ANALYSIS OF ASPECTS OF PERSONAL DATA PROTECTION RISK ASSESSMENT USING MODERN TECHNOLOGIES IN THE MINISTRY OF INTERNAL AFFAIRS

Milan Gligorijević, PhD[1]
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Marija Pećanac[2]
Ministry of the Interior of the Republic of Serbia

Olgica Vulević[3]
Ministry of the Interior of the Republic of Serbia

Aleksandar Maksimović[4]
Ministry of the Interior of the Republic of Serbia

Abstract: The application of modern information and communication technologies is an indispensable factor in improving public safety, which is one of the key priorities in the work of the Ministry of Internal Affairs, based on identified risks and threats defined in the "Strategic Assessment of Public Safety for period 2017-2021". At the same time, the development of modern information and communication technologies has affected the complexity of security risks posed by such systems. On the other hand, citizens rightly expect an adequate response and protection mechanism from modern forms of endangering public safety and legally recognized freedoms and rights of citizens. Having in mind the wide range of security challenges and the need for more efficient work of the police, as well as all the advantages offered by modern technologies, the Ministry assessed that the conditions for the introduction of modern technologies in its work, which includes improvement of video surveillance system, establishment of intelligent

1 milan.gligorijevic@mup.gov.rs
2 marija.pecanac@mup.gov.rs
3 olgica.vulevic@mup.gov.rs
4 aleksandar.maksimovic@mup.gov.rs

video, analytics and construction of eLTE wireless broadband radio network, based on LTE (Long Term Evolution) technology. All of the above, the justification for the use of modern information and communication technologies, legal frameworks and analysis of aspects of risk assessment of personal data protection will be discussed in more detail in this paper.

Keywords: information and communication technologies, video surveillance system, intelligent video analytics, modern radio networks, personal data protection.

INTRODUCTION

Based on the identified risks and threats defined in the "Strategic Assessment of Public Security for the period 2017 - 2021", the improvement of public security is one of the key priorities in the work of the Ministry of Interior. On the other hand, one of the very important priorities of the Ministry is to bring the police closer to the citizens and better mutual cooperation in order to improve security. Namely, citizens rightly expect a decisive and adequate response to the threats of the modern form of endangering public safety and legally recognized freedoms and rights. Bearing this in mind, the basic task of the Ministry is to engage all the necessary resources starting from the collection of data and information, through assessment, processing and analysis. If such an answer is not forthcoming, we risk the trust of the citizens and the foundations of democracy itself. The challenge is great, because modern forms of endangering public safety are constantly changing, especially due to the accelerated development of information technology and means of communication.

The application of modern information and communication technologies is an indispensable factor in improving the security protection of citizens (Ranđelović, 2014). At the same time, the development and availability of modern communication and information technologies has complicated security threats due to the possibility of their abuse, both for communication, propaganda, recruitment, financing and training, and for cyber-terrorist attacks. On the other hand, in the field of information and communication technologies, the challenges relate to problems regarding the availability, connectivity and compatibility of relevant records of various institutions, as well as providing the necessary level of knowledge and exchange of experiences with representatives of the EU member states. Likewise, the challenges include the impossibility of implementing new technologies in existing resources, i.e. lagging behind in technological development, which causes incompatibility with partners with whom the Ministry cooperates. In this regard, it is necessary to provide access to the Ministry of the latest technological solutions based on the best world experiences, which are applied in their work by the police of modern countries.

With the introduction of modern technologies, conditions are created for more successful police operations, application of model 3E (more efficient, effective and economical way), direct (on-line) insight into the event or history of events, fast and efficient police response, as well as for going to the scene and arresting perpetrators, for investigating criminal offenses and prosecution of misdemeanors, finding or arresting wanted persons, increasing the security of people and property, border control and checking at border crossings, surveillance of the state border outside the border crossing, maintaining public order and peace, providing public gatherings, personalities, facilities and premises, security protection of certain persons and facilities, identification and finding of perpetrators of criminal acts and missing persons on the basis of biometric data on the person, providing evidence for filing misdemeanor and criminal charges, conducting internal control, monitoring legality and improving the work of the Ministry, initiating and conducting disciplinary proceedings, etc. (Kovačević-Lepojević, Žunić-Pavlović, 2010).

LEGISLATIVE FRAMEWORK AND ADVANTAGES OF THE USE OF MODERN TECHNOLOGIES IN THE PROCESSING OF PERSONAL DATA

According to the Law on Personal Data Protection (2018), "personal data" is any data relating to a natural person whose identity has been determined or determined directly or indirectly, especially on the basis of an identity mark, such as name and identification number, location data , an identifier in electronic communication networks or one or more features of its physical, physiological, genetic, mental, economic, cultural and social identity. It is also important not to mention the fact that the law very clearly and unambiguously regulates the conditions for collecting and processing personal data, which aims to ensure equal exercise and protection of the right to privacy for every natural person.

Personal data processing is any automated or non-automated action taken in relation to personal data or their aggregates, such as collecting, recording, sorting, grouping, storing, matching or modifying, detecting, inspecting, using, duplicating, disseminating or otherwise making available, comparing, restricting, deleting or destroying (Manojlović, 2014). Therefore, any use or any contact with personal data, regardless of how long such processing lasted and of what kind it was (active or passive) will be considered data processing.

The law also defines the term "biometric data", which is personal data obtained by special technical processing related to physical characteristics, physiological characteristics or behavioral characteristics of a natural person, which allows or confirms the unique identification of that person, such as the image of his face or his dactyloscopic data.

A simple and logical question arises here: Is a photograph of a person a biometric data, and thus a data on a person? The answer to this question has several aspects. The Law on Personal Data Protection classifies a photograph into biometric data only if it was made by special technical processing in connection with the physical characteristics of a specific person. Furthermore, the photograph is not mentioned as personal data in the Law. However, the General Data Protection Regulation (GDPR) in art. 51 of the Preamble specifies that the processing of a photograph does not in principle constitute the processing of special types of personal data, as a photograph is considered biometric only if it is processed by special technical means enabling unique identification or face identification. This means that not every photo of a person is biometric data. However, photographs on an ID card, passport, photo taken with a camera that uses a face recognition technique, are considered biometric data.

All above discussed comes to the fore because there are numerous advantages of using modern technologies for face recognition, which use biometric data, i.e. personal data. The advantage of using this technology is reflected in the fact that it can influence the deterrence from illegal and antisocial behavior (Bebis et al, 2006). Suspects are easier to identify using face recognition software, i.e. by simply comparing their photographs with databases (e.g. criminal files). The use of software can act preventively on potential perpetrators of crimes and repressively on those who have already committed them. If an individual is aware that the identification software that can easily reveal his identity is used, he will see that the chances of committing a crime with impunity are significantly reduced and he will refrain from committing a criminal activity (Gligorijević et al, 2016). The repressive action is reflected in the easier finding and arresting of persons suspected of having committed a crime on the basis of databases in the possession of state bodies that contain biometric data of already known criminals and convicts.

One of the significant advantages of using this technology is that the input data about a person is collected without contact and interference with that person's activities, i.e. it is not necessary for a person to place fingers or palms on the device or to approach the device to recognize the retina and the like. Since software can work without contact with the people being identified, in some cases they are not even aware that their identity is being verified (Ratcliffe, 2006).

It is also important to note that biometric technology can be useful in the public sphere for border surveillance at the border crossings, identification of criminals, fight against terrorism and elimination of identity fraud, etc. In the private sector, biometrics can help verify information about employees and working hours, advertise more efficiently, help social media users identify and tag other users, and improve security by controlling access to sensitive locations. Employers cite biometric time as an almost flawless way to keep accurate employee time data. Biometric technology generally makes these tasks easier, more efficient and more accurate. Although biometrics are touted as a way to improve security and limit fraud, privacy advocates have raised serious concerns about the technology.

On the other hand, in addition to all the advantages brought by the use of modern information and communication technologies, attention must be paid to assess the risk of the impact of these technologies on the rights and freedoms of individuals and the protection of personal data. Namely, in accordance with Article 54 of the Law on Personal Data Protection, if it is certain that some type of processing, especially the use of new technologies, taking into account the nature, scope, circumstances and purpose of processing, will cause a high risk to the rights and freedoms of individuals, the controller is obliged to assess the impact of the envisaged processing operations on the protection of personal data before starting the processing.

When assessing the impact, the controller is obliged to seek the opinion of the person for the protection of personal data, if it is determined. Impact assessment from Art. 54 paragraph 1 must be performed in the case of:
- systematic and comprehensive assessment of the condition and characteristics of a natural person, which is performed through automated processing of personal data, including profiling, on the basis of which decisions relevant to the legal position of an individual or similarly significantly affect him;
- processing of special types of personal data revealing racial or ethnic origin, political opinion, processing of genetic data or processing of personal data in connection with criminal convictions, criminal offenses and security measures;
- systematic oversight of publicly available areas to a large extent.

The assessment of the impact of the processing carried out by the competent authorities for specific purposes must at least contain a comprehensive description of the envisaged processing operations, a risk assessment of the rights and freedoms of the data subject, a description of the measures to be taken in relation to the existence of risks, and technical, organizational and personnel measures in order to protect personal data and provide evidence of compliance with the provisions of this law, taking into account the rights and legitimate interests of the data subject and other persons.

RISK ASSESSMENT FOR IMPACT MODERN INFORMATION COMMUNICATION TECHNOLOGIES ON RIGHTS AND FREEDOMS OF INDIVIDUALS

Risks to the rights and freedoms of persons that may arise from the use of modern information and communication technologies in the Ministry of the Interior can in principle be divided into the following types:

- Risk relating to the identification of persons without a legal basis
- Risk relating to the recording of private space
- Risk relating to data security breach
- Risk relating to public disclosure of data

Potential events that would imply a risk to the rights and freedoms of persons are related to the identification of persons without a legal basis, based on data collected in the video surveillance system of public areas. At the same time, for the purposes of risk assessment, the reason for illegal identification is to a certain extent, i.e. the fact that the identification is motivated by reasons of a personal or other nature.

The following events could result in the following consequences for the rights and freedoms of individuals:

- Violation of the right to private life by observing the activities of persons identified in the video surveillance system, as well as by storing and other data processing activities on these activities, regardless of the fact that the activities are undertaken in public areas;
- Violation of freedom of association, assembly and expression, i.e. the right to peaceful protest, as well as freedom of movement, by identifying and further processing the data of persons who gather in public areas, as members of an association or regardless of membership in the association, express their opinion, ideas and attitudes, peacefully protest, i.e. move in public areas as part of a procession, protest rally, etc., in accordance with the law governing the conditions for the exercise of these freedoms and rights;
- Violation of freedom of religion by identifying and further processing the data of persons entering or leaving religious buildings or participating in the performance of religious rites in public areas;
- Violation of the principle of non-discrimination through profiling of identified persons on the basis of actual or presumed affiliation to an association, i.e. religious community, political or other opinion, sexual orientation or other personal characteristics.

Analyses have shown that the level of certainty of the occurrence of the mentioned events is low. When assessing the level of certainty, the following circumstances or facts are especially taken into account:

- Identification of persons based on the data collected in the video surveillance system is based in each case on the organizational structure in the system of divided roles in terms of processing, deciding on the need for identification and control, which largely prevents any individual attempt to abuse police powers;
- Any action of processing the data collected in the video surveillance system, including the identification of persons, shall be recorded in order to enable effective control of the exercise of police powers, which has the greatest deterrent effect on potential violators of police powers;
- The number of cases of abuse, i.e. violation of police powers has been very small in recent years in relation to the number of actions taken by authorized persons of the operator indicating the exceptional discipline and conscientiousness of police officers.

- Authorized persons of the controller are already educated on the legal regime of personal data protection, which indicates a high level of awareness of the need to respect the principles of legality and other principles of the Law regarding the exercise of police powers when processing data, especially in video surveillance.

Potential events that would involve a risk to the rights and freedoms of individuals are related to the recording of private space, such as the interior of apartments, houses and backyards, offices and other business premises, using video cameras placed on poles and buildings in public use (Welsh, Farrington, 2009). At the same time, for the purposes of risk assessment, the reason for illegal recording is to a certain extent, i.e. the fact that the recording is motivated by reasons of a personal or other nature.

As a result of the mentioned events, the consequences could occur, which consist in the violation of the right to privacy by inspecting the activities of the person in the space being filmed, as well as by storing and other data processing activities on these activities.

Analyses have shown that the level of certainty of the occurrence of the mentioned events is low. When assessing the level of certainty, the following circumstances or facts are especially taken into account:

- Fixed cameras are physically positioned to record only public space, while mobile cameras can be used to capture private space only in exceptional cases when shooting is not limited by physical obstacles (for example, the camera is placed in a lower position relative to private space or in a position that is very far from the private space or the private space is sheltered by trees, curtains, blinds, fences, etc.), which to the greatest extent limits the possibility of monitoring the activities of persons in the private space;
- Monitoring the activities of persons using mobile video cameras is based in each case on the organizational system of divided roles in terms of processing, deciding on the need for monitoring and control, which largely prevents any individual attempt to abuse police powers;
- The information on the rotation of the camera in each specific case can be determined in order to enable effective control of the exercise of police powers, which has the greatest deterrent effect on potential violators of police powers;
- The number of cases of abuse, i.e. violation of police powers has been very small in recent years in relation to the number of actions taken by authorized persons of the Ministry, which indicates the exceptional discipline and conscientiousness of police officers.
- Authorized persons of the controller are already educated on the legal regime of personal data protection, which indicates a high level of awareness of the need to respect the principles of legality and other principles of the Law regarding the exercise of police powers during data processing, especially in the video surveillance system.

Potential events that involve a risk to the rights and freedoms of individuals are related to the violation of the security of the data collected in the video surveillance system due to access to the equipment used for video surveillance (for example, taking control of cameras), or copying, detecting or transmitting data by a third party. At the same time, for the purposes of risk assessment, the reason for the security breach is not relevant, i.e. the fact that the security breach is motivated by reasons of a personal or other nature.

These events could result in a violation of the right to protection of personal data of persons whose data are violated.

Analyses have shown that the level of certainty of the occurrence of the mentioned events is low. When assessing the level of certainty, the following circumstances or facts are especially taken into account:

- Equipment and data are provided with technical protection measures at the highest level, especially in terms of software protection, data transmission network protection, data protection with cryptosecurity system, as well as physical protection of cameras, lines, data storage equipment, etc., as much as possible measures effectively prevents data security breaches by third parties;

- Equipment and data are provided with comprehensive organizational protection measures, especially the application of a system of divided roles in terms of processing, which most effectively prevents data security breaches by third parties in cooperation with police officers;

- Authorized persons of the controller have already been trained to take technical and organizational measures for the protection of personal data, which largely effectively prevents the violation of data security by a third party;

- For years, there has been no violation of data security by a third party, which indicates the effectiveness of the protection measures taken when it comes to data processing performed by the controller.

Potential events that imply a risk to the rights and freedoms of individuals are related to the legally inadmissible public disclosure of the data collected in the video surveillance system through the media, social networks or the use of other means of communication. In addition, for the purposes of risk assessment, the reason for public disclosure is of some importance, i.e. the fact that public disclosure is motivated by reasons of a personal or other nature.

The following events could result in the following consequences for the rights and freedoms of individuals:

- Violation of the right to private life by inspecting the activities of a person covered by the video surveillance system by the public, i.e. the recipient of information published in the media, within social networks or disseminated through other means of communication;

- Violation of the right to identity in cases when the person covered by the video surveillance system is misidentified in public;

- Violation of personal moral integrity in cases when due to public disclosure of information related to the private life of a person, the reputation, honor or piety of that person has been violated;

- Violation of rights in cases when due to the public disclosure of information related to the private life of a person one of the stated rights has been violated.

Analyses have shown that the level of certainty of the occurrence of the mentioned events is low. When assessing the level of certainty, the following circumstances or facts are especially taken into account:

- The processing of the data collected in the video surveillance system is based in each case on the organizational system of divided roles in terms of performing processing operations, which largely prevents unauthorized public disclosure of data;

- Any action of processing the data collected in the video surveillance system is recorded in order to enable effective control of the exercise of police powers, which has the greatest deterrent effect on unauthorized submission of data to the media, or data transfer for public disclosure;

- The number of cases of unauthorized public disclosure of the data processed by the controller decreases from year to year and is very small in relation to the number of actions taken by authorized persons of the controller, which indicates exceptional discipline and conscientiousness of police officers.

- Authorized persons of the controller are already educated on the legal regime of personal data protection, which indicates a high level of awareness of the need to respect the principles of legality and other principles of the Law regarding the exercise of police powers during data processing, especially in relation to preventing unauthorized public disclosure of data.

DESCRIPTION OF MEASURES AND MECHANISMS APPLIED IN RELATION TO RISK TO THE RIGHTS AND FREEDOMS OF PERSONS

In relation to the risk to the rights and freedoms of persons, the Ministry of the Interior applies a whole set of different measures and mechanisms with the aim of protecting the stated rights and freedoms. They can in principle be divided into:

- Data security protection measures and mechanisms for protection of human rights
- A system of divided roles in data processing
- Technical aspects of providing video surveillance systems
- Discipline and conscientiousness of police officers
- Mechanisms for the protection of human rights

The presented risks to the rights and freedoms of persons are effectively eliminated, i.e. reduced to a minimum through the application of general organizational, personnel and technical measures for data security protection, i.e. mechanisms for protection of rights and freedoms of persons related to personal data processing. These measures and mechanisms are prescribed by the Law and other regulations, such as the Law on Information Security, the Law on Police, the Law on Records and Data Processing in the Field of Internal Affairs and bylaws issued by the Ministry. Data security protection measures and mechanisms for the protection of the rights of persons are applied in a specific way in the video surveillance system (Kovačević-Lepojević, Žunić-Pavlović, 2012). Some of these measures and mechanisms are applied in relation to several different risks in the same or different way, while other measures and mechanisms are applied only in relation to an individually determined risk.

The video surveillance system is created so that it can be functional only in a system of shared roles.[5] This means that in the collection and further processing of data in the video surveillance system it is not possible to organizationally, technically and legally imagine a situation in which the decision to undertake processing activities aimed at identifying persons or monitoring activities of persons, in the context of assessing the level of certainty of risk, brings outside the system of divided roles.

From the technical point of view of providing a video surveillance system, it is important to point out that the video surveillance system is an integral part of the information and communication system (ICT), which is managed by the Ministry. This system is effectively protected, inter alia, by appropriate technical information security measures applied to the data and equipment used (Andenas, Zleptnig, 2003). In the context of assessing the level of certainty of the occurrence of risk, technical measures effectively protect data and equipment, especially taking into account the fact that no case of data security breach by third parties due to deficiencies related to these protection measures has been recorded in recent years. The technical protection measures provide in particular the recording of each processing operation, i.e. the technical possibility of establishing the facts relating to the use

5 Obavezna instrukcija o uslovima korišćenja i održavanja sistema video nadzora gradskih saobraćajnica i raskrsnica za grad Beograd, Ministarstvo unutrašnjih poslova, 2015.

of cameras and other equipment in the video surveillance system in each specific case (Lomell, 2004). In this way, effective control over processing operations is provided, which has the greatest deterrent effect on potential violators of official powers, in the context of assessing the level of certainty of the occurrence of risks to the rights and freedoms of persons.

Discipline and conscientiousness of authorized officials engaged in the video surveillance system is ensured by the application of preventive and reactive protection measures. Preventive protection measures are primarily implemented through continuous education of authorized officials in connection with the application of the provisions of the Law and other regulations relating to the protection of personal data. Education is performed in accordance with the Decree on Professional Training and Development in the Ministry of the Interior, based on the Program of Professional Development of Police Officers of the Ministry of the Interior and the Directive on the manner of performing work relating to personal data protection in the Ministry of the Interior. Reactive measures are applied in case of violation of data security, i.e. personal rights. The first group of these measures refers to the breach of data security, regardless of whether in a particular case the security breach was responded to by another protection mechanism. The application of measures from this group is prescribed by the Law and the Instruction on the manner of keeping records and notifying about violations of personal data in the Ministry of the Interior. The second group of these measures are disciplinary measures and they are prescribed by the Law on Police. The third group of measures prescribed by the Law and the Criminal Code is applied by the Internal Control Sector, the Prosecutor's Office and the Court. The fourth group consists of measures applied by the Commissioner for Free Access to Information of Public Importance and Personal Data Protection, in accordance with the Law.

From the aspect of mechanisms of protection of human rights, it is important to note that every person whose data is processed by the Ministry including the data collected and further processed in the video surveillance system is authorized to address the Ministry in accordance with the Law. The mechanism for controlling the handling of requests from persons whose data are processed is entrusted to the person for personal data protection in the Ministry, and the forms of control are regulated by the Directive on the manner of performing activities related to personal data protection.

CONCLUSION

Technology is conquering all spheres of our lives alluding to the fact that our quality of life will improve, productivity will increase, costs will be reduced, the level of security of citizens will be raised, etc. The fourth industrial revolution is developing at a rapid pace. It has an impact on all industries in every country in the world changing the entire production and business processes. The biggest risk posed by Industry 4.0 and digital transformation concerns the privacy and security of citizens. In the field of information and communication technologies, new challenges relate to problems regarding the availability, connectivity and compatibility of relevant records of different institutions. Furthermore, the challenges include the impossibility of implementing new technologies in existing resources, i.e. lagging behind in technological development, which causes incompatibility with partners with whom the Ministry of the Interior cooperates.

The "Safe City" project is an intelligent video surveillance system that means that high-resolution cameras are placed in several locations in Belgrade. An intelligent video surveillance system will contribute to more efficient investigation of criminal acts. One of the most important facts is that different types of databases can be created in this way. According to the Law on Police, for the purpose of

performing police work, the police can monitor and record a public place using equipment for video acoustic recordings and photography in accordance with the regulations on records and data processing in the field of internal affairs.

The goal of the Ministry of Internal Affairs is to contribute to more efficient work of the police by introducing modern technologies within the project "Safe Society", thus raising citizens' trust in the work of the police, which will result in better results and reduction of overall crime and security of all citizens.

REFERENCES

1. Andenas, M. & Zleptnig, S.: *Surveillance and data protection: Regulatory approaches in the EU and Member States*, European Business Law Review, 2003
2. Bebis, G., Gyaourova, A., Singh, S., Pavlidis, I.: *Face recognition by fusing thermal infrared and visible imagery*, Image and Vision Computing 24, 2006
3. Gligorijević, M., Maksimović, A., Vučković, J.: *Forenzički i pravni aspekti upotrebe sistema video nadzora u dokazivanju krivičnih dela i prekršaja*, Zbornik radova, Međunarodni naučni skup „Dani Arčibalda Rajsa", Kriminalističko-policijska akademija, Beograd, 2016.
4. Kovačević-Lepojević, M., Žunić-Pavlović, V.: *Primena video nadzora u kontroli kriminala*, Fakultet za specijalnu edukaciju i rehabilitaciju, Univerzitet u Beogradu, Beograd, 2012.
5. Kovačević-Lepojević, M., Žunić-Pavlović, V.: *Mere javnog nadzora u službi prevencije kriminala*, Fakultet za specijalnu edukaciju i rehabilitaciju, Univerzitet u Beogradu, Beograd, 2010.
6. Lomell, H. M.: *Targeting the unwanted: Video surveillance and categorical exclusion in Oslo*, Norway. *Surveillance & Society, 2* (2/3), 2004
7. Manojlović, Z.: *Pravni okvir za primenu video nadzora*, Narodna skupština, Republika Srbija, Br.11/14, 2014.
8. *Obavezna instrukcija o uslovima korišćenja i održavanja sistema video nadzora gradskih saobraćajnica i raskrsnica za grad Beograd*, Ministarstvo unutrašnjih poslova, 2015.
9. Randelović, D.: *Upravljanje informacionim sistemima i njihova zaštita,* Edicija monografije, Kriminalističko-policijska akademija, Beograd, 2014.
10. Ratcliffe, J.: *Video surveillance of public places*, Washington, DC: U.S. Department of Justice, Offce of Community Oriented Policing Services, 2006
11. Welsh, B. C., Farrington, D. P.: *Making public places safer: Surveillance and crime prevention*, Oxford University Press, New York, 2009
12. Zakon o zaštiti podataka o ličnosti ("Službeni glasnik RS" br. 87/2018)