the proper security and management of the data used and/or generated by smart city systems is therefore essential (Talari et al., 2017), which is why information and cyber security and defence, together with proper compliance and usage monitoring represent crucial safeguards. Numerous standards pertain to smart cities or their component parts and can help governments, cities or developers address various issues. While standards such as UNE 178301:2015, PNE 178106, PNE 178306, PNE 178501, PAS 182 and 183 etc. assure the proper development of smart city infrastructure, SCTS and data management, more comprehensive models and standards are also available and useful for managing and planning smart cities' development, such as PAS 181, PD 8101 ISO/TS 37151:2015, ISO 37120:2014, ISO/DIS 37101, ISO/DTR 37121, ISO/NP 37122, ISO/WD 37120. Further, standards like ISO/IEC 27001: 2013, ISO/IEC 27002: 2013 or IEC 62443 are also very important by including guidelines and measures for the proper development of information and cyber security. Guidelines and legislative frameworks that would more holistically address SCTS and the data deriving from them are still being developed and so we can expect the emergence of new regulations that will concretise access to and sharing of data with LEA alongside precise definitions of who can have access to which dataset, for which purposes and on which conditions.

4 DISCUSSION AND CONCLUSIONS

It is safe to assume that although SCTS raise great concerns over personal privacy, they will still be used in facilitating urban development. Their potentials for improving the quality of life, the economy and the environment are far too promising, which is why smart cities have become a solution framework recognised on the international level and an objective of many national strategies. When smart cities use systems and technology that do not track individuals, then such smart cities are far from the Orwellian dystopia with which they are so often associated. However, the line between citizen safety provision and citizen monitoring is indeed thin, but this should not discourage us from using such technology and instead encourage us to research and develop it further in the right way.

Smart security connected to the development of safe cities as sub-systems of smart cities is a trending topic in municipal development and governance plans. In this paper, we elaborated on the role of SCTS and their implications

for policing and criminal investigation/intelligence. We emphasised that the data generated by SCTS hold considerable potential for criminal intelligence and/or criminal investigations, yet access to this data should be properly regulated and safeguarded from unlawful LEA (and other agency) usage. In contrast, the products of criminal investigation, but even more so, criminal intelligence analysis could be used to recommend (or even co-develop) SCTS to tackle delinquency or other unwanted behaviour. This symbiosis can be an indicator of smart policing where big data plays a pivotal role in how policing is more effectively conducted.

There is, of course, also a danger that the data generated by SCTS is capitalised by smart city governance ("What truly makes a city intelligent is its capability to innovate and capitalize economically." (Joshi et al., 2016, p. 905)). Here big business, which is exploiting the data so amassed for commercial or even political purposes, is perhaps even a bigger threat to our privacy than police agencies, yet it is rarely seen as such (Galič, 2018; Kanduč, 2018; Završnik, 2018a, 2018b). Moreover, since the development of technologies and systems utilised by smart cities is sometimes made in a public-private partnership, often with private businesses safeguarding the intellectual property rights (Public-private partnerships for SMART city management, 2015), this raises additional concerns with regard to transparency, accountability and privacy.

Since privacy and information security are by far the most relevant issues in the development of smart cities, legitimacy must be considered a key quality of the technologies and solutions that are developed. Here, we must stress the role of people's perceptions of risks and benefits. Perceptions are typically a more crucial factor in adoption and the evaluation of the legitimacy of technologies than their actual design and functions. In practice, this means the pace of smart city development and smart policing depends on perceived risks rather than on their actual state (van Zoonen, 2016). Since the fearing of risks is often irrational, it seems reasonable to also address public opinion and support when promoting such development. For example, people are easily compelled to share their private data, yet are critical of new technologies proposed for LEA use. Steps to further improve the legitimacy of and trust in LEA and public approval of LEAs' use of data derived from ICT and SCTS should focus on improving transparency and promoting the benefits of such usage. Greater transparency could be achieved through better communication about safeguards – citizens must know how data is gathered and used, while the mechanisms the state applies to discover the unlawful behaviour of LEAs (and other agencies) must be promoted, as well as the prosecution of such behaviour. Research by Fujs and Markelj (2018) also shows that public knowledge about smart cities is relatively low and people are concerned with their lack of the technical skills needed to understand and properly use new technologies. That is why publicly-oriented awareness and education programmes must encompass smart city development. At the same time, private entities that provide services that accumulate user data must be compelled to uphold standards and protocols. Periodical political, scientific, non-governmental etc. inquiry into these private entities' behaviour and use of data derived from SCTS should be encouraged and promoted. Clearly, further research into the public perceptions of LEAs' role in the smart city ecosystem is needed. When

discussing possible negative implications of the digitisation and datafication of the city's functions, unease is of course not unreasonable because SCTS generate unprecedented amounts of data that may be used in a variety of ways. They can be exploited by LEAs, private businesses and criminals. Considering that smart cities are the future direction of urban development, it is vital to address the issues concerned with privacy and the development of regulation accordingly. This includes providing proper legislation, guidelines and recommendations or implementing those already developed (Galdon-Clavell, 2013). Proper research must be conducted that dissects the impacts of smart technology, privacy concerns and future development in these spheres (Meijer & Thaens, 2018).[14]

Moreover, we should also encourage setting up some form of watchdog institution/s to safeguard citizen privacy rights and simultaneously monitor the behaviour of governments and businesses. The key question here is whether the current mechanisms and already established institutions (e.g. Information Commissioner) are sufficient for monitoring and preventing privacy violations that are set to become more complex and widespread as smart cities and SCTS develop. In this regard, further discussions and system reviews are needed to clarify whether we need agencies, institutions and watchdogs that would focus exclusively on monitoring the compliance of safe city operations and smart city management, developing regulations and exercising control over advances and the use of SCTS.

At the end of our discussion, there is one other important aspect we need to highlight. In all areas related to the topic of this paper, for example, research and education, public and private sector, there is a growing need for properly educated and competent personnel to deal with smart technologies and related issues. Here students from faculties that provide a combination of ICT knowledge and public administration/governance knowledge would be best qualified. While some countries still perhaps need to develop such study programmes, in Slovenia the Information Security study programme at the Faculty of Criminal Justice and Security of the University of Maribor already produces such a skillset. Further, since students taking this programme also receive knowledge relating to criminal investigation, they are properly equipped to be either users of data produced by smart city technologies (e.g. in the role of criminal investigator or criminal intelligence analyst) or to safeguard against potential privacy intrusion (e.g. if they are in the role of a smart city technology developer or working for a city administration planning to incorporate such technology). In the future, police professionals with insights into ICT as well as criminal investigative know-how will be most appropriately equipped for investigating crimes as their cognitive and critical investigative thinking skills will need to include focusing on the possibilities of data created by ICT or SCTS.

The outcome of this paper calls attention to the knowledge-based approach to managing smart cities. The future success of urban development depends on the awareness, integrity and flexibility of all stakeholders involved. The evolution and transformations of urban life require societies' culture and climate to adapt

14 *We also agree with Baig et al. (2017) that extensive research and developmental focus should be given to the tools and methods of digital forensics that can be used in the IoT, ICT and smart cities.*

to the changes as well. The open-mindedness of citizens and receptiveness of political and governing bodies will play a significant role in the adoption of further innovations. Given market reports and trend predictions (e.g. Deloitte, 2015), the skills and competencies of those responsible will be a major challenge in the provision of effective smart city governance. Recent security incidents around the world (natural disasters, terrorist attacks, mass casualties, use of means of mass destruction, AMOK situations, extortions, organised criminal activities) clearly show the threat landscape is also transforming, while global threats are manifesting in local communities and no society is immune. As a result, security authorities face new situations and risks and often lack specific experience and competencies. Together with the technological development of societies, this problem is only intensifying. The increased complexity of urban communities requires a consideration of professionalising the management of urban safety and security. Thus, challenges relating to the management of urban problems sparked a discussion on the urban security management system. In this relation, the European URBIS project, featuring the Faculty of Criminal Justice and Security as a partner, was carried out to study the professionalisation of urban security managers' role. The essential idea was that the contemporary security environment requires a professional in the community who can meet the whole range of expected challenges. The project reasoned that urban security managers, as coordinators, must possess the skills and knowledge to analyse situations and coordinate a response, enabling them to cooperate successfully with state and local authorities and security provision institutions and organisations, as well as with the general public/society (Meško, Tominc, & Sotlar, 2013). The correlations of smart cities with such observations, by either playing the role of incentives and contributors to problems or as a solution to those problems, is more than evident.

REFERENCES

Abel, W. (2009). Agents, trojans and tags: The next generation of investigators. *International Review of Law, Computers & Technology*, *23*(1–2), 99–108.

Allied Market Research. (2018). *Physical security market by type (system and services), industry vertical (BFSI, commercial, government, residential and transportation) – Global opportunity analysis and industry forecast, 2017–2023*. Retrieved from https://www.alliedmarketresearch.com/physical-security-market

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M. … Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, *22*, 3–13.

Berst, J., & Logsdon, D. (October 17, 2016). *The hill: At smart cities week, tackling opportunities and challenges*. Retrieved from https://smartcitiescouncil.com/article/hill-smart-cities-week-tackling-opportunities-and-challenges

Boels, D., & Verhage, A. (2016). Plural policing: A state-of-the-art review. *Policing: An International Journal of Police Strategies & Management*, *39*(1), 2–18.

Braga, A. A. (2014). Problem-oriented policing. In G. Bruinsma, & D. Weisburd (Eds.), *Encyclopedia of criminology and criminal justice* (pp. 3989–4000). New York: Springer.

Bryant, R. P. (2010). Theories of criminal investigation. In S. Tong, R. P. Bryant, & M. A. H. Horvath (Eds.), *Understanding criminal investigation* (pp. 13–33). Oxford: Wiley-Blackwell.

Burack, C. (January 27, 2018). German federal police use Trojan virus to evade phone encryption. *Deutsche Welle*. Retreived from https://www.dw.com/en/german-federal-police-use-trojan-virus-to-evade-phone-encryption/a-42328466

Chokshi, N. (May 25, 2018). *Is Alexa listening? Amazon echo sent out recording of couple's conversation*. Retrieved from https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html

CISCO. (n. d.). *What is a smart city?* Retrieved from https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/what-is-a-smart-city.html

Deloitte. (2015). *Smart cities – How rapid advances in technology are reshaping our economy and society* (Version 1.0). The Netherlans: Deloitte. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/public-sector/deloitte-nl-ps-smart-cities-report.pdf

Douglas, T. (January 23, 2018). *Chicago police cut crime with major upgrades to analytics and field technology*. Retrieved from http://www.govtech.com/public-safety/Chicago-Police-Cut-Crime-with-Major-Upgrades-to-Analytics-and-Field-Technology.html

Dvoršek, A. (2008). *Kriminalistična metodika* [Criminal investigative methods]. Ljubljana: Fakulteta za varnostne vede.

Eremia, M., Toma, L., & Sanduleac, M. (2017). The smart city concept in the 21st century. *Procedia Engineering*, *181*, 12–19.

European Commission. (2015). *A European agenda on security (COM/2015/185/FINAL).* Retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

European Commission. (April 6, 2016). *Security: EU strengthens response to hybrid threats*. Retrieved from http://europa.eu/rapid/press-release_IP-16-1227_sl.htm

European Commission. (n. d. a). *Smart cities*. Retrieved from https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en#what-are-smart-cities

European Commission. (n. d. b). *Urban development*. Retrieved from http://ec.europa.eu/regional_policy/en/policy/themes/urban-development/

FICCI-E&Y. (2015). *S.M.A.R.T. policing for smart cities*. Retrieved from http://ficci.in/spdocument/20615/FICCI-Report-SMART-Policing-for-Smart-Cities.pdf

Fujs, D., & Markelj, B. (2018). Privacy in smart cities or privacy for smart people? *Varstvoslovje*, *20*(1), 5–24.

Galdon-Clavell, G. (2013). (Not so) smart cities? The drivers, impact and risks of surveillance-enabled smart environments. *Science and Public Policy*, *40*(6), 717–723.

Galič, M. (2018). Živeči laboratoriji in veliko podatkovje v praksi: Stratumseind 2.0 – razprava o živečem laboratoriju na Nizozemskem [Living laboratories and Big Data in practice: Stratumseind 2.0 – debate on a living lab in the Neth-

erlands]. In A. Završnik, & L. Selinšek (Eds.), *Pravo in nadzor v dobi velikega podatkovja* (pp. 85–110). Ljubljana: Pravna fakulteta: Inštitut za kriminologijo pri Pravni fakulteti.

Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanović, N., & Meijers, E. (2007). *Smart cities – ranking of European medium-sized cities*. Vienna: Centre of Regional Science.

Glaser, B. G., & Strauss, A. L. (2009). *The discovery of grounded theory: Strategies for qualitative research*. New Brunswick: Aldine.

Gottschalk, P. (2010). *Policing organized crime: Intelligence strategy implementation*. Boca Raton: CRC Press.

Grand View Research. (2018). *Physical security market worth $290.7 billion by 2025: CAGR: 9.1%*. Retrieved from https://www.grandviewresearch.com/press-release/global-physical-security-market

Hess, K. M., & Orthmann, C. M. H. (2010). *Criminal investigation*. Clifton Park: Delmar, Cengage Learning.

Joshi, S., Saxena, S., Godbole, T., & Shreya. (2016). Developing smart cities: An integrated framework. *Procedia Computer Science*, *93*, 902–909.

Kanduč, Z. (2018). Stroji, podatki, ljudje, kontrola in kapitalizem [Machines, data, people, control and capitalism]. In A. Završnik, & L. Selinšek (Eds.), *Pravo in nadzor v dobi velikega podatkovja* (pp. 133–166). Ljubljana: Pravna fakulteta: Inštitut za kriminologijo pri Pravni fakulteti.

Khalid, M. A., Babar, M. I. K., Zafar, M. H., & Zuhairi, M. F. (2013). Gunshot detection and localization using sensor networks. In *2013 IEEE International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA)* (pp. 1–6). Kuala Lumpur: IEEE.

Komninos, N. (2008). *Intelligent cities and globalisation of innovation networks*. London: Routledge.

Lacinák, M., & Ristvej. J. (2017). Smart city, safety and security. *Procedia Engineering, 192*, 522–527. doi:10.1016/j.proeng.2017.06.090

Larson, C. (August 20, 2018). Who needs democracy when you have data? *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/

Leydesdorff, L., & Deakin, M. (2011). The triple-helix model of smart cities: A neo-evolutionary perspective. *Journal of Urban Technology*, *18*(2), 53–63.

Maver, D. et al. (2004). *Kriminalistika: Uvod, taktika, tehnika* [Criminal investigation: Introduction, tactics, techniques]. Ljubljana: Uradni list Republike Slovenije.

Meijer, A., & Thaens, M. (2018). Quantified street: Smart governance of urban safety. *Information Polity*, *23*(1), 29–41.

Meško, G., Tominc, B., & Sotlar, A. (2013). Urban security management in the capitals of the former Yugoslav republics. *European Journal of Criminology*, *10*(3), 284–296.

Modic, M., Lobnikar, B., & Dvojmoč, M. (2014). Policijska dejavnost v Sloveniji: Analiza procesov transformacije, pluralizacije in privatizacije [Policing in Slovenia: An analysis of the processes of transformation, pluralization, and privatization]. *Varstvoslovje*, *16*(3), 217–241.

Mohammadi, M., & Al-Fuqaha, A. (2018). Enabling cognitive smart cities using big data and machine learning: Approaches and challenges. *IEEE Communications Magazine*, *56*(2), 94–101.

Mohanty, S. P., Choppali, U., & Kougianos, E. (2016). Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE Consumer Electronics Magazine*, *5*(3), 60–70.

Newburn, T. (2007). Understanding investigation. In T. Newburn, T. Williamson, & A. Wright (Eds.), *Handbook of criminal investigation* (pp. 1–10). Cullompton; Portland: Willan.

Orr, D. A., & Sanchez, L. (2018). Alexa, did you get that? Determining the evidentiary value of data stored by the Amazon® Echo. *Digital Investigation*, *24*, 72–78.

Palmiotto, M. J. (2013). *Criminal investigation*. Boca Raton: CRC Press.

Pereira, G. V., Macadar, M. A., Luciano, E. M., & Testa, M. G. (2017). Delivering public value through open government data initiatives in a Smart City context. *Information Systems Frontiers*, *19*(2), 213–229.

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. Santa Monica: RAND Corporation.

Peterson, M. (2005). *Intelligence-led policing: The new intelligence architecture.* Washington: US Department of Justice, Office of Justice Programs. Retrieved from https://www.ncjrs.gov/pdffiles1/bja/210681.pdf

Pillaipakkam, P. (2017). Data powers next-gen applications. In *Smart cities & utilities report: 2018 Black & Veach Strategic Directions* (pp. 33–36). Black & Veach. Retrieved from https://www.bv.com/sites/default/files/gated-content/strategic-directions-report/18-SDR-Smart-Cities-Utilities.pdf

Powell, A. (2014). 'Datafication', transparency, and good governance of the data city. In K. O'Hara, M.-H. C. Nguyen, & H. Peter (Eds.), *Digital enlightenment yearbook 2014: Social networks and social machines, surveillance and empowerment* (pp. 215–224). Amsterdam: IOS Press.

Public-private partnerships for SMART city management: Recommendations for local governments to prepare and implement SMART PPPs. (2015). Uraía Platform, UN-Habitat, & FMDV. Retrieved from www.uraia.org/documents/46/oct-2015-uraia-smart-ppp-eng_1.pdf

Ramaprasad, A., Sánchez-Ortiz, A., & Syn, T. (2017). A unified definition of a smart city. In M. Janssen, K. Axelsson, O. Glassey, B. Klievink, R. Krimmer, I. Lindgren … D. Trutnev (Eds.), *Electronic government* (pp. 13–24). Cham: Springer.

Ratcliffe, J. (2008). *Intelligence-led policing*. Cullompton: Willan.

Regulation (EU) 2016/679 of The European Parliament and of The Council. (2016). *Official Journal of the European Union,* (L 119/1).

Rich, S. (August 19, 2011). *Predictive policing project reduces crime in Santa Cruz, Calif.* Retrieved from http://www.govtech.com/public-safety/Predictive-Policing-Project-Reduces-Crime-Santa-Cruz-Calif.html

SeaSkate. (1998). *Evolution and development of police technology*. Washington: SeaSkate. Retrieved from http://www.ncjrs.gov/pdffiles1/Digitization/173179NCJRS.pdf

Sotlar, A. (2015). Reševanje varnostnih problemov – med nacionalno, lokalno in človekovo varnostjo [Resolving safety problems – between national security, local security and the safety of individuals]. In G. Meško (Ed.), *Varnost v lokalnih skupnostih zbornik prispevkov Prve nacionalne konference o varnosti v lokalnih skupnostih, Ljubljana, 27. november 2015* (pp. 26–33). Ljubljana: Fakulteta za varnostne vede.

Spencer, S. B. (2017). Predictive surveillance and the threat to fourth amendment jurisprudence. *Journal of Law and Policy for the Information Society, 14.1,* 109–149.

Stratistics Market Research Consulting. (2017). *Home security solutions – global market outlook (2016–2022)*. Retrieved from https://www.strategymrc.com/report/home-security-solutions-market-2016

Talari, S., Shafie-khah, M., Siano, P., Loia, V., Tommasetti, A., & Catalão, J. (2017). A review of smart cities based on the internet of things concept. *Energies*, *10*(4), 421–444.

The British Standards Institution. (2014). *Smart cities – vocabulary*. Retrieved from http://shop.bsigroup.com/upload/PASs/Free-Download/PAS180.pdf

The Economist Intelligence Unit. (2017). *The safe cities index 2017*. Retrieved from https://dkf1ato8y5dsg.cloudfront.net/uploads/5/82/safe-cities-index-eng-web.pdf

The European Network of Living Labs (ENoLL). (n. d.). Retrieved from https://enoll.org

United Nations. (May 16, 2018). *2018 revision of world urbanization prospects.* Retrieved from https://www.un.org/development/desa/publications/2018-revision-of-world-urbanization-prospects.html

Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472–480.

Willis, J. J. (2014). A recent history of the police. In M. D. Reisig, & R. J. Kane (Eds.), *The Oxford handbook of police and policing* (pp. 3–33). Oxford: Oxford University Press.

Završnik, A. (2018a). Algokracija: Od vladavine prava do vladavine algoritmov [Algocracy: From the rule of law to the rule of algorithms]. In A. Završnik, & L. Selinšek (Eds.), *Pravo in nadzor v dobi velikega podatkovja* (pp. 35–83). Ljubljana: Pravna fakulteta: Inštitut za kriminologijo pri Pravni fakulteti.

Završnik, A. (2018b). Big data: What is it and why does it matter for crime and social control? In A. Završnik (Ed.), *Big data, crime and social control* (pp. 3–28). London; New York: Routledge, Taylor & Francis Group.

About the Authors:

Kaja Prislan, PhD, Assistant Professor at the Faculty of Criminal Justice and Security, University of Maribor. E-mail: kaja.prislan@fvv.uni-mb.si

Boštjan Slak, Assistant at the Faculty of Criminal Justice and Security, University of Maribor. E-mail: bostjan.slak@fvv.uni-mb.si

VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 20 no. 4 pp. 414–433

The Impact of the EU General Data Protection Regulation (GDPR) on Mobile Devices

Domen Hribar, Miha Dvojmoč, Blaž Markelj

Purpose:

The purpose of this paper is to examine novelties introduced by the European Regulation (2016/679) on the Protection of Natural Persons with Regard to the Processing of Personal Data (GDPR) and its key impacts on mobile device users. The paper also presents some of the main changes affecting both natural persons and legal entities. Further, certain issues that might occur while implementing the Regulation are raised together with the degree of individuals' awareness of the need to protect the personal data stored on their mobile devices.

Design/Methods/Approach:

For the purpose of this paper, we reviewed the legislation, Slovenian and international literature, brochures and media stories in the field of personal data protection. We also used a questionnaire to determine the degree of awareness of the importance of protecting personal data among the general population.

Findings:

The findings show that no revolutionary changes are introduced. Nevertheless, quite a few novelties concern data controllers and processors. In particular, penalties for breaching the GDPR are now much higher. Individuals' rights are strengthened and easier to control. In contrast, data controllers and processors are subject to more stringent duties and legal obligations. These changes also apply to mobile device users. The research findings show that individuals are relatively well aware of the concept of personal data; however, the scope of their knowledge shrinks as this concept becomes increasingly complex. Familiarity with the new Regulation (2016/679) having been introduced at the EU level was claimed by 55% of the respondents (N = 195).

Research Limitations/Implications:

The limitations stem from the selective choice of the GDPR's impact on mobile device users. More important influences are emphasised.

Originality/Value:

The findings will help both individuals and legal entities understand the changes brought to the area of data protection and tackle them more successfully.

UDC: 004.056:[342.7:621.391]

Keywords: personal data protection, GDPR, Personal Data Protection Act, mobile devices

Vpliv evropske Splošne uredbe o varstvu osebnih podatkov (GDPR) na mobilne naprave

Namen prispevka:

V prispevku smo predstavili ključni vpliv evropske uredbe (2016/679) o varstvu posameznikov pri obdelavi osebnih podatkov na uporabnike mobilnih naprav. Poleg vpliva smo predstavili ključne spremembe, ki vplivajo tako na fizične kot tudi na velik delež pravnih oseb. Poudarili smo določeno problematiko, s katero se organizacije srečujejo. Hkrati smo prikazali stanje ozaveščenosti ljudi o varstvu osebnih podatkov na mobilnih napravah.

Metode:

Prispevek temelji na pregledu zakonodaje ter domače in tuje literature, brošur in medijskih člankov na področju varstva osebnih podatkov. Izvedli smo tudi anketo, kjer nas je zanimala ozaveščenost o pomembnosti varstva osebnih podatkov.

Ugotovitve:

Na področju je prišlo do številnih novosti, ki so spremenile način upravljanja in obdelave. Predvsem se bodo povečale globe za kršitelje. Pravice posameznika bodo podkrepljene in lažje nadzorovane. Po drugi strani bodo upravljavci in obdelovalci dobili veliko novih dolžnosti. Spremembe veljajo tudi za uporabnike mobilnih naprav. Ugotovitve raziskave so pokazale, da ljudje sorazmerno dobro poznajo pojem osebni podatek, vendar se to znanje s kompleksnostjo pojma zmanjšuje. Udeleženci so v 55 % (N = 195) odgovorili, da vedo za prihod nove uredbe (2016/679).

Omejitve/uporabnost raziskave:

Omejitve so pri selektivni izbiri vpliva uredbe na uporabnike mobilnih naprav. Poudarjeni so pomembnejši vplivi.

Izvirnost/pomembnost prispevka:

Ugotovitve prispevka bodo pomagale tako posameznikom kot tudi organizacijam pri dojemanju sprememb in zato lažjem spoprijemanju z njimi.

UDK: 004.056:[342.7:621.391]

Ključne besede: varstvo osebnih podatkov, GDPR, Zakon o varstvu osebnih podatkov, mobilne naprave

1 INTRODUCTION

The present paper focuses on mobile devices and the way in which the new personal data protection legislation affects their use. This field is extremely broad and complex, which is why the paper only concentrates on certain more significant changes. Mobile devices are placed at the forefront simply because we can hardly envisage our everyday lives without them. Further, mobile devices can hold personal data that must be protected under the GDPR. If the device is

lost or stolen that constitutes a data breach. While data breaches are common, they are easier with mobile devices. This example shows that mobile devices are a weak link while trying to comply with the GDPR. Mobile devices include, among others, devices with a built-in adapted operating system. They also encompass devices able to transfer data and access the Internet wirelessly (Markelj & Bernik, 2016). Mobile device use is extremely widespread across the globe (GSMA Intelligence, 2018). The available figures are extremely high and refer to the quantity of data transferred at the global level. The need to protect such data is therefore in the interest of anyone conducting any transaction that involves any type of information.

Naturally, not all pieces of information are equally important. The value of a piece of information depends on numerous factors linked to one another, thus creating or increasing the value of information. That is why the State recognises, inter alia, that information related to individuals is a fundamental element in guaranteeing human rights and freedoms. This type of information is known as personal data and denotes "any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [GDPR], 2016, Article 4). Personal data thus includes a great deal of information regarding an individual. After all, the colour of one's hair also constitutes personal data. It is also important to distinguish between protected and unprotected personal data. The 'identifiability' of natural persons plays a considerable role in making this distinction (Bolognini & Bistolfi, 2016). Information regarding natural persons not falling in the scope of the definition of personal data and, in particular, not meeting the identifiability condition does not belong to the category of protected personal data (Article 29 Data Protection Working Party, 2007). The mentioned Regulation does not apply to such information. Therefore, the Regulation only applies to information that meets the criteria listed in the personal data definition, especially the identifiability condition. With respect to identifiability, the question of who determines whether a person can be distinguished from all other individuals is crucial. Above all, the concept of identifiability must be considered in the broadest possible sense and not merely on the basis of one's own capabilities (Informacijski pooblaščenec, 2017a). The rules enshrined in the GDPR therefore apply to clearly defined cases. For instance, these rules do not need to be followed where a natural person keeps a database containing personal data for their own use. On the other hand, natural persons are not allowed to process certain types of personal data that are prescribed in other legal acts.

Mobile devices and the data stored on them are crucial for our everyday lives. The fact such data may fall into the hands of unauthorised persons is

therefore highly undesirable. The loss or unauthorised processing of any data, both conventional information as well as data stored on any information and communications technology devices (henceforth: ICT devices), is extremely unpleasant. This is particularly problematic when considering the use of ICT devices where data protection issues are even more complex. Mobile devices are exposed to various, unique risks. For instance, a mobile device is easy to lose, which potentially jeopardises all the data stored on it. Apart from external risks, individuals also tend to transfer large quantities of data whose origin, reliability and security are unknown (Hettrich, 2015). For instance, we all use various applications that are downloaded to our mobile devices, yet we are unaware or may not even care about the type of data being collected about us. Such applications often collect data they should not be collecting or may actually require less data for their normal functioning, meaning they are in full breach of the principle of minimisation (Pedro, 2016).

2 THE GDPR IN BRIEF

In April 2016, the European Parliament and the Council adopted the General Data Protection Regulation (GDPR, 2016) and the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences (Informacijski pooblaščenec, n. d.). Both legal acts pay considerable attention to the processing and management of personal data. This paper focuses merely on the GDPR, which entered into force in May 2018. The fact that technological development has brought numerous changes in the past few years was one of many arguments underpinning adoption of the GDPR. In fact, the cyber world is developing, changing and spreading extremely fast, thus demanding necessary amendments to the applicable legislation. Such legislative amendments must not restrict further development, but create an environment in which individuals are able to trust the already guaranteed human rights and simultaneously use modern technologies to freely conduct their business. The GDPR also increases the level of individuals' rights, thus serving the interests of the people. Personal data protection is extremely important for the protection of human rights and so must find its place among other fundamental rights in such a way that it will strike the right balance with other rights and freedoms.

Slovenia is in a somewhat better position than other countries, which are still dealing with a larger number of more complex issues. It must be stressed that the new GDPR contains standardised provisions for the entire territory of the European Union (EU). Hence, the level of personal data protection in countries, such as Malta, Poland and the Czech Republic, is lower than in Slovenia since they have been facing several unresolved issues already at the level of legislative discussions (Baker McKenzie, 2017). Article 38 of the Constitution of the Republic of Slovenia (Ustava Republike Slovenije, 1991) defines certain fundamental rights of individuals concerning the protection of personal data, e.g. the right to be informed of the fact that personal data related to individuals are being collected and the right to judicial protection). Personal data protection is also regulated

by the current Personal Data Protection Act (Zakon o varstvu osebnih podatkov [ZVOP-1-UPB1], 2004), which has many similarities with the new GDPR (yet also several inconsistencies, which raise the problems discussed in the conclusion of this paper). The GDPR also contains provisions on the protection of children, an area not regulated until now. Children constitute a vulnerable group which is unaware of the potential consequences of personal data collection and processing. As such, they are subject to extra protection in numerous articles of the GDPR (GDPR, 2016). For instance, the GDPR defines the age limit for acquiring a child's consent for personal data processing. Organisations therefore violate the law if they process personal data of children below the defined age limit without having first obtaining the consent of the holder of parental responsibility (Ministrstvo za pravosodje RS, 2017).

3 FUNDAMENTAL CHANGES

Even though some similarities between the current Personal Data Protection Act (ZVOP-1-UPB1, 2004) and the new GDPR may be observed, the latter introduces a series of fundamental changes. These impact the retention, processing and management of personal data, as well as the rights of individuals. Changes in the area of personal data protection can be divided into two distinct parts. The first encompasses the rights of individuals, while the second refers to data controllers and processors.

3.1 Changes Relating to the Rights of Individuals

- Greater control and a more effective exercise of control;
- Easier access to one's own personal data;
- The right to be forgotten;
- The right to information regarding the retention period of personal data;
- The right to data portability;
- The right to judicial protection and sanctions;
- Individuals must not be subjected to measures based solely on profiling, analyses or predictions obtained by the means of automated processing (Informacijski pooblaščenec, 2017b).

The right to be forgotten, which may be described as a novelty in the field of personal data protection, is merely an extension and a stronger version of the right of individuals who wish to withdraw their consent for the processing of personal data on the basis of a legal act. The right to erasure is defined in Article 32 of the Personal Data Protection Act (ZVOP-1-UPB1, 2004), albeit under a slightly different name. This field has now been altered so that it is easier for individuals to invoke their right to be forgotten and to implement their requests for erasure faster (GDPR, 2016). The same conclusion was reached by Mantelero (2013) who stated the right to be forgotten was not a revolutionary change in the current rules since Article 12 of Directive 95/46/CE (a predecessor of the GDPR) had already given a similar right. The changes thus mainly relate to the way in which this right can be invoked. The Personal Data Protection Act (ZVOP-1-UPB1, 2004) prescribes that individuals must prove that personal data were incomplete, inaccurate or

obtained unlawfully. On the other hand, the GDPR (2016) does not contain the same requirement. This new aspect may be a thorn in the side of organisations not only because they are now required to prove that the request for erasure was unjustified, but also due to the much higher fines the GDPR introduces. The impact of this change and some specific examples are presented in the following sections.

A similar situation occurs with the right to judicial protection and sanctions. Article 34 of the Personal Data Protection Act (ZVOP-1-UPB1, 2004) provides for the judicial protection of individuals' rights and the possibility of instituting administrative proceedings against certain decisions taken by data controllers. In this respect, the change refers to the fact that individuals now have to right to lodge a complaint without prejudice to any other administrative or legal remedy (GDPR, 2016). Individuals have thus obtained additional remedies for invoking their rights.

3.2 Changes Relating to Data Controllers and Processors

- Collecting personal data on the basis of consent – consent shall be provided in the form of a clear and plain language declaration and contain a clear affirmative action, which the processor must be able to demonstrate;
- The withdrawal of consent must be as easy as giving consent;
- Data controllers must consider the principles of data protection by design and by default;
- Data controllers must provide individuals with transparent and easily accessible information about the processing of their personal data;
- Obligatory notification of a personal data breach;
- Designation of a data protection officer;
- Records of processing activities;
- Prior impact assessments (Informacijski pooblaščenec, 2017b).

The applicable Slovenian law already contains a provision similar to that in indent four. Under Article 30 of the Personal Data Protection Act (ZVOP-1-UPB1, 2004), individuals have the right to be informed about the personal data relating to them. At the same time, they have the right to have their data erased if they are incomplete or inaccurate or were processed contrary to the ZVOP-1-UPB1 (2004). The novelty is that access to data is easier and simpler, with data having to be presented in an easily understandable manner. This will facilitate the operation of certain companies. If a company conducts business in several countries, the control over individual branches will be exercised by the headquarters. This will enable simpler and more consistent control operations. It will also lead to a decrease of administrative and other burdens (Voss, 2014), particularly because the GDPR applies to the entire EU territory.

4 MOBILE DEVICES AND THE GDPR

The GDPR's impact is also observed in mobile applications, particularly in relation to consent and the right to be forgotten. As mentioned, the GDPR (2016)

introduces specific conditions for giving consent to the processing of personal data. Consent must be given "in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language" (GDPR, 2016, Article 7). At the same time, the GDPR stipulates that it must be as easy to withdraw as to give consent. Some applications have already been updated in order to adjust to these conditions. This is mainly shown in the numerous requests for renewed consent. Data controllers were particularly busy with verifying the existing forms of consent (GDPR, 2016). On the other hand, this change does not pose any particular challenge for individuals but enables them to obtain information more easily and facilitates their decision on whether to continue using a specific application. This change also brings advantages for data controllers and processors since they have used this opportunity to obtain an overview of data previously collected by organisations. The approval for the processing of data has been strengthened with respect to children, who are a more vulnerable group that is presumably unaware of all potential risks arising from the sharing of personal data. According to the GDPR, children below a certain age must obtain the consent of a holder of parental responsibility to use certain applications, while such consent must not be conditional on excessive conditions set by the controller (Ministrstvo za pravosodje RS, 2017), which would prevent the child's participation in or use of an application. Social media use is a case in point. Another question here is how exactly the consent based on obtaining the parental agreement is verified (Tikkinen-Piri, Rohunen, & Markkula, 2018). Significant problems also relate to verifying the age limit. Therefore, it will be neither easy nor inexpensive for organisations to determine the actual age of users. The issue of consent might become even more complex upon the merging of different databases. The collection of certain types of data does not require individuals' consent since they are not considered personal data. However, after a given period or after databases are merged individuals may become identifiable, demanding direct application of the GDPR (2016).

Sullivan and Burger (2017) emphasise the spread of EU policy to other areas, particularly the fact EU wishes to expand its influence to third countries, thus creating a future data protection system at the international level. Users may be affected by the websites or mobile applications of providers not headquartered in the EU. Gilbert (2016) finds that the GDPR (2016) does affect companies without their headquarters in the EU when their services are used by individuals in the EU. One can thus presume that certain products or services are no longer present in the EU market or their presence has either dramatically decreased or being unlawfully provided.

Irrespective of the presence of services within or outside the EU, the new GDPR provides the clearer and more transparent processing of personal data, meaning that individuals may expect fewer unwanted advertisements, unsolicited calls and e-mails (DPOrganizer, n. d.). Data controllers will have to closely monitor how the right to erasure is being implemented as it may happen that certain information that ought to have been erased will remain in databases (Voss, 2017). For instance, "Moneysupermarket", an English company, sent 7.1 million e-mails to consumers who had previously stated they no longer wished

to receive e-mails from the company (Information Commissioner's Office, 2017). A fine of GBP 80,000 was imposed on the company. Eation (2017) claims that had the new GDPR been applicable at the time the company would have faced a fine of GBP 12.6 million for the same infringement. Apart from substantial fines, the mentioned author stresses the quality of the data, which are gradually becoming inaccurate. Users who use their mobile devices for business purposes must ensure their databases are up to date. The easiest way to achieve this is to enable remote access without the possibility of transferring personal data. In the future, remote access will become increasingly widespread. This will have a special impact on the migration of databases since data can become inaccurate quite quickly. However, if remote access is the only type of access to such databases, data controllers find it easier to update personal data, while the risk of abuse falls. Companies will mainly be obliged to check where and what type of data are stored on mobile devices, where (backup) copies of such data have been created and are being processed. Following an impact assessment, an additional level of security will have to be implemented. This is why the GDPR (2016) promotes the pseudonymisation of personal data. Additional issues relate to when smartphones used for both private and professional purposes are lost. This is acutely problematic when devices contain personal data. In this case, employees are obliged to inform their employers about the misappropriation, unauthorised access to or loss of data (Sire, n. d.). In order to avoid fines or inconvenience caused to their clients, employers are advised to erase the data remotely (Ledino, 2012). These options are regularly used in everyday practice.

Voss (2017) also notes that Article 34 of the GDPR obliges data controllers to inform individuals of a personal data breach when that breach is likely to result in a high risk to the rights and freedoms of private individuals. In terms of mobile applications, it is likely the individuals informed of such a breach will lose their trust and stop using the application. De Hert and Papakonstantinou (2016) contend such notifications would be extremely rare. They believe the relevant provisions obliging that individuals be informed of data protection breaches are quite vague since they allow a great deal of leeway for data controllers to avoid such communications.

Ducato (2016) stresses that some changes may also arise in relation to cloud computing. She finds that the environment surrounding cloud computing might become more complex, especially because of transparency and accountability obligations. Both data recipients and data controllers were forced to introduce certain changes. For instance, companies conducting business transactions via mobile devices and simultaneously storing the data in a cloud are a case in point. Personal data entered into the device and stored in the cloud pose a challenge to data controllers, particularly in terms of the device's security. Companies will have to conduct an impact assessment to determine whether additional security features are needed to guarantee the required level of protection (GDPR, 2016). If the data are to be uploaded and stored directly in the cloud, individuals will have to be informed about the location of data storage. If devices are used for both private and professional purposes, individual files must be protected through additional means and unauthorised access to personal data by third parties

prevented. Even though the Personal Data Protection Act (ZVOP-1-UPB1, 2004) already required this level of security, the new GDPR imposes much higher fines for infringements. Therefore, violation of the GDPR may result in a maximum fine of EUR 20 million or 4% of the total worldwide annual turnover for the preceding financial year (GDPR, 2016). High fines will thus 'encourage' data controllers to handle personal data much more cautiously.

5 RESEARCH RESULTS

The research study presented here relied on a questionnaire available via the *www.1ka.com* online application. Respondents could provide answers between 9 January 2018 and 10 March 2018. A total of 246 questionnaires was partially completed. Not all respondents provided answers to all questions, which is why the N figure for individual answers varies and is presented below the respective results.

Table 1: Overview of answers related to the concept of personal data

Answer	No. of answers	*N* (%)
1 (No, I have never heard of that)	0	0%
2 (It sounds familiar)	29	12%
3 (I have heard about it)	21	9%
4 (I know what personal data are)	195	79%
Total	*N* = 245	100%

Table 1 shows the respondents' perception of the concept of personal data. The question was answered by 245 respondents. All respondents claim to be familiar with the 'personal data' concept in one way or another. No one indicated being unfamiliar with this concept. In fact, the overwhelming majority of respondents (79%) stated they knew the exact meaning of the concept of personal data.

Table 2: Overview of answers related to personal data

	YES	NO	Not sure	*N* (%)
Tax identification no.?	196	6	1	203
	97%	3%	0%	100%
Height?	90	94	15	199
	45%	47%	8%	100%
Name and surname?	181	15	4	200
	91%	8%	2%	100%
Facial image?	147	33	17	197
	75%	17%	9%	100%
DNA?	186	6	9	201
	93%	3%	4%	100%
Today's weather?	1	187	7	195
	1%	96%	4%	100%

	YES	NO	Not sure	*N* (%)
Fingerprints?	190	6	5	201
	95%	3%	2%	100%
Username for an online forum?	84	87	26	197
	43%	44%	13%	100%
No. of inhabitants in a country?	2	188	5	195
	1%	96%	3%	100%
Dental X-ray image?	155	29	13	197
	79%	15%	7%	100%
Religious belief together with eye colour and the status of a city councillor (in Ljubljana)?	89	76	33	198
	45%	38%	17%	100%

Table 2: Continuation

Table 2 shows answers to the question of whether the specific information described above constitute personal data. The differences in the number of answers are relatively small. The biggest difference amounts to 8 answers, which is negligible given the highest number of answers, i.e. 203. The responses show that all data with the exception of "today's weather" and the "number of inhabitants in a country" constitute personal data. A large majority of respondents (90%) thus recognised the two types of data that are not considered personal data and marked them accordingly. The name and surname category actually consists of two separate items of personal data since any information related to an identified individual is considered personal data. This category should therefore be split into two parts. The majority of respondents, i.e. more than 90%, provided correct answers to the more unambiguous questions such as "tax identification number", "name and surname", "DNA" and "fingerprints". They were slightly more hesitant with "dental X-ray image" and "facial image", however, three-quarters or more of the respondents answered correctly. Respondents' opinions diverged more with respect to an individual's "height", "username for an online forum" and "religious belief together with eye colour and the status of a city councillor (in Ljubljana)". All three categories attracted the highest number of "not sure" answers. At the same time, respondents' opinions on whether this type of information constitutes personal data seem to be split. Most respondents gave correct answers with respect to the last category, yet this question also had the biggest share (17%) of "not sure".

	YES	NO	*N* (%)
Personal identification no.	152	48	200
	76%	24%	100%
Information on sexual orientation	142	57	199
	71%	29%	100%
Vehicle registration plate details	60	136	196
	31%	69%	100%

Table 3: Overview of answers regarding special categories of personal data

Table 3: Continuation

	YES	NO	*N* (%)
Tax identification no.	148	52	200
	74%	26%	100%
Year of birth	83	114	197
	42%	58%	100%
Political opinion	105	89	194
	54%	46%	100%

Table 3 presents answers concerning certain types of sensitive personal data now, i.e. after the entry into force of the new GDPR, referred to as special categories of personal data. Again, the difference in answers is relatively small, whereas the largest difference is six answers. Among the listed personal data types, only "information about sexual orientation" and "political opinion" are considered special categories of personal data, while the remaining data types are classified as conventional personal data. With respect to sexual orientation, 71% of the respondents answered correctly while 54% of them gave correct answers for political opinion. Interestingly, 42% of the respondents believe that year of birth falls in the special category of personal data.

Table 4: Overview of answers regarding the question of risks to security

Unlikely	Less likely	Neither likely nor unlikely	Likely	Highly likely	Total: [*N*]
0	31	40	92	32	195
0%	16%	21%	47%	16%	100%

Table 4 shows whether the abuse of personal data may result in a serious risk to individuals' security. The question itself was not specified in any further detail, leaving the interpretation up to individual respondents. Almost 50% of the respondents believe the abuse of personal data would likely lead to a serious risk with regard to individuals' security. All 195 respondents agree that such events are likely to some degree.

Table 5: Overview of answers regarding the collection of personal data

	1 – I do not know	2	3	4	5 – I know very well	Total
Who collects your personal data?	12	31	85	53	17	198
	6%	16%	43%	27%	9%	100%
Which personal data are collected?	9	27	75	57	17	195
	5%	14%	38%	28%	9%	100%
What is the purpose of the data collection and processing?	15	51	58	54	17	194
	8%	26%	30%	28%	9%	100%
What is the extent of the data collection?	17	51	76	37	13	194
	9%	26%	39%	19%	7%	100%
Can your data can be transferred to a third party?	22	31	65	48	28	194
	11%	16%	39%	25%	14%	100%

Table 5 shows how well the respondents are informed of the above elements when downloading mobile applications to their mobile devices. We were particularly interested in whether they knew who collected their personal data, which personal data were collected, what was the purpose of processing that data, what was the extent of the data being collected and whether their data could be transferred to a third party. Respondents were asked to provide their answers on a 5-point Likert scale. The table shows that the distribution of answers concentrates somewhat around average values. The opinions of the respondents were not extremely divergent, meaning they either did not know the answers to the above questions or knew them very well. Nevertheless, a slight tendency towards more affirmative responses, particularly with respect to "who collects your personal data", may be observed. The answers in Table 5 correspond to those shown in Table 6, which contains information regarding the respondents' awareness of the statements below. No two questions in the table actually appeared alongside each other in the questionnaire.

	I am aware	I am not aware	*N* %
Who collects your personal data?	124	70	194
	64%	36%	100%
Which personal data are collected?	130	66	196
	66%	34%	100%
What is the purpose of the data collection and processing?	105	89	194
	54%	46%	100%
What is the extent of the data collection?	73	119	192
	38%	62%	100%
Can your data be transferred to a third party?	122	68	190
	64%	36%	100%

Table 6: Overview of answers regarding the awareness of the collection of personal data

Tables 5 and 6 provide the same choice of possible answers, with the only difference being in the answers. In Table 6, respondents could answer by selecting "I am aware" or "I am not aware". The results show strong correlations with the answers in Table 5 for each question posed. When an answer in Table 5 lent towards "I don't know", the answer in Table 6 fell into the "I am not aware" category. For instance, with respect to the question "What is the extent of the data collection?", 62% of the respondents stated they were unaware of the extent of the data being collected, as presented in Table 6. Most respondents answered the same question by choosing answers closer to the "I don't know" category, as shown in Table 5. We were also interested in determining what respondents were willing to do to ensure additional protection of their mobile devices. The results are given in Table 7.

Table 7: Overview of answers regarding respondents' willingness to adopt additional measures

	I am not willing at all	I am not willing	I am neither willing nor unwilling	I am willing	I am absolutely willing	N %
Antivirus software	8	10	23	90	65	196
	4%	5%	12%	46%	33%	100%
Additional data encryption	2	20	36	89	45	192
	1%	10%	19%	46%	23%	100%
Education in the field of mobile device security	5	12	40	90	46	193
	3%	6%	21%	47%	24%	100%
Data archiving	4	13	48	94	34	193
	2%	7%	25%	49%	18%	100%
Adoption of best practices when using a mobile phone	2	6	28	104	53	193
	1%	3%	15%	54%	27%	100%

Table 7 shows the respondents' willingness to take extra measures to boost the security of their mobile devices. Differences between answers are relatively small, which does not affect the potentially different interpretation of the results. Respondents could choose between antivirus software, additional data encryption, education in the field of mobile devices' security, data archiving, and the following of best practices when using their mobile phones. The results show the respondents are relatively strongly inclined towards the "I am absolutely willing" option for all of the questions. They expressed the greatest willingness to use antivirus software solutions and adopt best practices, while the respondents were the least willing to use additional data encryption solutions.

Respondents were also asked what they would do if their personal data fell into the hands of unauthorised persons. We did not directly specify which type of data this would involve. Therefore, it was up to individual respondents to conceive a possible scenario. They could choose from several answers, including: "I would completely lose my trust in the organisation"; "I would file a lawsuit"; "Depends on the consequences"; "I would do absolutely nothing"; "I would not really care"; and "Other". The results show 43% of respondents stated they would lose their trust in the organisation, 38% said their reaction would depend on the consequences, and 17% stated they would file a lawsuit against the organisation. This question was answered by 195 respondents. We were also interested in

determining how many respondents were aware of the fact that the new GDPR, which would apply in all EU member states, was to enter into force in May 2018, with 107 out of these 195 respondents stating they were familiar with the upcoming regulation.

6 DISCUSSION

When examining the above results, one must first look at the situation as a whole. It is important to stress that the questionnaire aimed to measure the level of respondents' awareness of the personal data protection issue. The results show the respondents have a sufficient level of awareness and familiarity with this topic, at least as far as the basics are concerned. However, the greater the complexity of the issue, the greater the insecurity detected among the respondents. With respect to the first question, the vast majority of respondents stated they were familiar with the personal data concept. This was also demonstrated in the second question where they correctly selected "name and surname", "fingerprints", and other answers. When it came to "religious belief together with eye colour and the status of a city councillor (in Ljubljana)" and "username for an online forum", a large share of respondents either gave a wrong answer or was unsure of the answer. The fact is that any information related to an identifiable individual constitutes personal data. The phrase "any information" is key in this respect. As mentioned in the literature review, there is a difference between protected and unprotected personal data. A piece of information may constitute personal data, but it does not necessarily have to be protected according to applicable legislation. In this case, the issue of the identifiability of an individual must be considered since this is crucial for determining whether such personal data must be protected or not. Table 3 presents the respondents' answers on sensitive personal data (special categories of personal data) and clearly shows that most of them do not distinguish between conventional and special categories of personal data. Almost three-quarters of the respondents stated that their personal identification number belonged to the special category of personal data. Although it is true that the personal identification number reveals several items of personal data, it does not belong to the special category of personal data *per se* because it merely allows one to use it in order to access sensitive data. Nevertheless, the same argument could also be made for the combination of one's name, surname and address since these pieces of information may allow information related to individual's health records, criminal records and other data. Therefore, information revealing individuals' health condition falls into the special category of personal data, whereas the combination of those pieces of information related to an individual does not.

When asked whether the abuse of personal data could be a serious risk for individuals' personal safety and security, all respondents stated that some degree of likelihood does indeed exist. The notion that personal data abuse could result in a threat to personal safety and security is, among others, an indicator of awareness. This question did not contain any specific details about what type of abuse this would entail or which data would be affected. Respondents

were thus able to come up with their own scenarios. This question is directly linked to the question of data abuse where the respondents were again left to conceive various scenarios. Even though 38% of the respondents stating their reaction would depend on the consequences, this question was posed in such a way that presupposed a slight tendency towards a specific answer. Therefore, respondents had less freedom while answering it, mainly because the "I would lose my trust in the organisation" option appeared first on the list of possible answers and represented a relatively logical choice, which is why slightly less than 50% of respondents chose this answer. For a more realistic answer, we would have to either leave the interpretation up to individual respondents or define a very clear scenario entailing such an infringement. Tables 5 and 6 present a list of simpler concepts which were used to verify the accuracy or authenticity of the responses. The results show that respondents' answers correspond, thereby adding credibility to the research study.

The results presented in Table 7 show that most respondents are willing to make a considerable effort to protect their mobile devices. On the other hand, the findings of Bernik and Markelj (2014) paint an entirely different picture. In business spheres, the security of mobile devices is poor. This contradiction could be explained by presuming that while individuals may declare their willingness to improve the security of their devices, in practice they are less efficient when it comes to actually implementing security measures.

When the above findings are placed in the context of some of the most strongly emphasised issues and, indirectly, some of the most problematic areas, the following characteristics appear that should be considered when discussing or even providing personal data protection for mobile devices. Mobile devices have taken on the role of a mobile office used by individuals to carry out different tasks and achieve numerous purposes. As such, they are a challenge to and introduce extra dimensions in the sphere of personal data protection compared to other media that require due consideration. As mentioned, smart devices can impact the way individuals and organisations conduct their everyday tasks enormously. Applications facilitating, complementing or even replacing the current ways of conducting spare-time activities or work-related processes are being developed continuously.

The IT aspect of mobile device use enables or, in other words, requires an individual user to also provide their consent for the handling of data by third parties, for storing personal data on servers etc. Further, IT solutions give users the possibility to use cloud services, characterised by flows of large data quantities which are difficult if not impossible to control, and numerous other options. It seems there are endless possibilities which can quickly become uncontrollable and, among others, raise the question of traceability. Third parties must be clearly and explicitly listed as such whenever individuals are asked to give their approval for the processing of personal data. However, this raises another issue related to the format and type of consent that is one of the key aspects of the GDPR. In terms of mobile devices, spatial limitations or the desire for greater transparency and accessibility raise new questions about the acquisition of consent and thus bring new challenges for organisations and service providers. So-called drop down

menus do not comply with the GDPR because they mostly enable individuals to provide their consent without being informed or aware of the entire scope of access and all the entities with potential access to their personal data. Users neither have an immediate insight into such information nor an opportunity to opt-in since they are not required to open or access certain types of consent in their entirety. Therefore, they provide their consent based on incomplete information or, in some cases, on the opt-out method, which is plainly out of step with the GDPR principles (consent forms must not be filled-in as being 'approved' in advance). From a legal point of view, such consent is considered wrongly obtained by being acquired through means of a pre-completed choice which, for instance, may also include the "agree to all" choice, whereby individuals are unfamiliar with what the "all" actually means or entails.

The issues surrounding consent forms and the fact they contain absurd conditions for visiting websites or using applications should not be delved into any deeper because they vary from one website or application to another. The issues of consent could be discussed at length in a separate paper. In the end, it is up to the individual to decide whether they will consent to certain aspects they might not otherwise like for the sake of using a service or receiving content from a service provider, or whether they will fully give up visiting a website or using an application and find what they were looking for elsewhere.

Another important feature in this respect relates to the multifunctionality of mobile devices, which are not only used to store our own personal data but also the personal data of others. For instance, our mobile devices also store large databases of names and surnames, phone numbers and e-mail addresses of other individuals, photographs and videos containing the images of other individuals, as well as e-mails containing a wide array of contents, which might again include various personal data. Therefore, we are no longer responsible merely for our own personal data, but also for those of others. As such, we not only play the role of the user or an individual whose personal data are being handled, but also act as personal data processors. We collect, store and use all of the mentioned data for both private and professional purposes if our mobile device is used for work-related tasks. In doing so, we enable access to our mobile device (and its contents) to numerous applications, which demand we sign a series of consent forms and operate based on cooperation with third parties acting as processors of all (or some) of the aforementioned personal data. In addition, we use cloud services for which intrusions and data leakages are no longer inconceivable etc.

When expanding on the issues discussed above, one quickly sees the attractiveness of mobile devices stems from the simplicity and ease of their use; a single device can help achieve various goals, for instance travel, search for or even locate a device in the event of loss or theft. By turning on the device's location services, we enable the processing of personal data related to one's place of residence and work, favourite locations and routes travelled. Information technologies and their fast-paced development require users to possess ever-greater amounts of knowledge and, in some cases or to a certain extent, perform specific processes and actions which might be overwhelming for some, particularly given the multiplicity of these processes and the varying features

(mostly age-related) of different user populations. The average mobile device user cannot be expected to be familiar with all types of risks arising from use of the mobile medium. However, individuals (irrespective of their age and educational background) should be required to hold at least knowledge related to network services, which might prove too demanding for the general population. Users are familiar with, for instance, access to an unsecured wireless network, but are not necessarily familiar with every threat arising from connecting to such networks. Similarly, users may be familiar with receiving and opening e-mails, but might not have the necessary knowledge about different website types and the meaning behind various terms or abbreviations (e.g. the difference between http, https and other protocols). They may be familiar with the principles underlying the functioning of a touchscreen display yet, due to their impulsiveness, carelessness or lack of knowledge, might also click on pop-up windows informing them they have won a prize as the '1 millionth visitor' of a certain website or that their device has been infected with a virus.

The simplicity of use also relates to the variety of services we all carry out on our mobile devices, such as online banking services, enabling us to use our mobile phones to pay our bills with a couple of clicks or use our credit and debit cards to shop online. The scope of (in)security and threat is therefore extremely broad, while the consequences of improper use may be reflected in various areas.

The concepts of mobility and user awareness constitute a new element which raises a host of issues. Nevertheless, the former cannot be ignored or avoided since mobility is the key to mobile devices, while user awareness is something we must consider but predominantly depends on individual users. In light of the above, we could say that the share of individuals who leave their mobile devices unattended and uncontrolled, and do not use any of the default security features (lock screen, phone lock etc.), for whatever reason is quite problematic. On the other hand, new ways of protecting and increasing the security of mobile devices, such as unlocking a device by using identification services based on biometric identifiers, fingerprints, iris and facial features, give new possibilities for personal data processing. Therefore, one needs to master the art of striking the right balance between the various aspects of protection, security and privacy while ensuring the legality of one's business and other operations.

7 CONCLUSION

Personal data protection is a multifaceted field. Today, it affects almost every area of our everyday lives. Modern technologies are increasingly present and will therefore have an ever-greater influence of our future way of life, showing why the new GDPR has an important role to play in creating our future. By presenting and discussing some fundamental changes, this paper describes the elements introduced by the new GDPR and examines their impact on individuals and organisations. We find the GDPR does not introduce any 'revolutionary' changes but, if applied carefully, the GDPR will bring certain advantages for both individuals and companies. However, compliance with the Regulation will cause some inconvenience for those companies that fail to deal with personal

data consistently. On the other hand, for companies that have taken the personal data protection issue seriously, the new GDPR will not bring any major changes. Here, one must also consider the type of service a company is providing. The central part of the paper focuses on the way in which the GDPR will impact the users of mobile devices. Some organisations will restrict the use and processing of personal data on mobile devices. The GDPR (2016) also provides for greater control in the field of personal data protection. Yet, effective control cannot be achieved without individuals' cooperation, an aspect that can be strengthened by raising their awareness.

It is also clear that companies are making great efforts to conceal certain incidents, as recently occurred in the case of Yahoo (Fiegerman, 2017). Such practices could be prevented through a higher degree of awareness and reporting. Increased transparency will also contribute to greater respect for human rights and fundamental freedoms. By considering the available literature and limitations, this paper selectively presented some of the more important impacts of the GDPR on mobile devices. The examination of all impacts would require a longer and more comprehensive paper. Codes of conduct, case law, guidelines, rules, regulations and standards, which will be the real indicators of the GDPR's implementation in practice, will undoubtedly importantly impact the use of mobile devices. It will only be then that the objective impacts of the GDPR on mobile devices can be observed and analysed. Until then, we can only presume what might happen. The GDPR will have to be transposed to national legislation and implemented in member states' legal systems. Slovenia is already lagging behind here since an extraordinary session of the Slovenian Parliament rejected the amendments proposed to the Personal Data Protection Act (ZVOP-2). Therefore, one may ask what sanctions await Slovenia for not having adopted the amended Act. We expect the case law to have the strongest impact in this respect as it will resolve certain issues raised by experts in the field.

REFERENCES

Article 29 Data Protection Working Party. (2007). *Opinion 04/2007 on the concept of personal data*. Brussels: EC. Retrieved from https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf

Baker McKenzie. (2017). *GDPR national legislation survey*. Chicago: Baker McKenzie. Retrieved from http://www.bakermckenzie.com/-/media/files/insight/publications/2017/06/bk_itc_gdprsurvey_2017.pdf?la=en

Bernik, I., & Markelj, B. (2014). Zagotavljanje varnosti informacij z razumevanjem uporabnikovega ravnanja z mobilno napravo [Ensuring the security of information by understanding user behaviour on a mobile device]. *Varstvoslovje, 16*(1), 5–15.

Bolognini, L., & Bistolfi, C. (2016). Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law & Security Review, 33*(2), 171–181.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review, 32*(2), 179–194.

Ducato, R. (2016). Cloud computing for s-Health and the data protection challenge: Getting ready for the General Data Protection Regulation. V *2016 IEEE International Smart Cities Conference (ISC2)* (pp. 404–407). doi: 10.1109/ISC2.2016.7580803

DPOrganizer. (n. d.). *5 reasons for individuals to care about GDPR*. Retrieved from https://www.dporganizer.com/5-reasons-individuals-care-gdpr/

Eation, A. (September 13, 2017). *How to solve your CRM data quality problems before GDPR*. [Video]. Preact Limited. Retrieved from https://www.youtube.com/watch?v=gDUdlSX2DvA

Fiegerman, S. (September 7, 2017). The biggest data breaches ever. *CNNtech*. Retrieved from http://money.cnn.com/2017/09/07/technology/business/biggest-breaches-ever/index.html

Gilbert, F. (2016). EU general data protection regulation: What impact for businesses established outside the European Union. *Journal of Internet Law. 19*(11), 3–8.

GSMA Intelligence. (2018). *Definitive data and analysis for the mobile industry*. Retrieved from https://www.gsmaintelligence.com/

Hettrich, M. (2015). Data privacy regulation in the age of smartphones. *Touro Law, 31*(4), 981–1011. Retrieved from http://digitalcommons.tourolaw.edu/cgi/viewcontent.cgi?article=2681&context=lawreview

Informacijski pooblaščenec. (2017a). *Iskalnik po odločbah in mnenjih VOP: Določljivost posameznikov in osebnih podatkov* [Search engine for VOP order and views: Identifiable person and personal data]. Retrieved from https://www.ip-rs.si/vop/dolocljivost-posameznikov-in-osebnih-podatko-3031/

Informacijski pooblaščenec. (2017b). *Kaj prinaša nova Splošna uredba (EU) o varstvu podatkov?* [What does the new general data protection regulation (EU) bring?]. Retrieved from https://www.ip-rs.si/fileadmin/user_upload/Pdf/pripombe/Splosna_uredba_o_varstvu_podatkov-letak_maj_2017.pdf

Informacijski pooblaščenec. (n. d.). *Reforma evropskega zakonodajnega okvira za varstvo osebnih podatkov* [European general data protection regulation reform]. Retrieved from https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/

Information Commissioner's Office. (2017). *Moneysupermarket fined for ignoring customers' marketing email opt-outs*. Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/moneysupermarket-fined-for-ignoring-customers-marketing-email-opt-outs/

Ledino, J. (2012). How to remotely disable your los tor stolen phone. *PCmag*. Retrieved from https://www.pcmag.com/article2/0,2817,2352755,00.asp

Mantelero, A. (2013). The EU proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review, 29*(3), 229–235.

Markelj, B., & Bernik, I. (2016). Vpliv raznolikosti podatkov na odvzem in preiskovanje mobilnih naprav v organizacijah [The impact of the diversity of

information on the seizure and investigation of mobile devices in organisations].*Varstvoslovje, 18*(1), 84–97.

Ministrstvo za pravosodje RS. (2017). *Osnutek zakona o varstvu osebnih podatkov (ZVOP-2)* [Draft of the Personal Data Protection Act]. Ljubljana: MP RS. Retrieved from http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/mp.gov.si/novice/2017/september_2017/171004_ZVOP-2_status.pdf

Pedro, C. F. (2016). *Privacy in the smartphone age: A study on the privacy and data protection risks and violations of mobile applications* (Master's thesis). Tilburg: Law and Technology. Retrieved from http://arno.uvt.nl/show.cgi?fid=142089

Sire. (n. d.). *Are you prepared for the General Data Protection Regulation?* Retrieved from https://www.sire.co.uk/blog/are-you-prepared-for-the-general-data-protection-regulation

Sullivan, C., & Burger, E. (2017). "In the public interest": The privacy implications of international business- to- business sharing of cyber-threat intelligence. *Computer Law & Security Review, 33*(1), 14–29.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134–153. Retrieved from https://www.sciencedirect.com/science/article/pii/S0267364917301966#

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [GDPR]. (2016). *Official Journal of the EU,* (L 119).

Ustava Republike Slovenije [Constitution of the Slovenian Republic]. (1991, 1997, 2000, 2003, 2004, 2006, 2013, 2016). *Uradni list RS*, (33/91, 42/97, 66/00, 69/04, 68/06, 47/13, 75/16).

Voss, W. G. (2014). Looking at European Union data protection law reform through a different prism: The proposed EU General Data Protection Regulation two years later. *Journal of Internet Law, 17*(9), 12–24.

Voss, W. G. (2017). European Union data privacy law reform: General Data Protection Regulation, privacy shield, and the right to delisting. *Business Lawyer, 70*(1), 221–233.

Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1) [Personal Data Protection Act]. (2004, 2005, 2007). *Uradni list RS*, (86/04, 113/05, 51/07, 67/07).

About the Authors:

Domen Hribar, MA in Criminal Justice and Security from the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: domen.hribar@student.um.si

Miha Dvojmoč, PhD, Assistant Professor of Security Studies at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: miha.dvojmoc@fvv.uni-mb.si

Blaž Markelj, PhD, Assistant Professor of Security Studies at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: blaz.markelj@fvv.uni-mb.si

VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 20 no. 4 pp. 434–447

Analysis of the Legal Aspects of Illegal Asset Recovery in Slovenia[1]

Katja Rejec Longar

Purpose:

The aim of the study was to analyse the legal aspects of asset recovery in Slovenia through a five-stage asset-recovery process: financial investigation; freezing or seizure of assets; confiscation; enforcement of the confiscation order; and asset disposal.

Design/Methods/Approach:

EU and Slovenian legislation in the area of illegal asset recovery was analysed and compared. Using legal analysis, gaps and inconsistences were discovered and discussed.

Findings:

The Slovenian legal order provides relevant bodies with several avenues to recover 'proceeds' and illegally acquired assets. There is the traditional confiscation of proceeds, *in personam* confiscation in criminal proceedings, extended confiscation in criminal proceedings, and civil forfeiture pursuant to the Forfeiture of Assets of Illegal Origin Act. One problem is the related provisions are dispersed across both substantive and procedural law. Another problem is that some provisions are formulated in such a way that makes them impossible to apply in practice. It would be necessary to introduce a category of financial investigation in criminal proceedings. It is inappropriate that financial investigations are carried out under the provisions of civil law. Financial investigation must, therefore, become an essential part of all police criminal investigations of relevant offences, and holds the potential to generate proceeds. However, at the same time, law enforcement authorities must obtain a clear mandate that in the particular conditions they may investigate all assets of a suspect and not simply the concrete proceeds of crime.

Practical Implications:

The study findings are useful for preparing systemic changes in relation to the seizure of assets of illegal origin, also because the changes can be used to help establish an efficient way of organising the work of state bodies in this area.

Originality/Value:

The purpose of the paper is to comprehensively analyse all aspects of the seizure of assets of illegal origin. The results of the analysis substantially complement existing knowledge in the analysed field.

1 *The paper presents an extended and in-depth version of an article on illegal asset recovery first published in the contribution of Rejec Longar, Šugman Stubbs, & Lobnikar (2018).*

UDC: 343.272(497.4)

Keywords: illegal asset recovery, law, Forfeiture of Assets of Illegal Origin Act, Slovenia

Analiza pravnih vidikov odvzema premoženja nezakonitega izvora

Namen:

Namen študije je analizirati pravne vidike odvzema premoženja nezakonitega izvora v Sloveniji skozi prizmo petstopenjskega procesa odvzema nezakonitega premoženja: finančna preiskava, zamrznitev oziroma zavarovanje premoženja, odvzem premoženja, izvršitev odločbe o odvzemu ter upravljanja z odvzetim premoženjem.

Metode:

V prispevku smo s pomočjo pravne analize primerjali evropsko in slovensko zakonodajo na področju odvzema premoženja nezakonitega izvora. S pomočjo primerjave pravnih dokumentov smo ocenili razkorake in nedorečenosti med želeno in dejansko ureditvijo tega področja v Sloveniji.

Ugotovitve:

Slovenski pravni red pristojnim organom ponuja več možnosti odvzema premoženja nezakonitega izvora. Uporabijo lahko klasični odvzem premoženjskih koristi v okviru kazenskega postopka, razširjeni odvzem po kazenski zakonodaji ter civilni odvzem preko tožbe v skladu z zakonom o odvzemu premoženja nezakonitega izvora. V analizi smo ugotovili težave pri jasnosti materialnih določb materialnega in procesnega prava. Nadaljnja težava je, da so nekatere določbe v slovenski zakonodaji oblikovane tako, da jih ni mogoče izvajati v praksi. Avtorji menimo, da bi bilo nujno opredeliti finančno preiskavo v okviru kazenske zakonodaje. Ni primerno, da se finančna preiskava izvaja po določbah civilnega prava. Poleg tega mora finančna preiskava postati ključni del vseh kriminalističnih preiskav kaznivih dejanj, kjer je mogoče uveljavljati odvzem premoženja nezakonitega izvora, pri tem pa mora biti v zakonu nedvoumno zapisan mandat in odgovornosti za izvedbo finančne preiskave.

Praktična uporabnost:

Ugotovitve študije so koristne pri pripravi sistemskih sprememb na področju zasega premoženja nezakonitega izvora, mogoče pa jih je uporabiti tudi pri vzpostavitvi učinkovite organizacije dela državnih organov na analiziranem območju.

Izvirnost/pomembnost prispevka:

Namen prispevka je celostno analizirati vse vidike zasega premoženja nezakonitega izvora. Rezultati analize bistveno dopolnjujejo obstoječe znanje na analiziranem področju.

UDK: 343.272(497.4)

Ključne besede: odvzem premoženja nezakonitega izvora, zakon o odvzemu premoženja nezakonitega izvora, finančne preiskave, Slovenija

1 INTRODUCTION

In recent years, Europe has adopted the American idea that illegal asset recovery is a particularly effective tool for tackling organised crime. Namely, long prison sentences for individuals from organised crime groups have proved ineffective, mainly by not being handed out to the heads of illegal business and that the illegally acquired assets are left intact (Jensson, 2011). The idea of the asset recovery being important goes back to the 1980s. Faced with Colombian drug barons, US law enforcement found the traditional law enforcement strategies were unsuccessful, primarily because they did not strike at the revenues of the illegal trafficking, which generated extremely high profits (Jensson, 2011). Further, the revenue drug trafficking gave organised crime groups considerable financial strength and influence, allowing them to start penetrating the licit economy (Vettori, 2006). Prison sentences for committing these types of criminal offences were no longer effective, especially since groups with substantial financial resources took to corruption and influenced the decisions of law enforcement agencies, the judiciary, as financial institutions, even legislators. Tools for dealing with organised crime had to be adapted to the specifics of this type of crime. Williams (2001) argues one can investigate criminal networks only with networks, i.e. with less bureaucratic structures and by using more innovative organisational models. Similarly, Dobovšek (2008) underlines the importance of a multidisciplinary approach in the cooperation of institutions at both national and international levels. The aim of organised crime is not only to generate and misappropriate the proceeds of crime or criminal assets, but also to gain power in society (Levi, 2015). Criminal networks invest their funds and rely on corrupt practices to obtain access to decision-makers, who in turn give them access to important information and decision-making powers. The concealment of criminal proceeds usually involves professionals and practitioners, such as lawyers, accountants and financial experts (Middleton & Levi, 2015), who apply their expertise to enable the transfer of 'ill-gotten gains' into legitimate business environments. Authors have long discussed the term "state capture", which denotes organised networks taking control over state mechanisms in order to manage and control policy-making and the economy, thus undermining the basic democratic foundations of society and hijacking the state. Therefore, this type of crime is particularly problematic and dangerous for society (Rejec Longar, Šugman Stubbs, & Lobnikar, 2018).

Another element adding to the complexity of prosecuting organised crime is globalisation. Globalisation has caused a certain openness of borders which, due to insufficiently effective cooperation among the authorities of different states, makes it easy to hide illegally obtained assets and launder money. Jager and Šugman Stubbs (2013) stress the importance of preventive measures for reducing crime rates and believe the state should support various preventive actions like education and situational crime prevention while simultaneously implementing criminal law repression. The authors conclude that criminal law repression is neither a miracle cure for addressing accumulated social problems nor a fundamental instrument regulating people's behaviour – criminal law can only be the *ultima ratio of* action in society. The tools to combat organised crime

had to be adapted, and one (probably the most effective) of them was to introduce the recovery of criminal assets into the legal system. On this basis, the aim of this paper is to analyse the acts proclaimed by international organisations (with an emphasis on EU legislation) and make a comparative legal analysis of the asset-recovery systems with that existing in Slovenia.

2 RECOVERY OF ILLEGAL ASSETS

We must first define the recovery of illegal assets before considering whether it is an effective tool in the fight against organised crime. The limited literature on the subject and the masses of related international documents allow the conclusion that the terminology in the area of asset recovery is quite confusing. Especially within national systems, the concepts of asset recovery, confiscation and forfeiture are often confused. Vettori (2006) defines the confiscation of the proceeds of crime as the permanent withdrawal by the court or other competent authority of any property which originates from or is in any way connected to a criminal offense. However, to ensure illegally gained assets that have been recovered really end up in the state's coffers, many more steps both pre- and post- confiscation are needed. More broadly, illegal asset recovery is defined as a process with the following steps (Council of the EU, 2012):

- Financial investigation, an investigative technique that interlinks actors, locations and events through financial facts. This phase is important for determining the full range of assets that potentially have an illegal origin.
- Freezing or seizing of assets; when all assets suspected of being of illegal origin are identified, they must be secured. This phase generally already contains a court's decision on the provisional measures.
- Confiscation, which is underpinned by a court decision (order) and means the permanent transfer of ownership rights to assets from the asset holder to the state.
- Enforcement of the confiscation order; this is the phase in which the assets are actually passed on to the state.
- Asset disposal; the phase that decides how the state will make use of the assets. This phase is closely linked to asset management.

The question is whether the Slovenian regulatory framework is established systematically by wholesomely considering all asset-recovery process phases or whether it is more the case there are only partial solutions in place, leaving the phases not dealt with coherently. In this context, it is important to stress that the legislative system (or norms) in society stems from the need for a static record of certain commitments with a view to resolving certain social problems (Kratochwil, 1995). Therefore, assuming that people are guided by rules which directly impact human lives (Kratochwil, 1995), we can logically conclude that rules must be clear and comprehensible or systematic if they are to be well understood and efficient. In our case, this means the law must enable a comprehensive view of the entire process and its stages (financial investigation, freezing or seizing, confiscation, enforcement, and disposal) supported by adequate substantive laws and effective reference to other procedural laws and procedures (e.g. the tax procedure).

3 ILLEGAL ASSET RECOVERY IN SLOVENIA

The five-stage procedure described above serves as a basis for examining the legal framework governing the recovery of assets of illicit origin in Slovenia in what follows. Nowadays, the field of asset recovery in Slovenia is regulated by the Criminal Code (Kazenski zakonik, 2012), the Criminal Procedure Code (Zakon o kazenskem postopku, 2012) and the Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega izvora, 2011). The legal system in Slovenia thus foresees confiscation in both criminal and civil law contexts. Starting with the first phase of the illegal asset recovery procedure, i.e. financial investigation, we can see that it is not defined in the Criminal Procedure Code (Zakon o kazenskem postopku, 2012). For this phase, general provisions on investigation may apply. Article 499 of the Criminal Procedure Code (Zakon o kazenskem postopku, 2012) binds the court and other agencies to gather evidence and inquire into circumstances material to the determination of proceeds of crime. Paragraph 3 of Article 507 of the same law *mutatis mutandis* expands this stipulation to the pre-trial and investigation procedure. Therefore, financial investigation is not systematically defined and shall be carried out according to the general provisions, except for *in personam* confiscation in criminal proceedings (Zakon o kazenskem postopku, 2012, Article 498.a), which applies only to offences of corruption and money laundering. In the case of *in personam* confiscation, the financial investigation is carried out *ex-post facto*. This is probably an additional financial investigation which complements that already done when investigating the offence. In contrast, in civil proceedings, financial investigation is well defined, and this unbalanced approach in the legislation could result in the tendency of law enforcement authorities to prioritise the civil procedure for asset recovery from criminals.

After the investigation phase, if the law enforcement authorities find that an individual does hold proceeds of crime, the prosecutor can propose the freezing or seizure of the said assets to the court. More specifically, Article 502 of the Criminal Procedure Code (Zakon o kazenskem postopku, 2012) provides that the court may, upon the proposal of the State Prosecutor, issue a freezing or seizing order where there is a risk the defendant could use these proceeds for further criminal activities or could conceal, alienate, destroy or otherwise make use of the proceeds. This provision is from a substantial point of view simple and logical, especially when the procedure is about an uncomplicated classical confiscation or the confiscation of instrumentalities of crime. Namely, in this case, the police can – when encountering certain assets during an investigation – easily identify them as proceeds of crime, even more so when the proceeds are an element of the criminal offence. But the case can be quite different if the crime is committed by a criminal organisation where the material law distinguishes between the proceeds of crime and illegally acquired assets, with the latter having a much broader meaning. The key question is whether Article 502 of the Criminal Procedure Code (Zakon o kazenskem postopku, 2012) gives the legal basis for the court to secure illegally acquired assets in the broad sense. The problem is already initially with the financial investigation because the Criminal Procedure Code (Zakon o

kazenskem postopku, 2012) does not extend it beyond investigating a concrete offence and does not allow the investigation of all assets of an individual. This questions whether such property can be identified in the criminal investigation in the first place. But even if we assume that in the financial investigation all assets were identified and that the prosecutor by a literal interpretation of Article 77.a of the Criminal Code (Kazenski zakonik, 2012) identified them as proceeds of crime, this situation may not be upheld by the Constitutional Court of the Republic of Slovenia. Namely, Constitutional Court decision U-I-296/02 (Constitutional Court of the Republic of Slovenia, 2002) found that a confiscation pursues two constitutionally permissible objectives while seeking to secure proceeds: to prevent criminal activity, and to ensure the effective confiscation of proceeds with a view to preventing unjust enrichment. In addition, they performed the proportionality test and held that the state can secure only assets that match the estimated value of the proceeds, which derive from the actual criminal offence in question. Yet such an interpretation does not prevent law enforcement authorities conducting an extensive investigation of a suspect's assets. However, when sufficient assets have been found, they cannot secure more than the concrete proceeds of the alleged crime. Further, in a later decision Up-6/14 dated 5 March 2015 the Constitutional Court of the Republic of Slovenia (2015) specifically stated that assets have to be secured up to the value that corresponds to the estimated amount of proceeds derived from the criminal offence. According to the Constitutional Court, it is therefore inadmissible to secure more assets than it would be permitted to take (see para. 13 of the decision on p. 5). Based on this, we may conclude that the legislator did not adjust the provisions of the Criminal Procedure Code (Zakon o kazenskem postopku, 2012) on freezing and seizure to the subsequent amendment of the Criminal Code (Kazenski zakonik, 2012), which as introduced in Article 77.a extends confiscation.

From a procedural perspective, a freezing or seizure order is issued by the court upon a proposal by the prosecutor. The order is then served on all parties participating in the proceedings. This is quite a common procedure, but from here on the Slovenian procedure becomes more complicated compared to most other countries. This is partly due to numerous rulings of the Constitutional Court of the Republic of Slovenia, which has dealt with the problem of the time limitation for securing assets. Namely, the legislation limits the duration of a seizure or freezing order to three months maximum in the pre-trial stage or six months after the indictment. When this period has elapsed, the court may on a reasoned proposal from the public prosecutor extend the measure, but it must allow all other participants to voice their opinions. From the indictment till final judgment of the court at first instance, the total duration of a temporary measure may not exceed three years. Three- or six-month intervals at which the prosecutor must extend the securing of assets are extremely short and at the same time require the considerable commitment of both the prosecutor and the court (court hearings, justification for proposing an extension, etc.).

The inadequacy of the freezing and seizure provisions in criminal proceedings seems to be compensated by civil proceedings in Articles 20 to 24 of the Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega

izvora, 2011). In civil proceedings, a seizure or freezing order can be issued if there is a reasonable suspicion that a catalogue crime was committed and there is a disparity between the suspect's income and the value of assets they have available and, further, that there is a risk the owner will hide or destroy the assets. These conditions allow the national prosecutor a much easier burden of proof because there is no need to prove there is a certain degree of suspicion that the proceeds were obtained from crime. The court in civil proceedings also does not deal with the legality of the acquisition of the assets, but only assesses the proportionality of the gained wealth based on the data submitted. The freezing and seizure order cannot be appealed against but, on the other hand, grounds for giving it must be given. Further, there are no additional court hearings, nor is the judge obliged to inform the participants about the case file, like in criminal proceedings. The duration of the order in civil proceedings is limited to one month after completion of the financial investigation if the prosecutor does not file an action. Yet, if an action is filed, the prosecutor may apply for an extension of the validity of the order. However, the law is not clear on the maximum length of this extension. We can easily conclude that with the civil procedure for securing assets being uncomplicated compared to the criminal, the prosecutor will certainly not be so motivated to pursue a freezing and seizing order under the Criminal Procedure Code (Zakon o kazenskem postopku, 2012) provisions and will prefer to apply under the Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega izvora, 2011).

From a historical point of view, the rule on traditional confiscation in criminal law, i.e. the principle that no one may gain from crime, has been found in the Slovenian system from the beginning. The provision on classic confiscation is contained in Article 74 of the Criminal Code (Kazenski zakonik, 2012). The difference between classic confiscation and the recovery of illicit assets is that the latter is much broader and also covers the benefit obtained by other unlawful manner, and is not necessarily derived from committing a criminal offence (Gorkič, 2011). Slovenian theory and jurisprudence do not define the confiscation of proceeds of crime as a criminal sanction, even though it affects the assets of a convicted person or any other person the confiscation order is addressed to (Plesec, 2014). That the benefit was obtained from crime is merely a circumstance or precondition for this measure to be imposed. Similarly, the Constitutional Court divides the phase up until the conviction and the phase of confiscating the proceeds of crime.

In the Slovenian legal system, an amendment to the Criminal Code in 2012 (Kazenski zakonik, 2012) introduced extended confiscation when the offence is committed by a criminal organisation. Therefore, under Article 77.a of the Criminal Code (Kazenski zakonik, 2012) it is sufficient that a criminal group has these assets at their disposal. This provision stipulates that an offender who commits a crime within a criminal organisation is also subject to the confiscation of all assets resulting from the criminal activity engaged in by this organisation. This means the provisions of the first paragraph of Article 77.a of the Criminal Code (Kazenski zakonik, 2012) distinguish between a pecuniary benefit or proceeds of crime (a narrower term) and illicit assets acquired by a criminal activity within

a criminal organisation (broader term). However, the Criminal Code (Kazenski zakonik, 2012) does not define the difference between illicit assets and proceeds, except when it comes to assets the criminal organisation disposes of. Proceeds derived from a crime that individual members of a criminal organisation were convicted for are dealt by the traditional confiscation provisions found in Article 74 of the Criminal Code (Kazenski zakonik, 2012). Still, the second paragraph of Article 77.a of the Criminal Code (Kazenski zakonik, 2012) also provides for the confiscation of assets gained through criminal activity, and we may conclude the Criminal Code (Kazenski zakonik, 2012) is quite inconsistent when applying the concepts of illicit assets and proceeds. Further, since the recipient of the proceeds is a criminal group, it may be questioned to whom the confiscation order should be addressed. Since confiscation orders are enforced according to civil law provisions, it would be very difficult to execute one addressed to a criminal organisation without recognising its legality, and that would mean infringing the public order. This provision is therefore very difficult to apply in practice and, in fact, leaves the prosecutor only with the classic confiscation path. As an example, in a decision made in 2006 the Supreme Court of the Republic of Slovenia (2006) noted that in the case of organised criminal activity it is very difficult, if not impossible, to obtain direct evidence on direct recipients of the proceeds (Judgment I PSP 281/2005 of 26 10 2006). Therefore, in such cases, the court considers members of organised groups as accomplices and, for proceeds to be confiscated, the court is allowed a discretion by considering the circumstances of the case, including the importance of the role of each accomplice in the group (Supreme Court of the Republic of Slovenia, 2006). In other words, while the old Criminal Code allowed only the confiscation of proceeds derived from a concrete offence, the current alternative offers no progress. In practice, it is impossible to recover illicit assets within the criminal procedure as the case law counts members of organised crime group as accomplices in the offence. Moreover, if one of the organised group members, i.e. accomplices, is acquitted and if the court issues a confiscation order for illicit assets of the organised group, this would in fact constitute a new indictment (Gorkič, 2014). Taking account of this, we may conclude the procedural provisions in Article 499 of the Criminal Procedure Code (Zakon o kazenskem postopku, 2012) are inappropriate.

After a final confiscation order is issued, a new phase of the procedure starts, i.e. the enforcement of the order. This phase is extremely important because it is only if this phase is successfully concluded that the proceeds and illicit assets actually become the property of the state. As regards execution in civil proceedings, Jenull (2014) notes the provisions of the Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega izvora, 2011) in this phase are confusing and contradictory. Jenull (2014) highlights one aspect that is problematic, namely the law refers to tax enforcement, but does not distinguish between enforcement of movable and immovable property. Namely, in the first paragraph of Article 35 of the Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega izvora, 2011) there is reference to other laws upon which the competent authorities carry out their tasks, depending on the type of property. Then, in the second paragraph, the provision applies mutatis

mutandis to the Law on Execution and Interim Protection of Claims (Zakon o izvršbi in zavarovanju, 2007) for the enforcement of these orders. However, in the third paragraph of the same article, the law sets Financial Administration as the competent authority for the purpose of the enforcement. The problem of this provision is that the Law on Execution sets the court as the competent authority for execution, while the Financial Administration is competent for enforcement only under the Tax Procedure Act (Zakon o davčnem postopku, 2011). Further, tax enforcement is limited solely to monetary claims because under the tax procedure it is impossible to execute on immovable property or company shares. The Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega izvora, 2011) is hence completely unclear on the question of whether the Financial Administration can carry out enforcement on immovable property. This dilemma is quite problematic because the Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega izvora, 2011) governs *in rem* confiscation, which aims at confiscating concrete assets. The Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega izvora, 2011) otherwise defines assets as property and rights which may be the subject of enforcement, in particular immovable property, movable property and all other assets that have a monetary value, as well as assets which derive directly or indirectly from such assets (item 1 of Article 4 of the Forfeiture of Assets of Illegal Origin Act). This definition leads us to conclude that the assets which are to be the subject to enforcement under the Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega izvora, 2011) will mostly be assets which cannot be the subject of monetary enforcement. Therefore, the law will have to be amended in this part, something also proposed by Jenull (2014). In criminal proceedings, there is no such dilemma. Namely, Article 131 of the Criminal Procedure Code (Zakon o kazenskem postopku, 2012) covers both situations, i.e. enforcement under the provisions of the tax procedure law and the option of using the law on enforcement.

The management phase offers flexible legal solutions for the disposal of the secured and confiscated assets. Yet, one may question whether the system works in practice. The most pertinent problem, among others, is surely the issue of determining the value of seized assets. The fact is that, especially in cases of value confiscation, determining the value of assets brings some problems (Selinšek, 2007).

The Slovenian system also faces some issues with the organisational aspects of the asset recovery regime. In the pre-trial procedure, the organisational structure for conducting investigations is extremely varied and complex (Dežman & Erbežnik, 2003). In this phase, Slovenian law intertwines the competence of the police and prosecutors, but without the clarity needed as to which of the two holds primary responsibility for conducting investigations in the pre-trial procedure (Vrtačnik & Hostnik, 2015). This raises very important questions about responsibility for a proper investigation: is it the responsibility of the police, the prosecutor, or the two bodies together? The state prosecutor is responsible for directing the investigation, while the police are responsible for the correct implementation of investigative measures. From the laws dealing with the

responsible authorities for an investigation, we may assume that if an offence which generated proceeds is detected by the police, the police conducted the initial investigative steps while, if the offence was brought directly before the prosecutor, the prosecutor's office will carry out the investigation by properly directing the police. As financial investigations are conducted under the general rules on investigation, the dispersed responsibility naturally applies to this phase, too.

The law gives an opportunity to set up specialised investigative teams under Article 160 a. of the Criminal Procedure Code (Zakon o kazenskem postopku, 2012). These teams are directed by a public prosecutor, and combine various bodies and institutions, with the aim to provide a multidisciplinary approach to the investigation of criminal offences. The duration of such a group's operation is questionable because the law is silent on this matter; however, logically the duration should be limited with the procedural powers of the prosecutor. Therefore, it is very dubious if the investigative team can engage in any action regarding the seeking of property after the final conviction has been secured. This is particularly important in matters of organised and economic crime where the perpetrators use sophisticated ways to hide criminal assets. It would therefore be very important for a multidisciplinary financial investigation to be extended to the enforcement phase of recovery. Another problem of specialised teams is they do not have a permanent structure. Under the legislation, teams consist of members of all competent national authorities and institutions whose powers and tasks are connected to investigating the offence. But this does not necessarily mean that members have the experience required for work on financial investigations. Further, for members of the team this is just extra work on top of their regular tasks, and they cannot be fully dedicated to the financial investigation only. A financial investigative team can also be established in civil proceedings pursuant to Article 14 of the Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega izvora, 2011). Yet the organisational structure is clearer in the phase of financial investigations within civil proceedings. In this case, the police do not have their own competences and depend entirely on the directions of the prosecutor. But the same problem arises with the duration of financial investigation teams' operations, which is limited to the phase of financial investigation and does not extend to the final execution or payment to the state budget.

In the stage of securing assets, Article 506 of the Criminal Procedure Code (Zakon o kazenskem postopku, 2012) gives the court powers to manage the assets and it must act with due diligence and take very quick action in these cases. In practice, determining when the storage of the assets is associated with excessive costs has proven very problematic for the courts. Judges often do not have the required knowledge and are unable to estimate the value of certain property types or decide on the ways of storage and all associated costs. External contractors, on the other hand, do not have any interest in selling the assets further as their storage retention is a very profitable business. A very similar situation occurs later in criminal proceedings after the conviction has been declared, and the proceeds have to be determined ex officio or independently of the will of the state prosecutor.

Under Article 501 of the Criminal Procedure Code (Zakon o kazenskem postopku, 2012), the court can use its discretion to determine the amount of proceeds if its determination would cause disproportionate difficulties or if the procedure would be unduly protracted. Although the court must substantiate its decision and justify it by reference to facts, such a legal solution is inappropriate. Namely, it is impossible for the judge to hold all this knowledge and skills, in particular when a complex matter is entailed, such as managing larger companies, exotic animals and the like.

For asset management, the Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega izvora, 2011) authorises different institutions and refers to different laws. It is obvious that by using such general blanket references to other provisions the legislator wished to avoid various problems (Jenull, 2014), especially the establishment of new institutions that might during the deepest economic crisis in 2010 have been viewed as considerably unpopular. Altogether, it is illogical that the management of assets is left to two different regimes: first in criminal proceedings where management is assigned to the court, and second in the civil procedure, where such management is left to different institutions, depending on the asset types.

4 CONCLUSION

Through analysis of legal acts, we may conclude that only a systematically formed legislative framework can ensure an effective system for confiscating proceeds and illegal asset recovery. For Slovenia, this would initially mean it would be necessary to define financial investigation in criminal proceedings (Zakon o kazenskem postopku [Criminal Procedure Code], 2012). Namely, a financial investigation is the starting point for the whole asset-recovery process. And that includes financial investigation in the civil procedure because the trigger for launching the procedure is a suspicion that certain assets were acquired by committing an offence. It is therefore inappropriate for a financial investigation to be carried out under the provisions of civil law. We believe that, already in this stage, the legislator should give a clear message that the primary attempt to confiscate proceeds and illegal assets should occur through criminal proceedings and, only if this proves impossible, should the law enforcement use civil forfeiture proceedings. Financial investigation must therefore become an essential part of all police criminal investigations of offences which could generate any proceeds. However, at the same time, law enforcement authorities must obtain a clear mandate that in certain conditions they can investigate all assets of the suspect, not only the concrete proceeds of crime. Such a mandate would also make the financial investigation useful for extended confiscation in criminal proceedings and civil forfeiture. In this phase, it is also necessary to very clearly define the responsibility of the leading actors in the investigation and, in our opinion, this must be the prosecutor because immediately after a financial investigation has been concluded the prosecutor may propose the seizure or freezing of assets. The prosecutor should also be given a mandate to secure assets in urgent and exceptional circumstances with only the subsequent confirmation of the court,

while at the same time the procedural provisions for securing assets in criminal proceedings must be simplified in the same way as they are in civil proceedings under the Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega izvora, 2011). From the institutional point of view, it would make sense to set up a multidisciplinary body – an Asset Recovery Office (ARO) – which would enable investigators to have easy access to data both at home and internationally. The ARO could act as a think-tank and would ensure through training that, where relevant, financial investigations become part of all police investigations.

On a positive side, Slovenia's legal order provides the competent authorities with several avenues for recovering proceeds and illegally acquired assets. There is the traditional confiscation of proceeds, *in personam* confiscation in criminal proceedings (Article 498.a of the Criminal Procedure Code) (Zakon o kazenskem postopku, 2012), extended confiscation in criminal proceedings (Article 77.a of the Criminal Code) (Kazenski zakonik, 2012) and civil forfeiture after the Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega izvora, 2011). One problem is that the relevant provisions are dispersed across both substantive and procedural law. Another problem is that some provisions are formulated in such a way that they are impossible to implement in practice. In particular, we showed that Article 77.a of the Criminal Code (Kazenski zakonik, 2012) *de facto* does not bring any changes with respect to classical confiscation since the assets of a criminal organisation, which has no legal personality, are impossible to confiscate. Further, contrary to some other legal systems, the Slovenian legislation does not define the concept of criminal activity that should be the basis for applying extended confiscation. It is thus necessary to introduce extended confiscation with a reversed burden of proof into the Criminal Code (Kazenski zakonik, 2012) and link it with criminal activity, which would be best defined as the implementation of certain elements of a criminal offence in a given period.

The enforcement phase should be stipulated in a completely different way in both the criminal and civil procedure. Chiefly, it is a question of organisation because, at the moment, especially following the Forfeiture of Assets of Illegal Origin Act (Zakon o odvzemu premoženja nezakonitega izvora, 2011), it is unclear which institution is responsible for enforcing confiscation orders. Moreover, it is necessary to establish a record of how many confiscation orders have in fact been enforced and the exact amount sent into the state budget. This record will show how cost-effective the asset recovery system in Slovenia is and whether proper criteria and methods for evaluating assets are in place. The evaluation of assets is a particularly problematic aspect of the Slovenian system because, as a general rule, it is performed by judges who often do not possess adequate knowledge and skills. The creation of a centralised body to manage the assets would be a good solution: it would take care of assets from the time of their valuation, deal with their freezing and seizure until they are finally disposed.

REFERENCES

Council of the EU. (2012). *Accompanying document to the proposal for a Directive of the EP and Council on the freezing and confiscation of proceeds of crime in the EU – Impact Assessment*. Brussels: Council of the EU.

Constitutional Court of the Republic of Slovenia. (2002). U-I-296/02. Retrieved from http://odlocitve.us-rs.si/sl/odlocitev/US23565

Constitutional Court of the Republic of Slovenia. (2015). Up-6/14. Retrieved from https://www.us-rs.si/aktualno/novice/odlocba-ustavnega-sodisca-st-up-614-z-dne-5-3-2015/

Dežman, Z., & Erbežnik, A. (2003). *Kazensko procesno pravo Republike Slovenije* [Criminal procedural law of the Republic of Slovenia]. Ljubljana: GV Založba.

Dobovšek, B. (2008). Economic organized crime networks in emerging democracies. *International Journal of Social Economics, 35*(9/10), 679–690.

Gorkič, P. (2011). Stranske žrtve uvedbe odvzema premoženja z obrnjenim dokaznim bremenom [Secondary victims of introducing deprivation of property by reversal burden of proof]. *Podjetje in delo, 37*(6/7), 1031–1037.

Gorkič, P. (2014). Dokazovanje v postopku odločanja o odvzemu premoženjske koristi in premoženja [The evidence procedure of illegal asset recovery]. *Pravnik, 69*(9/10), 575–601.

Jager, M., & Šugman Stubbs, K. (2013). Za več preventive pri obvladovanju gospodarske kriminalitete [For more prevention in dealing with economic crime]. *Revija za kriminalistiko in kriminologijo, 64*(2), 154–162.

Jensson, A. (2011). *Crime should not pay: Iceland and the international developments of criminal assets recovery* (Master thesis). Haskoli Islands: School of Social Sciences.

Jenull, H. (2014). Izvršitev odvzema premoženja po ZOPNI [Enforcement of the asset seizure according to the FAIOA]. *Pravna praksa, 33*(49–50), 8–9.

Kazenski zakonik [Criminal Code] (KZ-1-UPB2). (2012, 2015, 2016, 2017). *Uradni list RS*, (50/12, 54/15, 6/16, 38/16, 27/17).

Kratochwil, F. V. (1995). *Rules, norms and decisions: On the conditions of practical and legal reasoning in international relations and domestic affairs*. Melbourne: Cambridge University Press

Levi, M. (2015). Money for crime and money from crime: Financing crime and laundering crime proceeds. *European Journal on Criminal Policy and Research, 21*(2), 275–297.

Middleton, D., & Levi, M. (2015). Let sleeping lawyers lie: Organized crime, lawyers and the regulation of legal services. *British Journal of Criminology*, *55*(4), 647–668.

Plesec, P. (2014). Pravna narava odvzema po Zakonu o odvzemu premoženja nezakonitega izvora [Legal nature of the confiscation of property by FAIOA]. *Pravnik, 69*(11/12), 809–838.

Rejec Longar, K., Šugman Stubbs, K., & Lobnikar, B. (2018). Effectiveness of asset recovery in Slovenia – comparison of police officers' and prosecutors' opinions. In G. Meško, B. Lobnikar, K. Prislan, & R. Hacin (Eds.), *Criminal justice and security in Central and Eastern Europe: From common sense to evidence-based*

policy-making: Conference proceedings (pp. 598–615). Maribor: University of Maribor Press; Ljubljana: Faculty of Criminal Justice and Security.

Selinšek, L. (2007). *Kazensko pravo – splošni del in osnove posebnega dela*. [Criminal law - the general part and the basics of special part]. Ljubljana: GV Založba.

Supreme Court of the Republic of Slovenia. (2006). I PSP 281/2005. Retrieved from http://www.sodnapraksa.si/?q=id:26307&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&page=0&id=26307

Vettori, B. (2006). *Tough on criminal wealth: Exploring the practice of proceeds from crime confiscation in the EU.* Doordrecht: Springer.

Vrtačnik, M., & Hostnik, M. (2015). *Državno tožilstvo v Republiki Sloveniji* [State Prosecutor's Office in the Republic of Slovenia]. Ljubljana: Vrhovno državno tožilstvo.

Williams, P. (2001). Transnational criminal networks. V J. Arquilla, & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 61–97). Santa Monica: RAND Corporation.

Zakon o davčnem postopku [Tax Procedure Act] (ZDavP-2-UPB4). (2011). *Uradni list RS*, (13/11).

Zakon o izvršbi in zavarovanju [Law on Execution and Interim Protection of Claims] (ZIZ-UPB4). (2007, 2009, 2010, 2011, 2014, 2015, 2018). *Uradni list RS*, (3/07, 93/07, 28/, 09, 51/10, 26/11, 53/14, 54/15, 11/18).

Zakon o kazenskem postopku [Criminal Procedure Code] (ZKP-UPB8). (2012, 2013, 2014). *Uradni list RS*, (32/12, 47/13, 87/14).

Zakon o odvzemu premoženja nezakonitega izvora [Forfeiture of Assets of Illegal Origin Act] (ZOPNI). (2011, 2014). *Uradni list RS*, (91/11, 25/14).

About the Author:

Katja Rejec Longar, Ministry of Justice of the Republic of Slovenia. E-mail: katja.rejec-longar@gov.si

VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 20 no. 4 pp. 448–461

Formal Boundaries of Slovenian Law

Bojan Tičar

Purpose:

The article is primarily intended for foreign exchange students (e.g. students participating in the Erasmus+ programme) at the Faculty of Criminal Justice and Security of the University of Maribor studying how Slovenia regulates the field of criminal justice and security. The article deals with the formal boundaries of Slovenian law mostly from the viewpoint of the legal order in force in the country. Readers will learn how the Slovenian legal order functions, which general acts are adopted by the state and which by local bodies, the rules governing their application, and the relationships between them, as well as the way EU law is applied in Slovenia.

Deign/Methods/Approach:

The article is a review article based on a descriptive analytical method and linguistic interpretation of the relevant regulations. The author also applies a historical method – primarily by presenting the Roman law perspective on legal concepts – as well as teleological and legal philosophical methods in defining legal concepts.

Findings:

The article examines fundamental legal institutions. The author establishes the attitude of writers in the fields of the theory of law and critical jurisprudence regarding the definitions of key legal concepts and phenomena. The article concludes with Kant's remark that lawyers are still seeking a definition of their concept of law (Perenič, 2007).

Research Limitations/Implications:

The article is short. The legal definitions are occasionally simplified which, however, is not to the reader's disadvantage. In some instances, the author attempts to simplify complicated legal concepts with the objective of making the study of other subjects in the field of criminal justice and security easier for the reader and to provide a clear foundation for a basic understanding of the categorical apparatus in law.

Practical Implications:

The article has practical value for foreign, English-speaking students who, generally, are not students of law, but need a basic understanding of the fundamental legal concepts useful in most social science research. The definitions of the concepts are appropriate and contemporary and thereby contribute to better understanding of the field.

Originality/Value:

The article is a review article and therefore its originality is limited. The author namely does not establish any new scientific findings, but summarises and defines already known concepts. The article's original value is that the author presents fundamental legal concepts and definitions in a readable and easy-to-digest manner that the reader can easily remember. The definitions of the legal concepts addressed in the article are precise and useful and will serve the reader in further study or research.

UDC: 34(497.4)

Keywords: law, legal order, morality, classification of law, sources of law, legal norm, statute, lex specialis

Formalne meje slovenskega prava

Namen prispevka:

Prispevek je v prvi vrsti namenjen študiju na Fakulteti za varnostne vede Univerze v Mariboru, in sicer tujim študentom (npr. tistim iz programa Erasmus+), ki prihajajo na izmenjavo in študirajo slovensko pravno ureditev na področju varstvoslovja. V prispevku so predstavljene formalne meje slovenskega prava predvsem z vidika veljavnega slovenskega pravnega reda. Bralec se lahko seznani, kako slovenski pravni red deluje, katere splošne akte sprejemajo državni in lokalni organi, kakšna so pravila uporabe in razmerij med njimi ter kako deluje pravo EU v Sloveniji.

Metode:

Članek je pregledni znanstveni članek, ki temelji na deskriptivni in analitični metodi ter jezikovni razlagi relevantnih predpisov. Od pravnih metod avtor uporabi še historično metodo – predvsem s prikazom rimskopravnega pogleda na pravne pojme – pa tudi teleološko in pravno-filozofsko metodo pri opredeljevanju definicij pravnih pojmov.

Ugotovitve:

V prispevku so na pregledni način prikazani temeljni pravni instituti. Avtor sproti ugotavlja, kakšen je odnos piscev s področja teorije prava pa tudi s področja kritičnega prava na definiranje ključnih pravnih pojmov in pojavov. Članek zaključi s Kantovo mislijo, da »pravniki še zmeraj iščejo svoje bistvo prava« (Perenič, 2007, str. 69).

Omejitve/uporabnost raziskave:

Pogled na pravne definicije je zaradi krajšega prispevka poenostavljen, kar pa za bralca ne pomeni ničesar slabega. Avtor skuša bralcu približati pravno zapleten pojem včasih tudi na poljudni način zaradi lažjega študija drugih predmetov s področja varstvoslovja ter zaradi potrebe po osnovnem razumevanju pravnega kategorialnega aparata.

Praktična uporabnost:

Prispevek je praktično uporaben za tuje, angleško govoreče študente, ki praviloma ne študirajo prava. Kljub temu lahko spoznajo temeljne pravne pojme,

ki so uporabni v večini družboslovnih raziskav. Opredelitve pojmov so korektne in sodobne, zato prispevajo k večanju znanja na tem področju.

Izvirnost/pomembnost prispevka:

Prispevek je pregledni znanstveni članek, zato je njegova izvirnost omejena. Avtor namreč ne postavlja znanstvenih spoznanj na novo, pač pa povzema in opredeljuje tisto, kar je že znano. Izvirna vrednost prispevka je v tem, da avtor postavlja temeljne pravne pojme in definicije v berljiv in lahko razumljiv kontekst, ki si jih bo bralec zapomnil. Definicije pravnih pojmov, prikazanih v članku, so točne ter uporabne in bodo marsikateremu bralcu prišle prav pri nadaljnjem študiju ali raziskovanju.

UDK: 34(497.4)

Ključne besede: pravo, pravni red, morala, sistemizacija prava, viri prava, pravna norma, zakoni, *lex specialis*

1 INTRODUCTION

Law is a system of rules and principles that, within the boundaries of legal regularity, regulate the vitally important external conduct and behaviour of the subjects in a state-organised society (Pavčnik, 2017).

This definition of law is not universal. Many different definitions can be found in contemporary critical jurisprudence (Flander, 2012).

The science dealing with law is legal science. Legal science comprises several fields. Legal history, for instance, deals with the applicable law of the past, whereas the focus of interest of the science of positive law is the law that is currently applicable. Legal science is divided into the legal sciences of individual fields of law or legal disciplines. Legal science studies various levels of law: e.g. legal dogmatic deals with its normative structure, the sociology of law observes law as a social phenomenon, the politics of law evaluates its normative elements, and legal theory determines what the general legal terms and general rules are (Pavčnik, 2017). Positive law is law laid down that applies to a certain territory at a certain time (Bradač, 1990). The Latin expression *de lege lata* means the law as it exists. It is usually used with the Latin expression *de lege ferenda*, which means what the law should be.

The applicable law can be adopted internal law, i.e. national law, or adopted external law, i.e. international law. Positive law applies to a certain territory at a given time. It always applies in advance and thus must be adopted beforehand in legally determined forms of legal acts.

Natural law is the opposite of positive law. Natural law comprises the rights held by every human being based on the natural order of things, i.e. as a human being. Natural law originates in nature. It is in the nature of humans that through their consciousness and freedom they perceive with their minds the sensible natural order as a source of principles, which they must realise in their own existence. Modern natural law – proceeding from a modern understanding of science – strives to avoid the above-mentioned problem and attempts to be

constituted as rational natural law. It considers a human being as a rational being, but also a being of interests and needs.

2 LEGAL ORDER OR LEGAL SYSTEM

A legal system or legal order is the integrated whole of the hierarchically regulated principles of law, rules and general legal acts which apply in a particular country, are published, and enter into effect from a certain date following their adoption.

The term legal order is used as a synonym for the term legal system. A legal order reflects the entirety of the mutually connected normative and factual elements, which are reflected in legal relations. A legal order encompasses the law applying at a specific time, defined in advance, in effect for a certain territory of a given country. The elements of the legal order are the principles of law and legal rules.

The factual elements of a legal order are the legally relevant facts (e.g. the relevant course of time, the fulfilment of a condition) and the legally relevant behaviour and conduct of legal subjects, which have legal consequences. The connecting elements of the legal order and the practical application of the law entail legal relations. They are defined in Part II of this article as the basic form of the application of the law in practice.

The legal order is based on the presumption that "being ignorant of the law harms" (*ignorantia iuris nocet*). This means that claiming that one does not know the principles of law, rules and general acts does not result in exculpation. The excuse that there was a mistake of law, which is another term for being 'ignorant of the law', is usually not a recognised defence (Cancik & Schneider, 2003). Legal certainty assumes that all subjects are aware of the law. Therefore, no one can seek to excuse their unlawful conduct by stating they were unaware of a certain rule or that such conduct was not allowed. In exceptional circumstances, a mistake of law can be the basis for exculpation, but only within the scope of criminal law.

Regardless of the above-mentioned exception, a legal order is based on the presumption that being ignorant of the law harms. Thus, every person must know the law, as every person bears the consequences of being ignorant of the law.

2.1 The Systemisation of Law

A further characteristic of the systemisation of law are basic double divisions (Tičar, 2012). In this sense, the law is divided as follows: external and internal law, civil and common law, substantive and formal law, private and public law.

International or external law is a set of principles and rules which regulate the behaviour and conduct of countries and international organisations (e.g. the United Nations, the Red Cross, and UNICEF). It comprises diplomatic and consular law, international law of the sea, the law on good-neighbourliness, as well as the law of war and international humanitarian law. One characteristic of international law is that in cases of violations of its rules there is no organisation which can impose direct coercive sanctions on subjects who have violated them.

However, the violation of international law rules can trigger or be a cause for unarmed or even armed interstate conflict; in other words, a war.

National law comprises a different set of rules than international law. Such rules consist of national state principles and rules which only apply in the territory of a certain state; they also regulate the behaviour and conduct of state authorities, local community authorities, citizens, foreigners, and all legal entities in a certain state territory. With its coercive apparatus (i.e. police, armed forces), a state has a monopoly over and absolute authority regarding the imposition of sanctions for violations of the state's rules.

Law in Europe has developed historically according to two concepts, namely the Continental European concept of civil law, and the Anglo-Saxon concept of common law.

The concept of codified, positive law is the basis for regulating the legal systems of the countries of Continental Europe. This includes all the countries of Central Europe, the countries on the Iberian Peninsula, the Scandinavian countries, and the countries of Eastern and Southern Europe. In Continental Europe, it is positive law that is codified in applicable legal acts.

Unlike the concept of codified law, the concept of unmodified law is based on precedents. Such a system can be found in the United Kingdom and in countries whose legal heritage may be traced to the United Kingdom, i.e. its former colonies. Common law is not based on formal sources of law, but on court decisions adopted in similar cases. These are known as precedents.

Precedents are judgements of the highest courts in Anglo-American law (i.e. the common law). The rationale for a decision in an individual case (i.e. *ratio decidendi*) has the effect of a general and abstract legal rule. Such a precedent when deciding on subsequent cases with similar issues binds the court which adopted the precedent, as well as the lower courts. Common law based on precedents arose as the courts had to carry out integrative and law-creating functions, which in Continental European law is reserved for the legislative branch of power (Perenič, 2007).

The main criteria for the substantive regularity of any modern law, be it civil or common law, are human rights. They are a universal and constituent part of the legal orders of all democratic countries.

Law can also be divided into substantive and formal law. Substantive law determines the substance of the rights, obligations and legal entitlements of subjects under law. Formal law regulates the organisation and procedures regarding the judicial conduct of legal subjects.

Within the Continental European concept of law, both substantive and formal laws comprise legal rules and principles which are written in legal regulations.

Substantive law entails all the legal rules which determine the substance of the rights, obligations and legal entitlements of subjects, and are static. Substantive law consists of several different laws in which the substantive rights, obligations and legal entitlements of legal subjects are determined.

Formal law determines the organisation and powers of state authorities and other aspects of public administration as well as all general and special rules of legal procedures. Procedural law, i.e. procedural formal law, is dynamic. It

determines the actions of legal subjects in order to ensure enforcement of the rights and obligations whose substance is determined in substantive law.

In addition to substantive rights and obligations, in legal procedures subjects have procedural rights and obligations. The latter are intended for the lawful exercise of procedural acts.

It is only when all substantive and procedural rights and obligations are entirely respected that this can result in a legally binding decision, which constitutes the individual rights or obligations of individual subjects.

The final, traditional division of law is into private and public law (also see Hess-Fallon & Simon, 2003). The development of the division of law into public and private law dates back to the ancient Roman state when public matters were interwoven with private interests and vice versa. At the same time, coercive authority as a public matter was also subordinated to the private interests of those who held power. The main law that developed in those times was private law, primarily contract law.

Only a small number of institutions and rules referred to public matters. Public matters were those in which, apart from private interests, there was also the interest of the state. The classical Roman jurist Domitius Ulpianus (Kranjc, 2018) named this *law ius publicum.* Ulpianus (in Stojčević & Romac, 1984) wrote: Public law is concerned with the organization of the [Roman] state, while private law is about the well-being of individuals. – Ius publicum est quod ad statum rei publicae spectat, privatum autem quod ad singulorum utilitatem; Ulpianus thus developed the division of private and public law which remains intact in legal systems today (Stojčević & Romac, 1984).

Private-law relations are chiefly contractual relations. This entails that dispositive rules (i.e. *ius dispositivum*) apply to such. The free will of the contractual parties has precedence over state regulation. Only if the contractual parties do not agree is the law applied. Such application of the law is secondary, i.e. subsidiary.

2.2 Law and Morals in General

Norma means a rule (Bradač, 1990). Therefore, the term system of norms is a synonym for the term system of rules. In addition to law, which is a normative system of rules sanctioned by the state, there exist other normative systems in society. These include moral rules, general social, personal and family rules, the rules of religious communities and church rules, the special rules of voluntary associations, etc.

The word morals derives from the Latin word *mos*, meaning custom (plural *mores – customs*). Morals entail a person's attitude to the world, other people and towards himself or herself. In a normative system, morally relevant actions are assessed as either good or bad. What is good is morally correct and what is bad is morally incorrect (Meško, Eman, & Flander, 2016). Morals comprise the values and customs of the people in a given society. In general, morals include unwritten rules, which apply not only to individuals, but also to the entire society. Law should include the most important moral rules and thus represent the minimal moral code.

It holds true for all the above-mentioned normative systems, which are not legal systems, that in cases of the violation of their rules the imposed sanctions never entail the use of state coercion. For instance, if a person violates a moral rule, a negative consequence of or sanction for such violation is contempt, social devaluation, the loss of one's good reputation, etc. If a person violates a family rule, other family members impose sanctions on them such that they feel bad, they lose a certain benefit, or have a bad conscience (e.g. if children breach family rules, they might not be given pocket money by their parents). If a member of a religious community violates a church rule (e.g. one of the Ten Commandments, which is a sin in the Catholic Church) a sanction is imposed transcendentally. The person is punished after their death by being sent to hell instead of heaven. In comparison with the rules of other coexisting social normative systems, legal rules are the only ones whose violation results in the imposition of a coercive sanction by the state. Such is executed here and now. With its coercive apparatus, the state namely punishes a person who has violated a certain rule by imposing, for instance, a fine, a prison sentence or in certain countries even the death penalty. Certain rules can naturally be legal, moral and church rules all at once. For instance, if the rule "do not kill" is breached, this results not only in a legal sanction (e.g. a prison sentence), but also in a moral (e.g. contempt) and church sanction (e.g. punishment in the hereinafter for having committed a deadly sin).

In substance, modern positive law rules are general and abstract on one hand, and concrete and individual on the other. Regulations are general and abstract, whereas contracts and decisions, which create direct rights and obligations of legal subjects, are concrete and individual.

3 SOURCES OF SLOVENIAN LAW

Sources of law are mutually connected legal elements necessary for the existence of a legal phenomenon (Bohinc, Cerar, & Rajgel, 2006). Sources of law may be direct or indirect. The former comprise legal regulations and customs, while the latter include case law and legal science.

Sources of law may be formal or informal. In Continental legal systems, regulations (*leges*) are formal normative acts, whereas customs are informal normative acts. Collections of customs are termed usages.

Laws (*leges*) are legal acts which are formal, general, abstract and published. The principal sources of Continental European law are regulations. The general nature of regulations entails that they apply to everyone. All are equal before the regulations and regulations must apply equally to all. The abstract nature of regulations means they refer to undetermined yet envisaged social relations.

Regulations must be adopted and published in a manner prescribed by law, which is described below in the section dealing with the principle of legality. The regulations also have different mutual relations. Their correct application is ensured by three binding rules of interpretation.

The principal regulation is a law discussed in more detail in the section below dealing with the legal acts of the legislature. In the legal system, a law is applied in such a manner that in cases where the same legal relation is regulated by a general

and a special law the regulation of the special law prevails (*"Lex specialis derogat legi generali"* – Stojčević & Romac, 1984, p. 262).

In cases in which an earlier and a more recent law govern the same relation, the more recent law prevails (i.e. *lex posterior derogat legi priori*). With reference to such, special laws hold priority over general laws. A later general law thus does not prevail over the earlier special law (*lex posterior generalis non derogat priori speciali*).

The rule that a higher regulation is stronger than a lower regulation (*lex superior derogat legi inferiori*) entails the rule of the supremacy of a higher regulation over a lower regulation. However, when applying regulations in practice, this is less important as the consistency of lower regulations with higher regulations is decided primarily by the courts. If such court proceedings are not initiated, the parties involved must respect the legal regulations as adopted until the Constitutional Court abrogates or annuls them with its decision or until the state authority which adopted the regulations amends or repeals them.

In the following text, the types of regulations will be introduced from the viewpoint of which authority adopts and issues them.

4 IMPACT OF THE EU LEGAL SYSTEM ON THE SLOVENIAN LEGAL SYSTEM

The supremacy of EU law means the legal acts of the EU prevail over those of the member states. In accordance with Article 10 of the Treaty establishing the European Community, which determines that member states must take all appropriate measures in order not to jeopardise compliance with EU law, every violation of EU law by the authorities of any member state also involves a violation by the state itself.

Before joining the EU, candidate states had to align their body of national law with EU law and had to correctly apply it from the day of becoming a member of the EU. As a special type of a supranational organisation, the EU does not have any bodies in the member states in the form of ministries or branch offices for implementing the decisions of EU institutions, therefore the state authorities of the member states are tasked with implementing EU policies and EU law. Within the framework of EU law, there is a distinction between primary and secondary sources of EU law.

The primary sources of EU law are the founding treaties with all the subsequent amendments, annexes and protocols; the treaties of accession of new EU member states with annexes and protocols; and agreements with third countries.

Secondary sources of EU law are the regulations, directives, decisions, recommendations and opinions of the EU. The difference between these acts is whether they are binding or not, whether they are general or individual, whether they must be transposed into national law, etc.

As general binding acts, regulations and directives interfere to the greatest extent with the national laws of the member states and with the position of individuals. There are important differences between a regulation and directive.

A regulation can be compared with a law – it is directly applicable in its entirety and does not need to be transposed into the national law of the member states.

A directive typically cannot be applied directly, contrary to what applies for EU regulations. A directive can be addressed to all or only certain member states, which must then transpose the content and objectives of the directive into their national law by means of binding regulations of the national legal order in light of the objectives pursued by the directive; however, the choice of form and methods for achieving such is left up to the national authorities of the member states involved. A directive is thus binding as to the result to be achieved in each member state to which it is addressed, but leaves the national authorities with the choice of form and methods. A directive requires the action of the national legislative body, which must transpose it into national law, whereby the legislature must ensure that the national legislation conforms with the requirements of the directive, which entails that a national regulation not in conformity with the directive must be amended or that a new regulation be adopted in cases in which, for example, a directive regulates an area which is not yet regulated in the national legislation.

5 GENERAL LEGAL ACTS IN THE REPUBLIC OF SLOVENIA

The Constitution of the Republic of Slovenia (Ustava Republike Slovenije, 1991) is a fundamental general, normative legal act in Slovenia adopted by the legislature by a two-thirds majority vote. The legislature is in this case the constitution framer. The Constitution contains principles and rules of the highest legal importance. The principles contained in the Constitution are the foundation of the activities of all citizens, state authorities, local communities, legal entities and foreigners in the territory of the state. Laws (i.e. constitutional acts, statutes, etc.) are a fundamental direct source of law. Laws regulate fundamental social issues that are important for the legal order. Laws are subordinate to the Constitution and superior to other laws in the country (Tičar, 2012).

Laws regulate the content of the Constitution in more detail. The content of the Constitution is generally not directly applicable to the regulation of concrete and individual legal relations, except in the field of human rights.

Laws have a double guarantee (Čebulj & Stermecki, 2005):

- the guarantee of the applicability of a law entails that only the legislature has the constitutional authority to prescribe rights and obligations in the country (and to amend and abrogate them); and
- the guarantee of the existence of a law means the existing law cannot be abrogated other than by a new law, which must be a regulation on the same or a higher level.

Laws are a fundamental source of law. This also proceeds from the Constitution, in accordance with which the rights and duties of citizens and other persons may be determined by the National Assembly only by law. With reference to such, it must be emphasised that implementing regulations and other general legal acts must be in conformity with the Constitution and laws. Further,

individual acts and actions of state authorities, local community authorities, and bearers of public authority must be based on a law or regulation adopted pursuant to law.

Treaties ratified by the National Assembly are applied directly and are thus a source of law. In addition to the above-mentioned treaties, other ratified treaties are sources of law. Laws must comply with the former treaties, whereas implementing regulations and other general acts must comply with the latter.

On top of the Constitution and laws, the National Assembly of the Republic of Slovenia adopts the state budget, declarations and resolutions, national programmes, ordinances, recommendations to the Government and other state authorities, authentic interpretations of laws, the Rules of Procedure of the National Assembly, and decisions.

The National Assembly also adopts programmatic documents. These are national programmes for the future development of individual policies, declarations stating general positions on domestic and foreign policy issues, resolutions evaluating the state of affairs and problems in society, recommendations, opinions and guidelines comprising proposals for the work of national authorities, and authentic interpretations of laws adopted by the legislature itself (Grad & Kaučič, 2008).

5.1 General Legal Acts of the Slovenian Government

The Government adopts the most frequent implementing acts called decrees. Decrees are the most important general, implementing regulations issued by the Government. By decree, the Government regulates in detail and defines certain relations determined in a law or another act of the National Assembly in line with the purpose and criteria of the law or another regulation. The Law of Government determines that a decree on the exercise of the rights and obligations of citizens and other persons may only be issued in accordance with an express authorisation in a law.

By a decree, the Government defines certain relations determined in a law. Decrees are hierarchically lower than laws. The Government of the Republic of Slovenia does not have legislative authority based on which it can directly affect the rights and obligations of individuals. Only a law can constitute, reconstitute or abolish the rights and obligations of individuals.

The Government does not need any special statutory authorisation to adopt independent decrees and may adopt them independently. These are organisational decrees by which the Government regulates in greater detail the internal structure of the administration and work processes in the administration.

The Government adopts interpretational or explanatory decrees based on a general statutory authorization, i.e. a general clause. The Government adopts interpretational or explanatory decrees in instances in which it assesses that more detailed operationalization of the provisions of a certain law is needed for the implementation of such.

Supplementary decrees are not independent. The Government must adopt such based on a special statutory authorization or an executive clause. Decrees

supplement a law in a manner such that they define certain statutory rules whereby they may not interfere with the statutory subject matter, which is a domain reserved for the legislature.

By an ordinance, the Government regulates individual issues or adopts individual measures of general relevance. Furthermore, it adopts other decisions for which it is determined by a law or decree that are regulated by a Government ordinance.

Through the budget memorandum, the Government presents to the National Assembly the fundamental objectives and tasks of the economic, social, and budget policy of the Government and the global frameworks of overall public finances for the following year.

By a strategy for regional development in Slovenia, the Government determines objectives, policies, and tasks with regard to regional development in Slovenia. The Government regulates its internal organization and work by its Rules of Procedure. The Government issues decisions on appointments and dismissals, in administrative matters within its competence, and on other specific matters within its competence. The Government issues an order whenever it does not decide by any other act.

5.2 General Legal Acts Issued by Slovenian Ministers

Ministers issue rules, ordinances, and instructions for the implementation of laws, other regulations, and acts of the National Assembly and regulations and acts of the Government. It proceeds from the above-mentioned that this concerns implementing acts which are based on some higher regulation and that their substance proceeds from them. In addition, from the above-mentioned it can be concluded that there are two groups of regulations: the first group is issued for the implementation of laws, other regulations, and acts of the National Assembly, whereas the second group is issued for the implementation of regulations and acts of the Government (Tičar & Rakar, 2011).

Rules are the most important legal act issued by a minister. Rules define individual provisions of a law, some other regulation, or an act on its implementation. Measures of general relevance are determined by an ordinance. The contents of an ordinance regulate an individual situation of general relevance. An instruction prescribes the manner of implementing individual provisions of a law, other regulation, or act. An instruction thus mainly regulates issues of a technical nature. When deciding on administrative matters, ministers and heads of departments within ministries issue orders and decisions.

5.3 General Legal Acts of Slovenian Municipalities

Local matters which municipalities may regulate independently and which concern only the residents of a certain municipality fall within the competence of the given municipality. Legal acts that are adopted by municipalities are primarily statutes, rules of procedure, and decrees. These types of acts are the most common ones. Furthermore, municipalities adopt budgets; they may also adopt ordinances, rules, and instructions.

A municipality, more precisely a municipal council, adopts statutes. The statutes of a municipality determine the basic principles of the organization and operation of the municipality; the establishment and competence of municipal bodies; the manner of participation of members of the municipality in adopting decisions by the municipality; and other issues of common interest in the municipality as determined by law (Tičar, 2012).

A municipality regulates matters from its competence by municipal decrees. A municipality regulates matters from its vested competence by decrees and other regulations determined by law. Rules of procedure regulate the organization and work of municipal councils as well as the procedure for adopting decrees and other general acts.

6 INDIRECT SOURCES OF SLOVENIAN LAW

In addition to general legal acts, customary law and case law (*usus fori*) are supplementary and additional sources of law. In general, it can be noted that in the Republic of Slovenia the importance of customary law is relatively insignificant. Customary law is a supplementary source and can be applied only in the event of a gap in the law.

Objective and subjective reasons must naturally be taken into consideration in cases in which case law is applied in practice. From an objective point of view, this is a means, which ensures the uniform application of law.

Attention must furthermore be drawn to a special type of source of law, i.e. the decisions of the Constitutional Court of the Republic of Slovenia, especially in cases in which the Court acts as a negative legislature and abrogates unconstitutional statutory and implementing norms (Tičar & Rakar, 2011).

Any person suffering harmful consequences due to a regulation or general act which has been annulled by an individual act issued on the basis of such is entitled[1] to request that the authority which decided in the first instance change or annul that individual act. If such consequences cannot be remedied, the entitled person may claim compensation in a court of law.

With reference to Constitutional Court decisions, attention must also be drawn to its interpretative decisions, i.e. decisions in which the Court does not decide that the provisions of the challenged act are inconsistent with the Constitution or a law, but determines in the operative provisions of the decision in which manner they must be interpreted in order to ensure their application in individual cases is consistent with the Constitution.

7 CONCLUSION

In the present article, we have defined some basic elements of Slovenian formal law. This kind of law determines the organisation and powers of the state through

1 *[…] within three months of the day of publication of the Constitutional Court decision, provided no more than one year has elapsed from the service of the individual act till the lodging of the petition or request.*

laws (*leges*), governmental decrees and ministerial rules. Formal law covers the competences of state authorities as well as all general and special rules of legal procedures.

We may also conclude that law is a historical and civilizational phenomenon. Its development began with the emergence of civilisation and as contemporary legal writers say: It continues to develop today (Cerar, 2001).

There are numerous theories and points of view regarding what constitutes the essence of law. Immanuel Kant, for instance, claimed in his lifetime that lawyers are still looking for the essence of their law (Perenič, 2007). Legal theoreticians have still not agreed on a uniform definition of the essence of law. Law can also be understood instrumentally (*instrument* – a tool). Instrumental law is a tool prescribed in advance composed of rules suitable for preventing and resolving conflicts between subjects in society.

Finally, as stated above for the decisions of Slovenian courts, the judgements of the European Court of Human Rights in Strasbourg and the Court of Justice of the European Union in Luxembourg (i.e. the Court of Justice and the General Court – with the latter, judgements are issued in preliminary ruling proceedings, which are a source of law in the individual cases in which they were issued, are in this regard the most relevant) must be considered as a source of law within the framework of administrative proceedings and decision-making.

REFERENCES

Bohinc, R., Cerar, M., & Rajgel, B. (2006*). Temelji prava in pravne ureditve* [The basis of law and legal regulation]. Ljubljana: GV Založba.

Bradač, F. (1990). *Latinsko-slovenski slovar* [Latin-Slovene dictionary]. Ljubljana: Državna založba Slovenije.

Cancik, H., & Schneider, H. (Eds.) (2003). *Der neue Pauly: Enzyklopädie der Antike* [The new Pauly: Encyclopedia of antiquity]. Stuttgart: J. B. Metzler.

Cerar, M. (2001). *(I)racionalnost modernega prava* [(I)rrationality of modern law]. Ljubljana: Bonex.

Čebulj, J., & Strmecki, M. (2005). *Upravno pravo* [Administrative law]. Ljubljana: Fakulteta za upravo.

Flander, B. (2012). *Kriza prava: Odbleski kritične jurisprudence* [Crisis of law: Echos of critical jurisprudence]. Ljubljana: Fakulteta za varnostne vede.

Grad, F., & Kaučič, I. (2008). *Ustavna ureditev Slovenije* [The constitutional system of Slovenia]. Ljubljana: GV Založba.

Hess-Fallon, B., & Simon, A. M. (2003). *Droit civil* [Civil right]. Paris: Éditions Dalloz.

Kranjc, J. (2018). *Rimsko pravo* [Roman law]. Ljubljana: GV Založba.

Meško, G., Eman, K., & Flander, B. (Eds.) (2016). *Oblast, legitimnost in družbeno nadzorstvo* [Power, legitimacy and social control]. Ljubljana: Fakulteta za varnostne vede.

Pavčnik, M. (2017). *Teorija prava: Prispevek k razumevanju prava* [Theory of Law: Contribution to the understating of the law]. Ljubljana: IUS Software, GV Založba.

Perenič, A. (2007). *Uvod v razumevanje države in prava* [An introduction to the understanding of the state and the law]. Ljubljana: Fakulteta za varnostne vede.
Stojčević, D., & Romac, A. (1984). *Dicta et reguale iuris*. Beograd: Savremena Administracija.
Tičar, B. (2012). *Understanding law and the state*. Maribor: Inštitut za lokalno samoupravo in javna naročila.
Tičar, B., & Rakar, I. (2011). *Pravo javnega sektorja* [Public sector law]. Maribor: Inštitut za lokalno samoupravo in javna naročila.
Ustava Republike Slovenije [The Constitution of the Republic of Slovenia]. (1991, 1997, 2000, 2003, 2004, 2006, 2013, 2016). *Uradni list RS*, (33/91, 42/97, 66/00, 24/03, 69/04, 68/06, 47/13, 75/16).

About the Author:

Bojan Tičar, PhD, Full Professor of Law at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: bojan.ticar@fvv.uni-mb.si

VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 20 no. 4 pp. 462–475

User Violence Against Employees at Nursing Homes

Katarina Cesar, Liljana Rihter, Špela Selak, Branko Gabrovec

Purpose:

Earlier research has indicated the high exposure of those working in assisting occupations to workplace violence in Slovenia. The purpose of this study is to complement the research gap in investigating violence within social care and determine the types and extent of workplace violence among all employees in a social care institution, the influence of aggressive behaviour of users on the well-being of employees, and the need for education on dealing with the violence to which employees are being exposed.

Design/Methods/Approach:

Workplace violence was researched quantitatively using a descriptive method. We used a structured survey questionnaire, which was adapted using an existing questionnaire to research the occurrence of violent acts from users against employees at nursing homes and other social care institutions.

Findings:

The nursing home *Dom ob Savinji Celje* faces user violence against its employees. The most frequent form of violence against employees is verbal abuse (37.7% of respondents) and the least frequent is unwanted conduct of a sexual nature (5.2% of respondents). Workers employed in healthcare face user violence more often than employees in other fields. Employees most often face a certain form of user violence 1-2 times per year. When an employee meets an aggressive user, the most common emotions are fear, helplessness, uncertainty, feeling under threat, and least often a lack of understanding from fellow employees.

Originality/Value:

This study focuses on studying workplace violence within a social care institution and complements extant, yet inadequate scientific findings.

UDC: 343.62:614

Keywords: nursing homes, workplace violence, healthcare, social care, social care institutions

Nasilje uporabnikov nad zaposlenimi v domovih za starejše ljudi

Namen prispevka:

Predhodne raziskave v Sloveniji nakazujejo na visoko izpostavljenost nasilju na delovnem mestu med poklici, katerih temeljna naloga je pomoč in oskrba ljudi.

Namen pričujoče raziskave je zapolniti raziskovalno vrzel proučevanja nasilja v kontekstu socialnega varstva ter ugotoviti vrste in razširjenost nasilja na delovnem mestu med vsemi zaposlenimi v socialnovarstvenem zavodu, vpliv agresivnega vedenja uporabnika na počutje zaposlenih in potrebo po izobraževanju o ravnanju v primeru nasilja uporabnikov, ki so mu izpostavljeni zaposleni.

Metode:

Izvedena je bila kvantitativna raziskava s področja nasilja na delovnem mestu, z uporabljeno deskriptivno metodo. Uporabljen je bil strukturiran anketni vprašalnik, prilagojen na podlagi obstoječega vprašalnika za raziskovanje pojava agresivnih dejanj uporabnikov nad zaposlenimi v domovih za starejše ljudi in drugih zdravstvenih zavodih.

Ugotovitve:

V Domu ob Savinji Celje se soočajo z nasiljem uporabnikov nad zaposlenimi. Oblika nasilja uporabnikov nad zaposlenimi, s katero se je soočilo največ zaposlenih, je verbalno nasilje (37,7 % anketirancev), najmanj pogosto pa neželeno vedenje spolne narave (5,2 % anketirancev). Z nasiljem uporabnikov se pogosteje srečujejo zaposleni na področju zdravstvene nege kot zaposleni na drugih področjih. Zaposleni se z določeno obliko nasilja uporabnikov najpogosteje srečajo 1–2x letno. Ko se zaposleni sreča z uporabnikom, ki je agresiven, se ob tem najpogosteje sooča z občutkom strahu, nemoči, negotovosti in ogroženosti, najredkeje pa občutijo nerazumevanje sodelavcev.

Izvirnost/pomembnost prispevka:

Pričujoča raziskava se osredotoča na proučevanje nasilja na delovnem mestu znotraj socialnovarstvenega zavoda in dopolnjuje obstoječa, še vedno pomanjkljiva, znanstvena dognanja.

UDK: 343.62:614

Ključne besede: domovi za starejše ljudi, nasilje na delovnem mestu, zdravstveno varstvo, socialno varstvo, socialnovarstveni zavodi

1 INTRODUCTION

Violent acts aimed at social care personnel at the workplace are on the rise (Gabrovec, 2017). Workplace violence can be defined as any act of physical violence, harassment, intimidation, or other threats that disturb the working process of a given worker and can include employees as well as users and visitors (Occupational Safety and Health Administration [OSHA], 2008). Workplace violence can thus be understood not just as exposure to physical attacks but as all types of abuse, intimidation, or attacks on employees related to their work which directly or indirectly influences their safety, well-being, or health (Bowie, 2002). This includes all types of behaviour, be it verbal or physical violence, causing either physical or psychological damage (Možina, 2009). The most common characteristic exhibited by perpetrators of workplace violence is altered mental status associated with dementia, delirium, substance intoxication, or

decompensated mental illness (Occupational Safety and Health Administration [OSHA], 2015; Pompeii et al., 2013).

There are several different definitions of violence, depending on the person defining it and the purpose of the definition (World Health Organization [WHO], 2002). In a broader sense, violence can be defined as an abuse of one person's power that adversely affects another (Društvo za nenasilno komunikacijo, n. d.) or as a deliberate use of physical force or power (the actual use or its use to make threats) against oneself, against another person, or against a group or community that is consequently very likely to cause an injury, death, psychological harm, a sense of devaluation, or detraction (WHO, 2002). It must be emphasized that different types of violent behaviour are often interrelated and not independent; the presence of one type of violent behaviour (e.g. psychological) can trigger the occurrence of another (e.g. physical) (Gabrovec, Eržen, & Lobnikar, 2014). Preventing violence at workplace especially in healthcare is a challenge and priority (NHS Employers, 2014; OSHA, 2015). Different forms of violence can be defined more narrowly. In Slovenia, the Domestic Violence Prevention Act (Zakon o preprečevanju nasilja v družini, 2008) defines physical violence (any use of physical force which causes pain, fear, or humiliation for a family member regardless of the resulting injuries); sexual violence (actions with sexual content that are opposed by the family member who is forced to do them or does not understand their meaning due to their current developmental stage); psychological harassment (actions of a perpetrator of violence that cause fear, humiliation, a sense of inferiority, hazard, and other types of mental distress); economic violence (unjustified control or limitation of a family member with income or asset distribution by which the family member possesses or manages independently or exercises unjustified limitation or management of family members' common wealth); and negligence (a type of violence where a person abandons obligated care for a family member that needed due to a sickness, disability, age, development, or other personal circumstances). It must be emphasized that different types of violent behaviour are often interrelated and not independent; the presence of one type of violent behaviour (e.g. psychological) can trigger the occurrence of another (e.g. physical) (Gabrovec et al., 2014).

1.1 Prevalence of Workplace Violence Against Healthcare Employees

Several studies have been carried out to date on the topic of violent user behaviour in Slovenian healthcare (e.g. Gabrovec, 2017; Kelbič, 2013; Klemenc & Pahor, 1999; Košir, 2012; Kvas & Seljak, 2015; Planinšek & Pahor, 1999) and recently, other studies on social care have followed this trend (e.g. Cink, 2008; Gabrovec & Eržen, 2016; Koprivnik, 2002;). Nursing care providers are considered to be employees who are the most exposed to workplace violence in healthcare (Koprivnik, 2002). The findings of the first study on violence against healthcare employees in Slovenia (Klemenc & Pahor, 1999) indicate a violent experience at the workplace for 72.3% of nurses; 72.3% of the respondents experienced verbal, 59% psychological, and 29% physical violence. Further research findings using the same sample indicate an experience of sexual workplace violence for 34.8%

of respondents employed in healthcare (Planinšek & Pahor, 1999). The findings of later research on workplace violence in Slovenia also show its high prevalence. In a study on emergency medical care (Kelbič, 2013) 98% of respondents reported that they had already experienced one of form of workplace violence. The study conducted one year later (Kvas & Seljak, 2015) reported that 60.6% of healthcare providers included in the sample had been exposed to workplace violence, most frequently to verbal abuse (60.1%). The presence of psychological harassment was found in a study that included employees from all healthcare fields. 60.1% of them reported psychological harassment at the workplace (Babnik, Štemberger Kolnik, & Kopač, 2012). All studies on violence against healthcare employees share a common finding, namely that they are exposed to workplace violence to a considerable extent in all fields, especially in intensive psychiatric healthcare (Gabrovec, 2017), where 92.6% of nurses experienced at least verbal abuse, 84.2% of them experienced psychological harassment, and 63.5% were injured during their working life from users according to data from one study (Gabrovec et al., 2014). According to results (Košir, 2012), users can commit violence against healthcare workers in all fields to a large degree (in 74.8% of the cases in the referred study).

There is a significantly lower number of studies on workplace violence in social care than in healthcare (Možina, 2009). One Slovene study (Cink, 2008) reported that the majority of the surveyed expert social care workers had already experienced verbal abuse; according to results, 81.52% of respondents had experienced workplace violence (violent client) in the last 12 months, 90.66% reported verbal abuse, 1 person reported physical violence, and 5 people reported verbal and physical violence. Furthermore, the results of a study at a social care institution (Koprivnik, 2002) indicate that healthcare employees often meet physical and verbal abuse and these results coincide with the following findings of previous studies: employees are more exposed to verbal than physical abuse; 95% of respondents who were exposed to verbal abuse reported shouting and negligence from inmates. The findings of a recent study on the occurrence of violence aimed at healthcare employees in Slovenian nursing homes (Gabrovec & Eržen, 2016) highlight the exposure of healthcare employees in nursing homes to violent acts. In the last 12 months, 71.1% of respondents reported verbal abuse, 63.8% physical violence, and 25.5% sexual harassment; 36.8% of all respondents were injured by their patients. When employees were faced with aggressive behaviour of users, they most often felt vulnerable, afraid, and uncertain, while they felt angry with a user or lacked understanding from co-workers the least often. Anger was among the least frequent feelings in the studies by Gabrovec and Eržen (2016) and Cink (2008), which dealt with respondents exposed to violent acts of users.

Although the data indicate a growing trend for the prevalence of workplace violence, many incidents still remain unreported; according to one study (Stokowski, 2010) in more than 70% of the cases. This means that the actual percentage of violent incidents at the workplace is probably much higher than the recorded percentage (Gates, Gillespie, & Succop, 2011). An individual organisation can contribute to this by influencing the establishment of a safety culture and developing systematic training models with prescribed precautions

to assure safety and prepare a protocol to be used in case of violent situations (Gabrovec & Eržen, 2016).

The presented results of previous studies indicate a high exposure of assisting healthcare occupations to workplace violence in Slovenia. Earlier and later studies come to similar conclusions, allowing us to assume that this field lacks the necessary attention, and that effective methods of preventing and facing user violence still have not been unidentified. The purpose of this study is to partially fill in the research gap in research on violence in social care and determine the types and extent of workplace violence among all employees in a social care institution, the influence of users' aggressive behaviour on the well-being of employees, and the need for education on dealing with violence to which employees are being exposed.

2 DESCRIPTION OF THE METHOD USED

2.1 Nursing Homes in Slovenia and Description of the Sample

Nursing homes offer professional protection for elderly people. Professional protection comprises all types of aid to the family and/or to the elderly person, by means of which functions at home and with his/her family are substituted or fulfilled to the clients, especially with regard to their dwelling, organized nutrition, security and health protection (Habjanic, 2009). Long term care in Slovenia is based on institutional settings, with too little support to help people to remain in their own homes (Normand, 2015). From 102 Slovenian nursing homes, the nursing home *Dom ob Savinji Celje* was chosen as it enables student working practice and conducting research in Savinjska region.

The study was carried out between 12 December 2017 and 31 December 2017 using a sample of 86 employees (except for employees of daily centre and home support centre) in the social care institution *Dom ob Savinji Celje*, which provides institutionalised care and services in users' living environments for up to 250 residents from the broader region of Celje. From 146 employees in the social care institution *Dom ob Savinji Celje*, 77 participated in the study. Participation in the survey was voluntary, and we provided all participants with anonymity and confidentiality.

75 (97.4 %) were women and 2 (2.6 %) were men. Median age was 42.96 years old, the youngest 19 years old, the oldest 60 years old. 5 (6.5 %) employees had 1 years or less working experience, 2 (2.6 %) employees stated that they have 40 years of working experiences. Largest share (11.7 %) employees has 15 years of working experience the social care institution *Dom ob Savinji Celje*. Due to the missing values, 9 units were excluded and the other 77 were included in the analysis. Our sample included 77 employees, 75 (97.4%) of whom were female and 2 (2.6%) male. This imbalance is largely the result of the uneven gender distribution among the employees at *Dom ob Savinji Celje*. The average age of respondents was 42.96 years (min = 19 years, max = 60 years). The participants averaged 18.22 years of professional experience (min = 1 year, max = 40 year). 66.2% of respondents were employed in healthcare and 33.8% of respondents in other fields.

2.2 Description of the Questionnaire and the Method

This was a quantitative study employing descriptive data analysis. A structured survey questionnaire was used as a metric. We adapted it based on an existing questionnaire to explore aggressive actions of users against nursing home and other healthcare institution employees (Gabrovec & Eržen, 2016) and used 12 variables with accompanying indicators and modalities. The structured survey questionnaire included 44 questions, divided into the following segments: 1) work and workplace violence (18 questions), 2) work organisation (7 questions), 3) influence of various factors on the safety of employees and patient treatment (8 questions), 4) field of education (6 questions), and 5) demographic data (5 questions). We used a 5-level agreement scale, where 1 signified the respondent's completely disagreement with the statement, and 5 meant that the respondent completely agreed with the statement.

2.3 Research hypothesis

Based on the reviewed literature and the purpose of the study, we set up the following hypotheses.

H1: "*The most common type of violence experienced by employees in nursing homes is verbal abuse*."
H2: "*Healthcare workers are exposed to verbal abuse more often than other employees."*
H3: "*Those who experienced physical violence evaluated their emotional state of fear more negatively than those who did not."*
H4: "*The majority of those who experienced physical violence at work assess that the available know-how on dealing with workplace violence is inadequate."*

The data was analysed using statistical software IBM SPSS Version 21 and IBM AMOS Version 21 (SPSS Inc., Chicago, IL, USA). The compiled data were processed by means of descriptive statistics and hypothesis tested with chi-square (χ^2) test and the Mann–Whitney U test. The significance level was calculated using the statistical significance value of $p < 0.05$. We checked the descriptive statistics and the relation between the variables; hypotheses were checked with a chi-square (χ^2) test. A significance level of $p < 0.05$ was used.

3 RESULTS

According to results (Table 1), 37.7% of respondents faced verbal abuse, 15.6% faced physical violence, and 5.2% unwanted user conduct of a sexual nature at their workplace in the previous year. Among the respondents who faced verbal abuse from a user in the previous year, the majority (62.1%) experienced it once or twice. The same applies for respondents (75%) who faced unwanted conduct of a sexual nature. The majority of respondents (58.3%) who faced physical violence experienced unwanted conduct of a sexual nature 3–5 times.

Table 1: Percentages of facing verbal abuse, physical violence and unwanted conduct of a sexual nature in the previous year

Frequency of encounters:	Verbal abuse (in %)	Physical violence (in %)	Unwanted conduct of a sexual nature (in %)
Total	37.7	15.6	5.2
1-2x	62.1	25	75
3-5x	34.5	58.3	25
6-9x	1.3	16.7	0
10x and more	0	0	0

According to the above data, we can confirm hypothesis H1, which states that employees face verbal abuse most frequently at their workplace.

We used a contingency table or a chi-square (χ^2) test to check hypothesis H2, which states that healthcare workers are exposed to verbal abuse more frequently than other employees.

Table 2: The contingency table of the relation between facing verbal abuse at the workplace from a user and at the workplace of healthcare workers

Did you face verbal abuse from a user at the workplace in the last year?					
			Your workplace		Sum of values
			Field of healthcare	Other	
Did you face verbal abuse from a user at the workplace in the last year?	YES	Number	24	5	29
		% within "facing verbal abuse from a user?"	82.8%	17.2%	100.0%
		% within "your workplace"	47.1%	19.2%	37.7%
		% of sum of values	31.2%	6.5%	37.7%
	NO	Number	27	21	48
		% within "facing verbal abuse from a user?"	56.2%	43.8%	100.0%
		% within "your workplace"	52.9%	80.8%	62.3%
		% of sum of values	35.1%	27.3%	62.3%
Sum of values		Number	51	26	77
		% within "Did you face verbal abuse from a user at the workplace in the last year?"	66.2%	33.8%	100.0%
		% within "your workplace"	100.0%	100.0%	100.0%
		% of sum of values	66.2%	33.8%	100.0%

The above table (Table 2) shows that 47.1% of employees in healthcare faced verbal abuse and merely 19.2% of employees from other fields. It follows that healthcare employees face verbal abuse more often. Then we used a chi-square (χ2) test to check whether the stated difference is statistically significant.

Before testing the third hypothesis H3 we were also interested in the feelings and emotional states that employees felt when facing an aggressive user. When facing an aggressive user, respondents most often felt fear (M = 3.65), helplessness (M = 3.38), uncertainty (M = 3.36), and hazard (3.36), and least often anger (M = 2.78), despair (M = 2.71), and lack of understanding from co-workers (M = 1.97).

Furthermore, we checked hypothesis 3, which states that those who experienced physical violence evaluated their emotional state of fear more negatively than those who did not. The results of the Shapiro–Wilk test ($W = 0.802$; $p = 0.01$) indicate an abnormal distribution (the data statistically differ from normal distribution) of the variable fear (if employees had faced physical workplace violence in the previous year). The analysis results of range values for the variable fear indicate that those workers who had faced physical violence from a user at the workplace ($N = 12$, $M_{rank} = 42.13$) gave higher average estimates of their level of fear and those workers who did not face physical violence gave lower estimates ($N = 65$, $M_{rank} = 38.42$). We thus established that there are differences between both groups. Furthermore, the results of the Mann–Whitney U test ($U = 352.0$, $z = -0.553$, $p = 0.580$) show (that the differences between the feeling of fear between both groups of employees who had or had not faced physical violence from a user are not statistically significant. On this basis, we can reject the third hypothesis 3.

Finally, we checked the fourth hypothesis, which states that the majority of those who experienced physical violence at work evaluate that the available know-how on dealing with violence is inadequate. The results of the Shapiro–Wilk test ($W = 0.786$; $p = 0.007$) indicate an abnormal distribution of the variable know-how (the know-how of the respondents was sufficient to control a violent user if employees had faced physical workplace violence in the last year). The analysis results of range values of the variable know-how indicate that those respondents who faced physical violence from a user at the workplace ($N = 12$, $M_{rank} = 39.08$) gave higher average estimates of their level of know-how, sufficient to control a violent user, and those workers who did not face physical violence gave lower estimates ($N = 65$, $M_{rank} = 38.98$). Based on these results, we determined that there are differences between both groups. Furthermore, the results of the Mann–Whitney U test ($U = 389.0$, $z = -0.016$, $p = 0.987$) show that the differences in the know-how between both groups of employed who faced or did not face user physical violence are not statistically significant. We can therefore reject the fourth hypothesis.

4 DISCUSSION

With this study conducted among the employees of the *Dom ob Savinji Celje* nursing home, we determined that there is ongoing user violence against nursing home employees. We confirmed the first two hypotheses (H1: The most common type of violence experienced by employees at their workplace is verbal abuse; H2: Healthcare workers are exposed to verbal abuse more often than other employees.) and rejected the other two (H3: Those who experienced physical violence evaluated their emotional state of fear more negatively than those who did not; H4: The majority of those who experienced physical violence at work assess that the available know-how on dealing with workplace violence is inadequate.). The majority of research participants faced verbal abuse at the workplace from a user. Fewer faced physical violence, and the fewest responded that they had faced unwanted user conduct of a sexual nature at the workplace. Similarly to previous ones (Cink, 2008; Gabrovec, 2017; Gabrovec & Eržen, 2016; Kelbič, 2013; Klemenc

& Pahor, 1999; Košir, 2012; Kvas & Seljak, 2015; Planinšek & Pahor, 1999), this study showed that employees are more exposed to verbal than physical abuse. We did not examine the reason for the low proportion of employees who had faced unwanted conduct of a sexual nature. In our opinion, one of the reasons could be the respondents' tolerance to this type of violence or the identification of sexual violence (Planinšek & Pahor, 1999). Some are for example already annoyed by improper looks or sexually-related comments regarding their appearance; others simply ignore such behaviour and choose not worry to over it, only defining sexual harassment as groping (Kuhar, Guzelj, Drolc, & Zabukovec, 1999). In Slovenia, the terms that define individual types of violence are still unclear. We usually only notice rough physical violence and largely ignore sexual, psychological, and verbal abuse (Klemenc & Pahor, 1999), which is a sign of demeaning attitude towards workplace violence. Verbal abuse is generally the hardest type of abuse to define since the border between what is acceptable and unacceptable depends on the individual, where the border of what is (un)acceptable marks one's tolerance for certain types of psychological violence. Personal borders are thus idiosyncratic and differ greatly from respondent to respondent. In consequence, everyone sometimes inflicts and experiences psychological harassment and is often unaware of it (Kuhar et al., 1999). According to researchers (Kuhar et al., 1999; Munc, 2010; Plaz, 2014), psychological violence is the prevailing type of violence in today's society.

Compared to existing studies that investigated user violence against healthcare employees (Cink, 2008; Gabrovec, 2017; Kelbič, 2013; Klemenc & Pahor, 1999; Košir, 2012; Kvas & Seljak, 2015; Planinšek & Pahor, 1999) and the study that examined this issue in terms of nursing homes in Slovenia (Gabrovec & Eržen, 2016), our results indicate a lower number of employees (37.7%) who faced user violence at the workplace (vs. e.g. 71.7% – Gabrovec & Eržen, 2016). In our opinion, we can attribute this difference to the non-uniform methodology between the above mentioned studies. We could also attribute the lower result to the fact that verbal abuse of users is an everyday phenomenon that is difficult for experts to identify and estimate its frequency (Cink, 2008). Despite the difference in the percentage of employees who faced violence at the workplace, the ratio distinctive of the frequency of a certain form of violent behaviour matches the previous studies.

We did not confirm the hypothesis that those who experienced physical violence evaluated their emotional state of fear more negatively than those who did not. We also established that the employees included in our study most frequently reported the presence of fear and helplessness, uncertainty, and hazard when facing aggressive users, and least frequently the presence of anger, despair, and a lack of understanding from co-workers. The results are in line with the study conducted by Cink (2008) or show similarities to previous results of study by Gabrovec and Eržen (2016) (fear as the second strongest expressed feeling). Facing violence can thus cause such feelings and states and can leave lasting consequences. Violent users can cause fear and stress with their actions for employees who meet them. The consequences of such occurrences can be seen in more frequent absences for sick leave, workers seeking employment elsewhere,

and consequently a fluctuation of employees and reduced productivity at work (Planinšek & Pahor, 1999).

Although we did not confirm the fourth hypothesis, which states that the majority of those who experienced physical violence at work assess the available know-how on dealing with violence as inadequate, we still find it important highlight the importance of addressing the issue of workplace violence in healthcare institutions. To successfully control it, we need to approach this issue comprehensively and act in different ways to prevent and face violence at the workplace. It is important to provide high-quality education and training for employees, and establish a protocol (or guidelines) for dealing with workplace violence once it is identified. They will thus be able to handle violent user behaviour safely and expertly. In our opinion, suitable know-how about control a violent individual can be crucial for achieving a favourable outcome in a given situation. Continuous theoretical and practical workshops can benefit it as well. A previous study (Gabrovec & Eržen, 2016) in Slovenia established that the need exists for a broader approach to handling workplace violence and that, as mentioned in the introduction, an organisation can influence the establishment of a safety culture in an organisation by developing systematic training models with required precautions to assure safety and prepare the protocol to be used in the event of violent situations. One of the possible measures is an organisational model of safety assurance and quality in dealing with the aggression of a user with a mental disorder in psychiatric healthcare in Slovenia (Gabrovec & Lobnikar, 2014), which includes frameworks of possible actions and practical techniques. It serves as a basis for functional education, which is predominantly grounded on practical training (Gabrovec & Lobnikar, 2014). The model is primarily intended for educating healthcare workers in psychiatric institutions. We nonetheless think that it could be used for testing in nursing homes as well, especially in places where employees face physical violence more often. Although the number of studies is increasing every year, this field needs more attention in order to find effective ways of preventing and facing user violence in the future. Thus, we see room for improvements and further research in this direction.

This study focused on investigating the violence of users against employees of nursing homes, but there are also studies available that focus on studying the violence enacted by employees against nursing home users. Conflicts between residents and employees often occur due to the way services are provided by employees (Mali, 2008). Nursing home residents often feel a clear dependency on others when receiving care, which fails to consider their individual needs and abilities, wherefore they lose a feeling of significance. Therefore, they wish to retain power in a relationship, where uneven distribution of power is typical, by taking it away from personnel by exercising violence (Zabukovec, 1999). This should be examined in the same environment as present study as well; the results of studies should be compared and cross-checked for links between users exerting violence against employees and employee violence against users. We believe that causes can originate from one another in a circular way.

Even though this study was planned carefully, we would like to highlight some restrictions which could influence the presented findings. Regardless

of several great efforts, our sample remained inhomogeneous, since it mostly includes females. This could also influence the results. We also had to face a 53% decrease of participants while acquiring data, which means that more than a half of the anticipated respondents did not provide an answer. This is why we cannot generalise the survey results to a complete population (Mesec, 2009) and assume that our findings apply to all employees in the *Dom ob Savinji Celje* nursing home. A descriptive and quantitative study enabled us an insight into the state of the examined issue in *Dom ob Savinji Celje* but we cannot generalise its results to the complete Slovenian area due to a non-representative sample. We also do not have an insight into a cause and effect relationship between the phenomena and a deeper insight into actual potential causes for certain violent behaviours. To do this, we would have to use a qualitatively-oriented study or mixed methods of research.

5 CONCLUSION

If we allow violence, it not only appears more frequently, but experience has shown that it even intensifies (Klemenc & Pahor, 1999). To detect and prevent violence, we should first of all increase awareness about the issue (Mrak, 1999). Causes for the escalation of violence can differ and the various ways of addressing this issue stem from these differences. We should develop a range of methods of mechanisms to identify, prevent, and decrease all types of violence within the working process. Relationships in healthcare and social care should be the most human and democratic form of cooperation, coupled with expert knowledge and the ability of every individual to do good for users and experts. This should additionally motivate us to solve conflicts in a friendly way for both users and experts (Zabukovec, 1999). This is why it is important that we have contributed to this research area with this study. In our opinion, the results of this study can contribute to designing a comprehensive plan of handling violent behaviour against employees in healthcare and social care institutions. Moreover, its findings support systematic measures to identify, report, prevent, and control this type of violence since comparing to healthcare institution this filed of the study is still overlooked at the social care facilities.

REFERENCES

Babnik, K., Štemberger Kolnik, T., & Kopač, N. (2012). Predstavitev rezultatov dela raziskave Nasilje nad medicinskimi sestrami na delovnem mestu – oblike, pogostost in povzročitelji psihičnega nasilja [Presentation of the results of the research Violence against nurses at work – forms, frequency and causes of psychological violence]. *Obzornik zdravstvene nege, 46*(2), 147–156.

Bowie, V. (2002). Defining violence at work: A new typology. In M. Gill, B. Fisher, & V. Bowie (Eds.), *Violence at work: Courses, patterns and prevention* (pp. 1–20). Portland: Willan.

Cink, T. (2008). Organizacijski dejavniki stresa v profesiji socialnega dela [Organizational factors of stress in the social work profession]. *Socialno delo, 47*(1/2), 1–21. Retrieved from https://www.dlib.si/details/URN:NBN:SI:DOC-FDA1RM08/?query=%27contributor%3dCink%2c+Tanja%27&pageSize=25

Društvo za nenasilno komunikacijo (n. d.). *Kaj je nasilje?* [What is violence?] Retrieved from https://www.drustvo-dnk.si/o-nasilju/kaj-je-nasilje.html#gor

Gabrovec, B. (2017). Violence towards nursing employees in Slovenia. *Varstvoslovje, 19*(2), 151–166.

Gabrovec, B., & Eržen, I. (2016). Prevalence of violence towards nursing staff in Slovenian nursing homes. *Slovenian Journal of Public Health, 55*(3), 212–217.

Gabrovec, B., & Lobnikar, B. (2014). Organizacijski model zagotavljanja varnosti in kakovosti obravnave agresije pri pacientu z duševno motnjo v zdravstveni negi na področju psihiatrije v Sloveniji [An organizational model for ensuring the safety and quality of dealing with aggression in a patient with a mental disorder in nursing care in the field of psychiatry in Slovenia]. *Obzornik zdravstvene nege, 48*(4), 286–293.

Gabrovec, B., Eržen, I., & Lobnikar, B. (2014). Prevalence and the nature of violence directed at the medical staff in psychiatric health care in Slovenia. *HealthMED, 8*(2), 228–234.

Gates, D. M., Gillespie, G. L., & Succop, P. (2011). Violence against nurses and its impact on stress and productivity. *Nursing Economics, 29,* 59–67.

Habjanic, A. (2009). *Quality of institutional elderly care in Slovenia* (Doctoral dissertation). Oulu: Oulun Yliopisto. Retrieved from http://jultika.oulu.fi/files/isbn9789514291869.pdf

Kelbič, A. (2013). *Nasilje nad zaposlenimi v nujni medicinski pomoči* [Vilence against staff in the emergency department] (Master thesis). Maribor: Fakulteta za zdravstvene vede.

Klemenc, D., & Pahor, M. (1999). Nasilje na delovnih mestih medicinskih sester v Sloveniji [Violence in nursing jobs in Slovenia]. In D. Klemenc, & M. Pahor (Eds.), *Nasilje in spolno nadlegovanje na delovnih mestih medicinskih sester v Sloveniji* (pp. 12–35). Ljubljana.

Koprivnik, N. (2002). Besedno in telesno nasilje oskrbovancev nad negovalnim osebjem v domu upokojencev in oskrbovancev Impoljca v Sevnici [Verbal and physical violence of persons in care against the nursing staff in nursing home Impoljca in Sevnica]. *Obzornik zdravstvene nege, 36*(3), 171–174.

Košir, I. (2012). Appearance of the physical violence against nurses at work place in Slovenia. *Obzornik zdravstvene nege, 38*(1), 43–52.

Kuhar, R., Guzelj, P., Drolc, A., & Zabukovec, K. (1999). *O nasilju* [About violence]. Ljubljana: Društvo za nenasilno komunikacijo.

Kvas, A., & Seljak, J. (2015). Sources of workplace violence against nurses. *Work, 52*(1), 177–184.

Mali, J. (2008). *Od hiralnic do domov za stare ljudi* [From poorhouse to elderly home]. Ljubljana: Fakulteta za socialno delo.

Mesec, B. (2009). *Metodologija raziskovanja v socialnem delu 1: Načrtovanje raziskave z osnovami informatike* [Methodology of research in social work 1: Planning the research with the basics of informatics]. Ljubljana: Fakulteta za socialno delo.

Možina, M. (2009). Tudi jaz sem lahko žrtev! Verbalno in fizično nasilno vedenje klientov do socialnih delavk/cev [I can be a victim too! Verbal and physically violent behaviour of clients towards social workers]. *Socialni izziv, 15*(29), 5–14.

Mrak, M. (1999). Timska situacija – možnosti ozaveščanja za prepoznavanje in preprečevanje nasilja v medsebojnih odnosih [Team situation – awareness raising opportunities for identifying and preventing violence in relationships]. In D. Klemenc, & M. Pahor (Eds.), *Nasilje in spolno nadlegovanje na delovnih mestih medicinskih sester v Sloveniji* (pp. 86–92). Ljubljana: Društvo medicinskih sester in zdravstvenih tehnikov.

Munc, M. (2010). *Nemoč nasilja* [Powerlessness of violence]. Maribor: De Vesta.

NHS Employers. (2014). *Health safety and wellbeing partnership group*. Retrieved from https://www.nhsemployers.org/your-workforce/pay-and-reward/nhs-staff-council/health-safety-and-wellbeing-partnership-group-hswpg

Normand, C. (2015). *Anaylysis of the health system in Slovenia: Long-term care, final report.* Copenhagen: WHO Regional Office for Europe.

Occupational Safety and Health Administration [OSHA]. (2008). *What is workplace violence?* Retrieved from https://www.osha.gov/SLTC/workplaceviolence/

Occupational Safety and Health Administration [OSHA]. (2015). *Preventing workplace violence: A road map for healthcare facilities.* Retrieved from https://www.osha.gov/Publications/OSHA3827.pdf

Planinšek, I., & Pahor, M. (1999). Spolno nasilje/nadlegovanje nad medicinskimi sestrami na njihovih delovnih mestih v Sloveniji [Sexual violence/harassment toward nurses at their workplaces in Slovenia]. In D. Klemenc, & M. Pahor (Eds.), *Nasilje in spolno nadlegovanje na delovnih mestih medicinskih sester v Sloveniji* (pp. 36–55). Ljubljana: Društvo medicinskih sester in zdravstvenih tehnikov.

Plaz, M. (2014). Nasilje nad ženskami v partnerskih in sorodstvenih odnosih [Violence against women in partnerships and kinships]. In Š. Veselič, D. Horvat, & M. Plaz (Eds.), *Priročnik za delo z ženskami in otroki z izkušnji nasilja* (pp. 75–93). Ljubljana: Društvo SOS telefon za ženske in otroke – žrtve nasilja. Retrieved from http://www.potpisujem.org/doc/91546425d3a1559c5b170983ac6057fa.pdf

Pompeii, L., Dement, J., Schoenfisch, A, Lavary, A., Souder, M., Smith, C., & Lipscomb, H. (2013). Perpetrator, worker and workplace characteristics associated with patient and visitor perpetrated violence (Type II) on hospital workers: a review of the literature and existing occupational injury data. *Journal of Safety Research, 44*(Feb), 57–64.

Stokowski, L. A. (2010). *Violence: Not in my job description*. Medscape. Retrieved from https://www.medscape.com/viewearticle/727144_1

Zabukovec, K. (1999). Nasilje je naš skupen problem, ustavljanja nasilja skupna odgovornost [Violence is our common problem, stopping violence is a shared responsibility]. In D. Klemenc, & M. Pahor (Eds.), *Nasilje in spolno nadlegovanje na delovnih mestih medicinskih sester v Sloveniji* (pp. 112–117). Ljubljana.

Zakon o preprečevanju nasilja v družini [Domestic Violence Prevention Act]. (2008). *Uradni list RS*, (16/08).

World Health Organization [WHO]. (2002). *World report on violence and health: Summary.* Geneva: World Health Organization. Retrieved from https://www.who.int/violence_injury_prevention/violence/world_report/en/summary_en.pdf?ua

About the authors:

Katarina Cesar, MA student at the Faculty of Social work, University of Ljubljana, Slovenia. E-mail: cesar.katarina@gmail.com

Liljana Rihter, PhD, Assistant Professor at the Faculty of Social work, University of Ljubljana, Slovenia. E-mail: liljana.rihter@fsd.uni-lj.si

Špela Selak, PhD, researcher at the National Institute of Public Health, Slovenia. E-mail: spela.selak@nijz.si

Branko Gabrovec, PhD, Assistant Professor, researcher at the National Institute of Public Health, Slovenia. E-mail: branko.gabrovec@nijz.si

Reviewers in 2018

Igor Areh, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Igor Bernik, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Bojan Dobovšek, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Miha Dvojmoč, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Benjamin Flander, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Danijela Frangež, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Mitja Gorenak, University of Maribor, Faculty of Tourism, Brežice, Slovenia

Rok Hacin, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Zoran Kanduč, Institute of Criminology at the Faculty of Law, Ljubljana, Slovenia

Blaž Markelj, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Darko Maver, external associate of University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Janez Mekinc, University of Primorska, Faculty of Tourism Studies – Turistica, Portorož, Slovenia

Mojca Mihelj Plesničar, Institute of Criminology at the Faculty of Law, Ljubljana, Slovenia

Danijela Mrhar Prelić, Ministry of Justice, Ljubljana, Slovenia

Iztok Podbregar, University of Maribor, Faculty of Organizational Science, Kranj, Slovenia

Kaja Prislan, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Boštjan Slak, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

David Smolej, Ministry of the Interior, Police, Ljubljana, Slovenia

Robert Šumi, Ministry of the Interior, Police, Ljubljana, Slovenia

Bojan Tičar, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Bernarda Tominc, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Rafael Viltužnik, Ministry of the Interior, Police, Ljubljana, Slovenia

Simon Vrhovec, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Sabina Zgaga Markelj, Constitutional Court of the Republic of Slovenia, Ljubljana, Slovenia

Miroslav Žaberl, external associate of University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia