

New technologies – need for new law enforcement capabilities: Situational analysis in the Former Yugoslav Republic of Macedonia, Montenegro and Serbia

Kristina Doda¹
Aleksandar Vanchoski

Institute for Human Rights, Skopje, the Former Yugoslav Republic of Macedonia



Abstract

Introduction of new IT hardware and software tools has a fearsome dynamic and directly is shaping the overall human interactions and patterns of economic and social development. All actors in the society, including decision makers, scientists, academia and civil society, must be aware that when new technologies are developed, which are capable of opening new dimensions of communication, transport or development, there must be comprehensive evaluation not only of the positive effects but also of the potential negative side effects of these new kinds of products and services which very easily could be used by individuals or groups for jeopardizing citizens' security and overall public safety. Furthermore, the implementation of new technologies by law enforcement agencies raises the question of proper implementation of human rights standards and legal accountability. This analysis is also giving a short overview of the law enforcement capabilities regarding new technological developments in three EU candidate countries: the Former Yugoslav Republic of Macedonia, Montenegro and Serbia. These countries are into EU accession process and they need to harmonize their national legislations with EU acquis and achieve full interoperability with the EU agencies. Recommendations for improvement of the capabilities for adopting new technologies and innovation in the day-to-day operational functioning of the police forces and law enforcement agencies in these three EU candidate countries are also proposed at the end of this analysis.

Keywords: innovations, technology, law enforcement, the Former Yugoslav Republic of Macedonia, Serbia, Montenegro

Introduction

The police as the only legitimate state actor which can use force, conduct criminal investigation and at the same time restrict and protect human rights and liberties are facing tremendous challenges which are direct or indirect products of ICT revolution and process of digitalization.

Introduction of new ICT hardware and software is shaping the overall human interactions and patterns of economic and social development. Taking into consideration the complexity and the dynamics of ICT and digital innovations, law enforcement agencies (LEA) including the police organizations are put in unfavourable position because potential and existing trends that new technologies are bringing as own side effects are numerous and are exceeding the police financial and human resources for prevention and investigation.

¹ Corresponding author's e-mail: Kristina.doda@ihr.org.mk

However, from another side ICT presents a main medium for developing and introducing many innovations and new methods in LEA and police work.

Although the development of ICT has positive influence on many social and economic activities still there are many “grey zones” from legalistic, moral and social aspects in domains such as use of autonomous or semi-autonomous vehicles, use of various size of flying drones, developing of overall digital economic activities, new ways of production especially of the 3D printing and manufacturing, privacy data protection in internet domain and data mass storage practices. The use of autonomous or semi-autonomous vehicles are opening a lot of legal and practical police dilemmas over numerous situations as a traffic safety, traffic accidents, possibility who can use them etc. The flying drones are already one of the most challenging devices that police officers are facing regarding jeopardizing the security of some public buildings and security interesting individuals.

The digital economy is becoming driver of economic and social development of many countries including the EU which placed digital economy as one of its strategic goals and even have developed own digital single market strategy. Having in mind that through these kinds of processes the economic and financial activities are becoming faster and more dynamic, police officers must develop new skills and toolkits for ensuring implementing the law and providing security.

Furthermore, the stakeholders and especially LEA and police management officials should not underestimate and neglect the human rights-based approach which should be seriously taken into consideration when new technologies with potential for mass data storage, easily exceeding citizens' privacy and restricting many fundamental human rights are adopted by LEA and police organisations. Moreover, in the time of digital societies and rapid development of ICT there is also raising tendency of questioning the inviolability of the right to privacy.

This analysis highlights the importance of adopting and utilizing new technologies by LEA and police organisations with a special focus on the current developments in this particular domain in three EU candidate countries: the Former Yugoslav Republic of Macedonia, Montenegro and Serbia. The analysis is an initial stage for further research and is based on content and qual-

itative analysis of the National strategies for development of police forces in these three countries.

New technologies, what are the new challenges?

Beside the positive sides and new possibilities that new technologies are bringing, in the same time there are numerous challenges and threats that are appearing such as: digital frauds, different cyber-crimes, traffic safety issues, various legal and practical difficulties related to traffic accidents investigation and personal accountability, guaranteeing the security of particular public spaces and individuals from abuse of flying drones etc.

Ideally, LEA should strive for solutions before problems appear which means making assumptions and propose sustainable solutions for effective prevention. Developing a systematic infrastructure in policing for maximizing technology's potential will also require both police and researchers to make a commitment for a strong common research and development (R&D) agenda. “Researchers can assist practitioners by collaborating on evaluation studies assessing theories behind technology adoption. In addition, research is needed to clarify what organizational strategies as training, management and evaluation are most effective for achieving desired outcomes with technology and avoiding potentially negative unintended consequences” (Koper et al., 2015).

Police can facilitate R&D policies by making greater efforts for strategic and operational planning, sustainable medium and long-term funding for R&D activities and higher transparency and openness for cooperation with academia and civil society organizations (CSOs).

A very important issue which should be taken into consideration is the fact that any new developed technological toolkit or method before its adoption and implementation as a standardized police measure or authorization should be carefully tested and analyzed with regard to its impact on human rights limitations and police accountability. Advances in technology do not always produce obvious or straightforward improvements in communication, cooperation, productivity, job satisfaction, or officers' effectiveness in reducing crime and serving citizens (Koper, Lum & Willis, 2014: 214).

Only inclusive and sustainable policies and strategies based on previous research on their effects upon society and law could lead towards higher levels of resilience to various forms of insecurity that ICT is bringing with its rapid development.

New technologies and the human rights perspective

Mostly when we think about technology we mainly focus on how technologies operate and not how and what is the impact of the technology on other police outputs such as police behaviour, effectiveness or relationships with citizens. Therefore, in order to increase the benefits of technology the new technologies in police need to be used with respect to the principles of accountability, transparency and data protection and privacy.

From a human rights perspective technology led policing (De Pauw et al., 2011), raises questions in relation to police accountability. As part of the development of the surveillance society (De Pauw et al., 2011) new police technologies including biometric databases, data collection and analysis, facilitate and hinder compliance with human rights. Although they are potentially useful ICT tools for law enforcement, the need for proper checks and balances is more than necessary when we speak about usage of new technologies by LEAs. This is especially important when LEAs are utilizing ICT tools whose capabilities enable collecting and storage of huge quantum of citizens' personal data, or easy access of surveillance over various forms of communication which requires setting a strict rules, procedures and ethical principles for protection and guaranteeing the right of privacy as a fundamental human right.

To gain the full potential benefits of technological innovations, police must also arguably address traditional and long-standing philosophical and cultural norms about the role of law enforcement. Training about proactive and evidence-based strategies—and how technology can be used in support of those strategies—is needed (Koper, et al., 2015:5).

Innovation and technologies in the EU candidate countries the Former Yugoslav Republic of Macedonia, Montenegro and Serbia

Regarding the innovation and new technologies in the area of law enforcement and more precisely in the police work we analysed the current strategic documents and approaches that are developed and present as guidelines for the political and professional police leadership in the Former Yugoslav Republic of Macedonia, Montenegro and Serbia. The purpose of this analysis is to emphasise how and to what extent the Former Yugoslav Republic of Macedonia, Montenegro and Serbia are prepared for the new security threats and challenges which are becoming more cyber space oriented and digitalized. Through the EU integration process these countries are committed to align their national legislation, strategic documents and goals with the EU values and acquis, including as well as the key EU strategic policy document and interests from the area of justice, security and freedom and area of common defence and security policy. Therefore, one of the most important benchmarks of the EU integration processes of the three countries is the EU based strategic planning and legislative alignment.

In situation when EU is facing more and more with technological driven security threats and criminal activities, there is a necessity for adopting new technology methods and instruments for prevention, detection and investigation of these phenomena as well as higher level of interoperability among law enforcement agencies of EU member and candidate states and EU institutions and agencies. The following chapters are focusing on national strategic goals and institutional capacities that the Former Yugoslav Republic of Macedonia, Montenegrin and Serbian law enforcement agencies are having, or more specifically the police forces, related to the adopting and developing new technology and technologies in conducting of its legislative duties and responsibilities. The analysis is done through analysing primarily the National strategies for development of police forces as a key strategic document that emphasises the main priorities and goals regarding the research and development capabilities of the police organisations in these three countries.

Also the paper gives a short overview whether the national police practices of utilizing new technologies are followed by proper privacy data protection stand-

ards which are in line with EU acquis as an important precondition for safeguard of the fundamental human rights.

The Former Yugoslav Republic of Macedonia law enforcement capabilities regarding new technologies

The most important document which sets the strategic goals for enhancing the operational capabilities and organizational potentials of the Former Yugoslav Republic of Macedonia law enforcement agencies is the "Police Development Strategy 2016 - 2020". In accordance with the strategic objectives, this Strategy foresees that the development of the Former Yugoslav Republic of Macedonia police is based on "...4 (four) main pillars: resource management, police work with the community, successful dealing with crime, and learning and development." (Ministry of Interior [MoI] of R. Macedonia; 2016:7)

In certain parts of the Police Development Strategy directly are noted the existing organizational and operational capabilities of the Former Yugoslav Republic of Macedonia police in the domain of utilizing ICT technologies in carrying out day-to-day police activities and tasks as well as the necessity for implementing new technologies in improving the police capacities for guarantee of the safety and prevention efficiency of different forms of criminality.

For the past three decades, the Former Yugoslav Republic of Macedonia police and other law enforcement agencies have been constantly reforming and improving with different dynamics in accordance with the basic democratic principles stipulated in the Constitution and in accordance with the good practices of numerous European LEA. Also it should be noted that such reform processes and changes in a significant degree were supported and financed by certain international actors such as the Organization for Security and Cooperation in Europe (OSCE), the Council of Europe (CoE) and, in particular, the European Union (EU) through the pre-accession funds. More dynamical reforms related to the organizational setup and functioning of the Ministry of Interior (MoI) and the Former Yugoslav Republic of Macedonia police were conducted after 2001 and especially after obtaining the candidate status for an EU membership at the end of 2005. However, very often the positive effects of the implemented reforms were not very visible or the reforms were not always implemented in the right manner.

According to the data presented in the Strategy for the period 2016-2020, the Former Yugoslav Republic of Macedonia police is facing with low level of application of advanced ICT software and hardware tools which actually reflects upon its operational efficiency. Also, there are no sustainable and systematic programs and funds for developing innovative tools and solutions that in the medium and long-term run would enable police forces to obtain capabilities for proper respond to the dynamic technological needs of the society as well as to the risks that digitization brings with itself. Namely, the Strategy suggests that "the majority of the police workflows are not covered by ICT support tools, which substantially causes higher costs for material and human resources" (MoI of R.Macedonia, 2016:21) Additionally, part of the ICT applications that are currently used by the police "were developed with own resources, but they are not based on the same entity structure, which is a problem for integrating the overall police database" (MoI of R.Macedonia; 2016:22). The documentation and the exchange of documents within the police still is carried out in paper form which has a significant negative impact on the effectiveness of the police work (MoI of R.Macedonia; 2016:22) There is no electronic centralized archive for storing all documents, thus preventing the possibility of effective monitoring, which is well known that is necessary in each segment of the police structure and work (MoI of R.Macedonia; 2016:21).

Another disadvantage that prevents the Former Yugoslav Republic of Macedonia police from having a more systematic approach for improving its operational functioning and establishing a sustainable system for development and application of new technologies is not existence of database and a checking mechanism for registering all police trainings, both nationally and internationally organized. Furthermore, related to the international cooperation, there is no common centralized record of projects that will enable management, monitoring, implementation, monitoring and supervision of these projects.

From an organizational and structural point of view, the police unit that has the authority and capacities to deal with the cutting edge forms of criminality closely related to ICT is the Department of Cybercrime and Digital Forensics of the MoI, which has the task of conducting investigations for the detection of serious and complex cases of cybercrime, such as malware analysis, internet fraud, social engineering, network attack, crit-

ical infrastructure attacks, child abuse via the Internet, “Darknet”, etc. This department is a centralized police unit and it has own regional subunits. However these subunits are not operational due to lack of human and financial resources (Mol of R.Macedonia; 2016:11). Therefore we can conclude that the Former Yugoslav Republic of Macedonia police is facing great challenges with regard to the implementation of innovative and advanced ICT software and hardware tools that inevitably imposes the need for drastic changes of the strategic approaches and operational concepts. It is also evident that certain basic preconditions firstly need to be established in order the officers from the Former Yugoslav Republic of Macedonia police to be able to respond to the challenges that the digital society imposes. One of these preconditions is certainly the ongoing process of development of a National Cyber Strategy which currently is in the process of drafting by various national stakeholders.

When it comes to the legal safeguards of fundamental human rights in situations when police officers are utilizing new high-tech ICT in conducting their duties and authorizations, unfortunately the Former Yugoslav Republic of Macedonia citizens have faced with serious challenges as a result of high volume of police misconducts. Just recently the Former Yugoslav Republic of Macedonia has experienced a mass wiretapping scandal because some police officers without court warrant or any other legally allowed security reasons made an illegal recordings of more than 20 000 citizens including politicians, businessmen, journalists and ordinary people. The recordings were acknowledged to have been made by the Administration for Security and Counterintelligence which is a structural part of the Mol. The content of many of the recordings provided numerous indications of unlawful activities and abuses of power which led to serious breaches of human rights and freedoms using advance ICT software and hardware technology illegally. These kind of unlawful practices have undermined the trust of the citizens in the organizational values and principles of the police.

The protection of privacy, the protection of personal data, and the protection of human rights related to freedom and dignity that were violated by this illegal recording of communication, are protected by the Constitution of the Republic of Macedonia and by number of laws, including the Law on Personal Data Protection, Law on Internal Affairs, Law on Police, while

the Criminal Code sanctions unauthorized wiretapping. However, the European Commission Progress Report on the former Yugoslav Republic of Macedonia indicated that it is necessary to further adjust the sector-specific laws in order to fully comply with the European regulations on personal data protection (European Commission, 2018).

Montenegrin law enforcement capabilities regarding new technologies

The reforms in the police in Montenegro were implemented together with the overall post-conflict reconstruction process in Montenegrin society especially after the ending of Yugoslav secession wars. The pressure for democratic policing and police accountability of the Montenegrin police was dual. Firstly, the pressure was coming from Montenegrin citizens and secondly was imposed by the ongoing process of European Union accession process.

Montenegrin police and other law enforcement agencies as many other European LEA is feeling the pressure that process of digitalization and rapid breakthrough in the ICT is affecting its operational functioning and their capabilities for preventing and countering new forms of crime committed by various ICT tools.

According to the Montenegrin “Development strategy for police for the period 2016-2020” the speed of changes in the field of information and telecommunications technologies, imposed inevitable need for constant improvement of technologies and procedures, used by police officers (Mol of Montenegro, 2015:19). Furthermore, into the Strategy is noted that the “adoption of new technologies, new knowledge and skills should enable police conducts, police methods of work and achieved results to be constantly monitored, improved and evaluated in order to be achieved maximum efficiency and transparency of the police work process, and the needs of the citizens and the society as a whole to be fully meet” (Mol of Montenegro, 2015:34). As one of the priorities in the efforts for implementing specific innovations in the functioning of the Montenegrin police is “introduction of the electronic management of cases (Case Management), processing and intelligence analysis of the data (Entity management), introduction of system for electronic statistics and reporting in the police as well as development of a unique geographic information system for the needs of all segments of the police” (Mol of Montenegro, 2015:34).

This strategy also points out that as a result of an increased number of Internet users, new electronic services and in particular electronic payments via the Internet in Montenegro there is a rapid increase in the abuse of various forms of information technologies with intention of committing various types of criminal offenses which on the end represent a special risk factor for the citizens and state security. Therefore, the strategy listed High-tech crime among the most serious security threats that Montenegrin police is facing currently or will face in the near future (Mol of Montenegro, 2015:19).

One of the steps for improving the operational capacities for preventing and countering high-tech crime is upgrading the ICT system of the financial intelligence unit of the Montenegrin police. However, shortcomings in the domain of the ICT and innovation implementing capabilities of the Montenegrin police include the lack of a secured data exchange link between prosecution office and law enforcement agencies as well as the need for increasing the administrative and ICT capabilities of the officers (Mol of Montenegro, 2015:35:40). Also, within the Ministry of Interior there is no special organizational unit that would deal exclusively with the planning and organization of training for the needs of police officers and there is no strategic multi-annual training planning (e.g. a five-year training plan).

Additionally, the Development strategy of the Montenegrin police regarding the innovations and new technologies is emphasizing that there is a need for strengthening of the educational and training programs at the Police Academy and establishing a more proactive role of the Ministry of Interior - Police Directorate in creating study/ training curricula that meet the needs of modern policing (Mol of Montenegro, 2015:40-41). Also, the study curricula need to be revised and aligned with modern standards of police education, human rights protection and technological innovations.

In 2017 Montenegro has adopted amendments related to video surveillance of the Law on Data Protection. However, according to the most recent European Commission report the implementation of the data protection legal framework remains weak. Work has not yet started on aligning the broader legal framework with the new EU data protection acquis in the field (European Commission, 2018). Furthermore, as the only one among the analyzed countries, Montenegro

has developed and adopted a special Cyber Security Strategy for the period 2013 – 2017. This actually shows the existence of awareness among the Montenegrin security stakeholders for the security threats that ICT and their everyday usage in all domains of the society could cause to the citizens' and the state security.

Serbian law enforcement capabilities regarding new technologies

Establishing a democratic and accountable police in Serbia was and still is a challenging step for the Serbian society. For a long period "the Ministry of Interior of the Republic of Serbia was an alienated force, deeply criminalized, politicized, centralized and with the absence of external democratic control, as well as a lack of efficient internal control. Since the democratic changes in 2000, the situation has slowly changed" (Paunovic, 2005:80). Numerous legislative and organizational reforms were undertaken for restructuring Serbian police forces in the notion of democratic and citizen oriented state organization. Furthermore as a result of the raising tendencies of more sophisticated forms of crime there is an evident pressure for reshaping of operational functioning of the Serbian police and other law enforcement agencies in accordance to the new social and technological realities.

In the case of Serbia for the purposes of this analysis firstly the "Development Strategy of the Ministry of Interior 2011 - 2016" was considered because in the time of writing this paper the new Strategy for the period 2018-2023 is under development at Serbian Ministry of Interior. This strategy still has the status of a draft version and process of public debates with academia and experts are ongoing. As a result of these developments the focus was mainly on the Development Strategy for the period 2011 – 2016 with taking in consideration eventual differences stated in the draft version of the new Development Strategy for the period 2018 – 2023.

A strategic approach to the development of the Ministry has been recognized as one of the key priorities in the scope of an overall reform of the public administration. In addition to this strategy, as other strategic and legal documents which are specifically related to the development of the Serbian police capacities for utilizing new technological and other innovations in day-to-day functioning are also: the "Strategic document - introducing e-learning as a support for the development of the training system in the Ministry of Interior" and the "Development Strategy for Informa-

tion - Telecommunications Technologies of the MoI for the period 2016 – 2020”.

According to the Development Strategy 2011-2016 as work areas that have strategic importance for the future development of the Serbian police are:

- Organization and management,
- Safety of the individual, the community and the state,
- Partnerships at national, regional and international level,
- Internal and external oversight systems and operational transparency (MoI of the Republic of Serbia, 2010:14).

In the “Organisation and management” section there is a sub-section “D) Developed Information and Communication Technologies (ICTs)” in which the necessity for development of the ICT capabilities of the MoI and police is acknowledged. Also, in the Development Strategy 2011-2016 several challenges which Serbian police are currently facing are detected. For example, it is noted that there is no secure platform for electronic data exchange or communication between law enforcement agencies (the prosecution service, the police, tax and other authorities (MoI of the Republic of Serbia, 2010:7:11).

In the Draft version of the new Development Strategy for the period 2018 – 2023 is stated that “Key challenges for MoI have been identified in the area of: Information and communication technologies; Cooperation at the national, regional and international level; Human resources; The availability of international development funds” (MoI of the Republic of Serbia, 2017:14).

Furthermore in the Development Strategy 2011-2016 is stated that “...substantial investments in Information and Communication Technologies (ICTs), material and human resources are needed” (MoI of the Republic of Serbia, 2010:9). Also, the Strategy unambiguously is acknowledging that “the use of ICTs is the prerequisite for:

- for having a functional organization based on the contemporary principles of a service-oriented institution, where the tasks are standardized and automated to the highest degree;

- for enabling the constant monitoring, improvement and appraisal of the organization, the work methods and the performance;
- Long-term planning regarding supplying of all levels of the organization with the proper knowledge, experience and equipment, while at the same time allowing their constant upgrading.”(MoI of the Republic of Serbia, 2010:17).

The necessity for improvement of the ICT capabilities of MoI and police are also emphasized again in the Draft version of the new Development Strategy 2018 – 2023.

The Development Strategy 2011-2016 also refers to the need for improving the computer and communication infrastructure by replacing analog communication with new installations in order to: enable faster data flow to police departments and Ministry facilities both through the Intranet and Internet communication infrastructure; Further improve and introduce new technological concepts and information systems for providing support to the Ministry’s work activities.

Similar objectives are stated in the Draft version of the new Development Strategy 2018 – 2023.

From the human resources point of view, there is a necessity to be improved the training and professional development system especially in the domain of providing specialized training, management training and continuous professional development. It is also necessary to develop new strategic and action plans as well as research and development projects.

Regarding the threats that ICT brings with their dynamic development, should be highlighted the fact that Serbia does not have a long-term strategy on how to address cybercrime.

Additionally the European Commission progress report for Serbia highlights “...a new law on personal data protection in line with EU standards needs to be urgently adopted. Processing and protection of sensitive personal data, biometrics and video surveillance, security of data on the Internet and direct marketing remain inadequately regulated, leaving a significant scope for abuse” (European Commission, 2016:61).

Regulation of the use of sensitive health data by public and private actors became an issue in Serbia following

media coverage of a request made by a local police authority to a local hospital. The reason given by the local police authority was to “update relevant dossiers”. (Journalism Development Network, 2015) The Serbian Data Protection Agency initiated the supervisory control over the implementation of the Law on protection of personal data (Official Gazette of the Republic of Serbia, nos. 97/2008, 104/2009, 68/2012, 107/2012) by the Ministry of internal affairs.

The Serbian government started working on a new law on personal data protection to harmonise the legislation with the new EU acquis entering into effect on 25 May 2018. The LEA have access to the personal data of the customers of Internet Service Providers and telecommunication companies in Serbia who according to relevant laws need to have a court decision to gain access to these data of online users. However there are no transparent information of how many requests for private information have been requested by LEA in Serbia.

From the above-mentioned, we can conclude that is necessary the Serbian police to undertake fundamental changes regarding the approach of adoption and utilizing new ICTs and innovations in its day-to-day operational functioning in order to deal more efficiently with the new forms of crime, to improve data protection and to ensure citizens’ right to privacy as well as to improve interoperability with the other regional and European LEAs.

Conclusion

After the analysis conducted on the situation in the Former Yugoslav Republic of Macedonia, Montenegro and Serbia we can conclude that more comprehensive and sustainable efforts and solutions should be considered in order to utilize ICTs for improvement of LEA and police capabilities and performances. In all three countries is evident that police organisations are facing with significant challenges related to adoption and development of innovative and technological advanced methods and tools. Furthermore can be notice that even some basic preconditions are non-existent (organisational and personal) for utilizing basic ICT infrastructures for enhancement of the operational functioning and mutual communication between LEAs and other local, national and international institutions. Taking into consideration the accessibility of advanced

ICTs to the crime networks and their trans-nationality these shortcomings need to be addressed systematically by LEA management and other relevant stakeholders. It is also evident that there is a necessity for more inclusive processes of cooperation with academia, ICT industry, civil society and citizens in the process of development innovative and technologically advanced solutions which can significantly help for day-to-day operational functioning of LEAs.

The privacy protection aspect during utilization of the advance ICT tools by LEAs in the observed countries is often weak due to the poor implementation of legislation and weak regulatory control practices. Socio-economic transformation and usage of ICT have radically changed the way of life in these countries as well. Therefore the LEAs and especially the police need to pay special attention both in building its own capacities for preventing the new sophisticated types of crime and also in providing accountable procedures and mechanisms to guarantee the fundamental rights when police officers used new ICT technological tools in providing public safety and crime prevention activities.

Recommendations

- Establishing productive cooperation and partnerships of the LEA and police organisations with private sector, academia and civil society organisations in order to be established more efficient process of following of the technological processes and minimizing the technological gap in the police workflow;
- Increasing the awareness of stakeholders, LEA management structures and police leadership for establishing special and sufficient funds for research and development in the law enforcement area and establishing a practice of conducting regular analysis of the current threats coming from abuses of the new technologies by criminals;
- Adopting and utilizing new ICT hardware and software for improving the analytical capacities of LEA and police, for reducing their response time in criminal investigation and crises management as well as for establishing secure channels of communication and data exchange at national, regional and European level;
- Conducting periodic awareness raising activities among the LEA and police officers on all organisa-

- tional levels, nationally and at EU level about the new technologies possibilities and potential treats;
- Developing educational and training programs for LEA and police officers which will correspond to the new digital realities and citizens' needs and will be focused both on the positive and negative sides of the new technologies over the safeguard of the fundamental human rights and over the outcomes of the police work activities and duties;
- Encouraging practices which allows bottom - top approach in developing new initiatives and innovation which actually means that any police officer beside his/her rank and position could propose and initiated development and adoption of new technologies and skills which will make police work more efficient and effective;
- Establishing formal and informal channels for initiatives, projects and recommendations by the state, non-state or international partners devoted for innovating the policing and maintaining the public security;
- Setting the protection of privacy as a priority when using the new technologies by LEA
- Strengthening the capacities of the Former Yugoslav Republic of Macedonia, Montenegrin and Serbian LEA and police for participation in EU funded projects (especially through Horizon 2020 programme) in order enhancing its organisational and human resources for adoption high -tech methods and toolkits in their day-to day work and for better interoperability with EU law enforcement and security systems for crime investigation and data exchange.

References

- Böhmelt, T. & Freyburg, T. (2017) Forecasting candidate states' compliance with EU accession rules 2017–2050. *Journal of European Public Policy*, 1-19.
- De Pauw, E., Ponsaers, P., Van Der Vijver, K., Bruggeman, W., & Deelman, P. (Eds.). (2011) Technological led policing. *CAHIERS POLITIESTUDIES (CPS)*. Antwerpen, Belgie ; Apeldoorn, Nederland: Maklu.
- European Commission. (2017) Horizon 2020 - Security, Available at: <https://ec.europa.eu/programmes/horizon2020/en/area/security>. Accessed on 15 October 2018.
- European Commission. (2015) "Priebe report" - The former Yugoslav Republic of Macedonia: Recommendations of the Senior Experts' Group on systemic Rule of Law issues relating to the communications.
- European Commission. (2018) A credible enlargement perspective for and enhanced EU engagement with the Western Balkans.
- European Commission. (2016) European Commissions country report Serbia 2016, 61.
- European Commissions' country reports for the former Yugoslav Republic of Macedonia, Serbia and Montenegro.(2018) Retrieved from: <https://ec.europa.eu/neighbourhood-enlargement/countries/package>, Accessed on 7 May 2018.
- Journalism Development Network (OCCRP), Rise Project and the European Actors Association (EAA) (2015). Who are the Gatekeepers of the Internet? Internet ownership project, Serbia: It's Hard to Tell Who Owns Some of Country's biggest internet service providers (ISPs). Retrieved from <https://www.reportingproject.net/internetownership/?p=116>, Accessed on 08 January 2018.
- Koper, S., Lum, C. & Willis, J. (2014) Optimizing the Use of Technology in Policing: Results and Implications from a Multi-Site Study of the Social, Organizational, and Behavioural Aspects of Implementing Police Technologies. *Policing: A Journal of Policy and Practice*, 8-2, Oxford University Press, 214.
- Koper, S., Lum, C., Willis, J., Woods, J. & Hibdon, J. (2015) *Realizing the Potential of Technology in Policing* (December edition). George Mason University.
- *Law on protection of personal data*, „Official Gazette of the Republic of Serbia“ nos. 97/2008, 104/2009, 68/2012, 107/2012.
- Ministry of Interior of Montenegro. (2015) *Development strategy for police for the period 2016-2020*. Retrieved from http://www.mup.gov.me/rubrike/strategija_razvoja_uprave_policije/. Accessed on 02 Jun 2017
- Ministry of Interior of Republic of Macedonia. (2016) *Police Development Strategy 2016 – 2020*. Retrieved from <http://www.mvt.gov.mk>. Accessed on 01 Jun 2017.
- Ministry of Interior of the Republic of Serbia. (2010) *Development Strategy of the Ministry of Interior of Republic of Serbia 2011- 2016*. Retrieved from <http://mup.gov.rs/wps/portal/sr/dokumenti/Strategije/>. Accessed on 02 Jun 2017.

- Ministry of Interior of the Republic of Serbia. (2017) *Development Strategy for the period 2018 – 2023*. Retrieved from <http://mup.gov.rs/wps/portal/sr/reforme/>, accessed on Jan 2018.
- Paunovic, D. (2005) Police Reform in Serbia. *Friedenskonsolidierung auf dem Balkan: Probleme und Perspektiven. Forschungen im Akademischen Netzwerk Südosteuropa 2003/2004*.