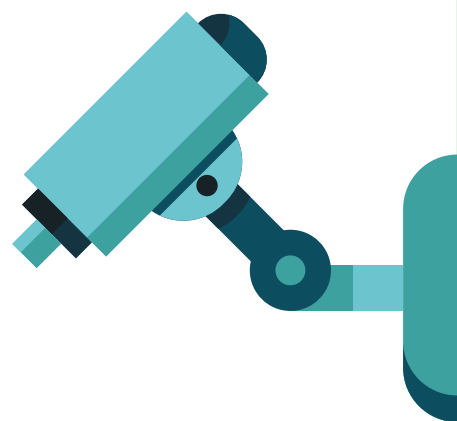


STUDY:

**VIDEO SURVEILLANCE
– A MEANS TO IMPROVE
SECURITY OR VIOLATE
CITIZENS' PRIVACY?**





CRTA:

This study is a joint effort by the Center for Research, Transparency and Accountability (CRTA), National Coalition for Decentralization (NKD), Belgrade Centre for Security Policy (BCBP) and Partners for Democratic Change Serbia (Partners Serbia) to encourage greater citizen participation in decision making through the project “Reconnecting Democracy – Citizens in Power”, supported by the United States Agency for International Development (USAID).



Beogradski
centar za
bezbednosnu
politiku



Author

Kristina Kalajdžić

Research Associates:

Uroš Mišljenović i Ana Toskić Cvetinović

Reviewer:

Blažo Nedić

Translation:

Tamara Ljubović

Design and Layout:

Dosije studio, Beograd

Publisher:


Partners for Democratic Change Serbia

For the Publisher:

Ana Toskić Cvetinović




C O N T E N T S



Summary	6
Introduction	8
Practical Examples of Inadequate Use of Video Surveillance System	10
Keeping Up with Trends: Cameras as a Means for Protection or Legal Tool for Controlling Citizens?	12
"SAFE CITY" Project	13
The Lack of Legal Framework	16
The Authorization for Setting up and Using Video Surveillance System	17
Personal Data Protection and the Use of Video Surveillance System	18
Conclusions and Recommendations	22

SUMMARY

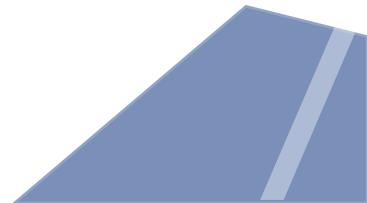


The practice of setting up and using video surveillance system in Serbia is characterized by the lack of transparency of the process itself, as well as insufficient compliance of these activities with the Law on Personal Data Protection and other regulations. The need for better regulations in the area of video surveillance arises from several examples in which such systems have been misused in Serbia.

The question regarding justification for conducting video surveillance of public spaces became a hot topic in early 2019, when the representatives of the Ministry of Interior informed the public about their intentions to initiate the “Safe City” project. As it was announced at the time, the Project alluded to mass processing of personal data of Serbian citizens, by means of video surveillance equipment, which includes facial recognition software. Even today, the public still has no reliable information regarding the exact number of cameras and locations where these cameras will be placed, and there is still no expert analysis regarding the justification for introducing this kind of video surveillance system.

Examples from all over the world indicate that countries often use video surveillance as a means for mass surveillance of citizens, rather than for its primary purpose, which is to protect the security. These types of technologies, aside from the consequences related to citizens’ privacy, have potential implications on other rights, such as the freedom of speech or freedom of assembly. If we are aware that they are watching us, we will feel less at liberty to express our views and/or take it to the streets and peacefully protest against decisions made by public institutions and the people who govern them.

In terms of the (mis)use of video surveillance system, it has repeatedly happened for the information obtained by security agencies and other bodies to be made publicly available and used to discriminate activists and political opponents. What guarantees us that data collected through the use of video surveillance system will be used more responsibly?



INTRODUCTION

Video surveillance is a system consisting of surveillance cameras, as well as equipment for storage, display and further processing of video material.¹ With the advancement of technology and development of different software and apps, these devices have more and more technical possibilities, making their use all the more creative. Although initially designed for the protection of people and property, nowadays cameras are used for various purposes, so thanks to them you can (along with Internet access) go on virtual tours of museums, or observe what is happening in the streets of, for example, Amsterdam, in real time.

When someone robs a bank, the police can quickly identify the perpetrator and have him apprehended, simply by looking at the footage made by video surveillance. So we can say that this is a sort of a victory for modern technology and video surveillance cameras. However, cameras keep rolling and recording even when no crimes are being committed. Cameras are recording citizens while they are shopping, driving, strolling around the city or drinking coffee in the garden of their favorite cafe. The development of surveillance technologies and their availability led to them being used both by states, as well as private entities. Even if the primary purpose of this technology is the security of people and property, abuses are possible, and they often occur.

The fear of video surveillance abuse primarily happens because we do not know who is (potentially) recording us and what is happening with these recordings. This fear further grows when we take into account that video surveillance is insufficiently regulated in the Republic of Serbia,

and that the state bodies, primarily those in charge of citizen and state security, lack transparency when it comes to introducing new video surveillance systems. Thus, the Belgrade public remained deprived of information on how the new smart video surveillance, announced by the Ministry of Interior in 2019, would look like. From several addresses of the Minister of Interior we learned that installation of video surveillance with facial recognition software is planned in Belgrade, and that the numbers of cameras to be set up varies between 1.000 and 2.000.² According to publicly available documents, this joint project between Mol and the City of Belgrade, called "Safe City" (Serbian: "*Siguran grad*"), should improve the level of security in the capital.

However, it is not that difficult to imagine a scenario in which this same technology is used to illegally monitor people, as a means of putting pressure on those who wish to express dissatisfaction with the work of institutions and public officials, or to exercise their right to organize and assemble in public.

The analysis below refers to pointing out the existing examples of (mis)use of video surveillance system by public authorities, the legal framework regulating video surveillance, and recommendations on how to improve regulations in this area, while reflecting upon the impact these systems have on citizen activism.

1 Depending on the type and purpose, they may have recording microphones, and be connected to the image transmission device by cable or wireless, etc.

2 N1, Stefanovic: A Thousand Cameras with Facial and License Plates Recognition Software: <http://rs.n1info.com/Vesti/a456247/Stefanovic-Hiljadu-kamera-sa-softverimaza-prepoznavanje-lica-i-tablica.html>

**PRACTICAL
EXAMPLES OF
INADEQUATE USE OF
VIDEO SURVEILLANCE
SYSTEM**

Caution related to the use of video surveillance system stems from several examples in which such systems have been misused in Serbia. In recent years, the Commissioner for Information of Public Importance and Personal Data Protection (hereinafter: the Commissioner) has responded to several legally problematic cases of the use of video surveillance by public authorities. One of the cases, though not related to public recording, but to the use of video surveillance within the premises of the institution itself, refers to video surveillance used at the Clinic for Psychiatry of the Clinical Centre of Serbia. Following citizens' petitions, the Commissioner conducted supervision at this psychiatric institution and determined that *"video surveillance cameras were installed in all areas that patients frequent, including their rooms, the sitting-rooms, occupational therapy rooms and corridors, and even inside the toilets, which is a rather delicate matter. As the purpose of such processing they cited security prevention, prevention of self-harm or injury to other persons by patients, the protection of Clinical Centre's property, and lastly evidence in case of an incident, referring to the provisions of the Law on Private Security."*³ During the supervision, it was also determined that patients were not previously informed about the use of video surveillance, and this type of processing of their personal data, nor did the institution have its own internal acts related to risk assessment or any other acts prescribed by the Law on Private Security, which would make such data processing legal. The Commissioner's statement regarding the supervision also states that the practice of psychiatric institutions is rather uneven in this regard, and that there are similar institutions that do not use video surveillance, as well as those in which video surveillance systems are set up, but are limited to certain premises⁴.

Another example of the use of video surveillance by public authorities, which the Commissioner has deemed controversial with regards to the Law on Personal Data Protection,⁵ is the case from 2016, where the communal police used video surveillance system. The Commissioner determined that the communal police have around 250 personal cameras, 216 of which are directly connected to the uniforms of the communal police officers. During the supervision, the Commissioner also noted that the communal police does not have a valid legal basis for the use of these cameras, given that the regulations the communal

3 The Commissioner, Press Releases, Video Surveillance in Psychiatric Institutions Must Be Lawful and Justified in Purpose: <https://www.poverenik.rs/sr/>

4 Ibid.

5 This refers to the previous Law on Personal Data Protection, adopted in 2008, which was in force until the implementation of the new Law on Personal Data Protection, August 21, 2019

police referred to were lower than the Law, which is the only legal basis for such processing of personal data. In addition, according to the Commissioner, these regulations are directly contrary to the provisions of the Law on Communal Police which regulate the possibilities and ways for using technologies for video surveillance of premises and facilities.⁶

The example from 2019, when footage from a public space made its way to the Montenegrin Tabloid "Borba", proves that video leakage poses a real threat. This video surveillance footage shows downtown Belgrade, on October 14, 2019, on evening when, during the promotion of Deputy Mayor of Belgrade, Goran Vesic's new book, one copy was set on fire. According to the "Borba" tabloid, whose article was, in part, broadcasted by the "N1" portal, *the opposition organized the burning of Vesic's book... the recording (the recording of the burning of the book) was allegedly obtained with the help of "one of the security agencies from the former Yugoslavia"*⁷ To date, the origin of this footage has not been clarified, nor it has been determined which type of cameras have been used to make the recording, whom they belong to, who got the hold of the recordings and then delivered it to the tabloid.

More broadly than the issue of (mis)use of video surveillance system, is what has repeatedly happened – the information from security agencies and other public authorities were made publically available and used to discredit political opponents. A well-known example is when health information of one of the Members of the Parliament was read during the National Assembly session, which was broadcasted by RTS.⁸ In addition, it has been shown that the practice of telecommunication providers/operators was such that security agencies had access to their customer data, without any court orders and with no compliance with other procedures,⁹ which poses the question on whether it would be any different with video surveillance system?

6 The Commissioner, Press Releases, A Warning to the Communal Police – Recording Citizens Unlawful and Purposeless <https://www.poverenik.rs/sr/>

7 N1, Tabloids Release Footage from Vesic's Book Promotion, Djilas Claims – A Montage: <http://rs.n1info.com/Vesti/a539217/Tabloidi-objavili-snimke-s-promocije-Vesiceveknjige-Djilas-tvrdi-montaza.html>

8 N1, Zivkovic Demonstrates Injury which Granted Him Medical Discharge from the Army: <http://rs.n1info.com/Vesti/a279908/Kako-su-naprednjaci-dobili-tajne-podatke-o-Zivkovicu.html>

9 SHARE Foundation, Invisible Infrastructures: Electronic Surveillance and Mobile Phone Data Retention: <https://labs.rs/sr/nevidljive-infrastrukture-elektronski-nadzor-i-zadravanje-podataka-sa-mobilnih-telefona/>

KEEPING UP WITH
TRENDS: CAMERAS
AS A MEANS FOR
PROTECTION OR
LEGAL TOOL FOR
CONTROLLING
CITIZENS?

Video surveillance systems are in use across the world, and it is estimated that there are between 4 and 6 million cameras in Great Britain alone. There are over 170 million cameras in China, and of top 10 cities in the world in terms of the existing number of cameras, eight of the cities are Chinese, with remaining two being London (UK) and Atlanta (USA).¹⁰ In the late 20th and early 21st centuries, as a result of the economic reform, computer and internet technologies became extremely developed in China. Nowadays, facial recognition cameras, internet surveillance and mobile app tracking that collect large amount of user data, as well as drones, are the most common mechanism used by the Chinese authorities to massively monitor their citizens. Aside from surveillance system, whose primary goal (at least according to claims made by authorities across the world) is to protect the security, video surveillance updated with facial recognition software is also used in commercial purposes. This means that, via *YouTube* you can watch live stream from different locations in Amsterdam and other parts on the Netherlands,¹¹ which is an example of the so-called *online* tourism. In practice, this means that as a tourist you can stroll through parts of Amsterdam, while your image is being broadcasted live via *YouTube*, without your knowledge or consent. In the State of Florida, facial recognition software are using during football matches (*Super Bowl*), also without knowledge or consent of spectators at the stadium.¹²

Facial recognition technology enables the identification of a specific individual, by using facial recordings of that individual made with this technology, further cross-referenced with another persons' record (for example, the Ministry of Interior's database containing record of all adult citizens of the Republic of Serbia), or by a reverse method, by inserting a photograph of said individual into facial recognition software, to identify all the places this person visited, or locate his current whereabouts.

Back in late 2017 was the first time the issue of mass video surveillance of public spaces in Belgrade was talked and written about. Specifically, the media reported about citizens' observations that new cameras appeared in several locations throughout Belgrade. The Commissioner designated the Ministry of Interior

- • • • •
- 10 South China Morning Post, Cities in China Most Monitored in the World, Report Finds: <https://www.scmp.com/news/china/society/article/3023455/report-finds-cities-china-most-monitored-world>
 - 11 Youtube: <https://www.youtube.com/c/WebCamNL/?gl=NL>
 - 12 T. E. Boulton, PICO: Privacy through Invertible Cryptographic Obscuration: <https://vast.uccs.edu/~tboulton/PAPERS/Boulton-PICO-preprint.pdf>

and the City Administration of the City of Belgrade as two institutions under whose jurisdiction road video surveillance system would fall under. This was followed by contradictory information from the officials: „*The media reported that the Secretary of The Secretariat for the Defense, Emergency Situations, Communications and Coordination of Public Relation claimed that the City Administration is not aware of who is installing the cameras, and they also reported the statement made by the City Manager, suggesting that the cameras are installed by the City of Belgrade, and that they are planning to install an even greater number of them.*“¹³

The supervision later conducted by the Commissioner over these institutions cleared the dilemma, since it was determined that in the second half of 2017, Mol had replaced the technically obsolete cameras with more advanced, next-generation, high-resolution cameras, on 61 different locations. The number of camera locations has not been increased, but fixed cameras were added in specific camera locations (a total of 47 cameras), which was then explained by the need for better visibility, faster search of recorded material and more efficient investigation of criminal offences.¹⁴ The Commissioner assessed that, despite the undisputed legal basis for the said processing of personal data, Mol had failed to adequately inform the public, prior to installing the cameras. This omission, along with newspaper articles and contradictory statements by the officials, caused unnecessary upset for the citizens.

“SAFE CITY” Project

The issue of justifying the introduction of video surveillance system to public areas became urgent in early 2019, when Nebojsa Stefanovic, the Minister of Interior, and Vladimir Rebic, the General Police Director, stated that nearly 1.000 surveillance cameras will be installed in 800 locations in Belgrade in the following period, and that these devices will have the facial recognition and license plates recognition software.¹⁵ The reason for introducing such system, they stated, was to ensure the security of citizens, as well as the crime decrease.

- • • • •
- 13 Insajder, The Commissioner: Who is Installing Cameras in Belgrade and Why: <https://insajder.net/sr/sajt/vazno/9172/>
 - 14 The Commissioner, Press Releases, Video Surveillance – Chronically Unregulated Area: <https://www.poverenik.rs/sr/>
 - 15 N1, The General Police Director: No Room for the Misuse of Cameras: <http://rs.n1info.com/Vesti/a458949/Direktor-policije-Ne-postoji-mogucnost-zloupotrebe-kamera.html>



"We are dealing with smart video surveillance, that involves the installation of high-quality cameras in around 800 locations in Serbia, which will monitor the streets, schools, all check points that the colleagues from Mol deemed necessary to be covered by cameras, based on detailed analysis and risk assessment"; stated Stefanovic, within the introductory lecture on "Modern Technologies in the Development of the Ministry of Interior", which he gave at the University of Criminal Investigation and Police Studies, on the occasion of the beginning of the school year, on October 1, 2019.¹⁶

The Ministry of Interior rejected the request made by journalists and researchers, to deliver the information regarding the procurement process for these devices, the introduction of this system, and other documentation that would confirm that all legal procedures were followed during the procurement and the installation of video surveillance system. In its response to a request to access to information of public importance, submitted by the SHARE Foundation, the Ministry of Interior stated, inter alia, that: *"all documents on the public procurement of video surveillance equipment in Belgrade are labeled 'Confidential', and that the requested information regarding the locations (of cameras) and the analysis are not contained in any document or information carrier, which is a legal precondition for access to information of public importance".¹⁷*

One of the first questions that emerged in the public is to which extent do these systems actually help prevent crime and make it easier to find the perpetrators, and whether relevant public authorities have previously conducted an analysis – an assessment that proves the justification for introducing video surveillance system.¹⁸ On the other hand, the misuse of such data remains another one of the burning questions.¹⁹ Once installed, the cameras record everything within their range, not just the perpetrators. It is important to know who has the access to these recordings, how they are stored, how protected they are from being compromised –

internally or externally, how long they are stored, etc..., given that we have repeatedly witnessed the leakage of video surveillance footage.

Finally, such massive video surveillance can potentially have an impact on other citizens' rights and freedoms, primarily the freedom of speech and the freedom of assembly. *"The feeling that we can be subjected to surveillance and monitoring can motivate us to modify our behavior, meaning it could discourage and distract us from something that is otherwise allowed, for example, to protest or express dissatisfaction publically. It is quite clear that developing such fear goes in favor of those against whom citizens may express dissatisfaction. In addition, collecting a large amount of data about a great number of people can lead to misuse, due to lack of adequate control and too much power given to those in charge of surveillance, in this case employees and officials within Mol."²⁰* An example from Russia testifies to that – namely, one Russian female rights activist has filed a lawsuit against state authorities in Russia, since facial recognition cameras were used to identify her in 2018, when she was protesting in front of the parliament building against an MP, whom several women have accused of sexual harassment.²¹

The public learned the most about the "Safe City" project through a case study conducted by the Huawei Company, the Republic of Serbia's strategic partner on this Project. For promotional purposes, Huawei shared some details regarding the Project timeline on its website – which is a part of a bigger project "Safe Society", where negotiations began back in 2011. In its case study, Huawei states that the Project should include the eLTE technology, smart video surveillance, intelligent transportation system, data center construction, etc... Shortly after parts of this case study became public, it was removed from the company's website.²²

Since the initial statement made by the representatives of the Ministry of Interior, a group of civil society organizations, including Partners Serbia, endeavored to monitor the compliance of procedures with the Constitution of the Republic of Serbia and the existing legislation, despite the lack of transparency of the

16 N1, Stefanovic: Video Surveillance – Less Crime on the Streets of Belgrade: <http://rs.n1info.com/Vesti/a530748/Stefanovic-Video-nadzor-manje-kriminala-na-ulicama-Beograda.html>

17 SHARE Foundation, Are the Locations of the New Surveillance Cameras and the Risks to Citizens' Constitutional Rights Known? <https://www.sharefoundation.info/sr/dali-su-poznate-lokacije-novih-kamera-za-nadzor-i-rizici-po-ustavna-prava-gradjana/>

18 Sasa Djordjevic, Video Surveillance Works No Miracles: <https://pescanik.net/video-nadzor-ne-cini-cuda/>

19 N1, Smart Video Surveillance – Everyone Can Be Monitored at Any Given Time, the Risks Are Enormous: <http://rs.n1info.com/Vesti/a545631/Krivokapic-o-pametnom-video-nadzoru.html>

20 Uros Misljenovic, Should Criminals Be the Only Ones Worried About Video Surveillance? <https://otvorennavratapravosudja.rs teme/ustavno-pravo/da-li-samo-kriminalci-treba-dabudu-zabrinuti-zbog-video-nadzora>

21 Radio Free Europe, Russia: Facial Recognition and Anti-Protest Technology: <https://www.slobodnaevropa.org/a/30205620.html>

22 SHARE Foundation, Huawei Knows All about Cameras in Belgrade, and it's Not Hard for Them to Say So! <https://www.sharefoundation.info/sr/huawei-zna-sve-o-kamerama-ubeogradu-i-nije-im-tesko-da-to-i-kazu/>

process itself. An important part of examining the lawfulness of the announced surveillance system is the development of impact assessment of this Project on citizens' rights. Following the intervention of the civil sector and the Commissioner, the Ministry of Interior drafted this document and delivered it to the Commissioner.²³ Based on this document, SHARE Foundation, Partners Serbia and Belgrade Centre for Security Policy developed *the Analysis of the Mol's Data Protection Impact Assessment on the Use of Smart Video Surveillance*.²⁴ The common conclusion of the Analysis is that the Mol's impact assessment does not meet the formal or material requirements prescribed by the Law,²⁵ and that the Ministry of Interior should postpone the introduction of smart video surveillance until further notice.²⁶ In this Analysis, the three organizations committed to protecting citizens' right to privacy, stated that:

*"The basic question that arises in case of smart video surveillance is its necessity, proportionality and efficiency, given the invasiveness of such measure. Therefore, it is the data controllers', meaning Mol's, additional duty to justify the need for introducing such measure, its proportionality with the purpose expected to be achieved, as well as efficiency in achieving the data processing goals."*²⁷

Regarding Mol's announcement on introduction of video surveillance system, the former Commissioner, Rodoljub Sabic, expressed his concern that *"in the existing conditions, system capable of rapid, automatic identification of each individual whose photograph exists in Mol's official database (meaning all adult citizens, and a significant number of minors as well) can be used, for example, to track political opponents, rather than to combat crime. Sabic also stated that this raises the question as to what extent the covering up of camera locations is in accordance or contrary to*

*the constitutional and legal provisions on recording and monitoring."*²⁸

Mol's Impact Assessment states that the project related to installing road video surveillance system will be done in 2 phases:

- ▶ Phase I (2017) - 100 cameras on 61 locations, the so-called smart video surveillance, with video analytics of materials, including material search in different criteria, license plate recognition;
- ▶ Phase II - 1000 cameras in 800 locations throughout Belgrade, with facial recognition software.²⁹

The Impact Assessment also states that this system is not yet operational. In January 2019, the Minister of Interior stated, as reported by the "Blic" daily newspaper, that this system will be set up in the next two to three years, and would be expanded towards the highway and trunk roads.³⁰ In Minister Nebojsa Stefanovic's later addresses, he stated that *"by the end of next year, 2.000 cameras will be installed in Belgrade"*.³¹

The fact that to this date the citizens have not been informed about the process of introducing smart video surveillance system, and that the associations of citizens did not manage to obtain information on Mol's plans regarding this Project, including the information regarding the number of cameras, locations where they will be installed, and timeframe for the use of smart video surveillance technology, all indicates that there has been a serious breach of the principle of transparency in data processing³².

23 Mol, Data Protection Impact Assessment on the Use of Smart Video Surveillance: <https://www.sharefoundation.info/wp-content/uploads/MUP-Procena-uticaja-obradena-zastitu-podataka-o-licnosti-koriscenjem-sistema-video-nadzora.pdf>

24 SHARE, Partners Serbia and Belgrade Centre for Security Policy, Analysis of the Impact Assessment on Personal Data Protection by Using the Ministry of Interior's Video Surveillance System https://www.sharefoundation.info/wp-content/uploads/Analiza_procene_uticaja_SHARE_Partneri-Srbija_BCBP.pdf

25 This refers to the Law on Personal Data Protection

26 Partners Serbia, Mol to Postpone Introduction of Smart Video Surveillance System until Further Notice: <http://www.partners-serbia.org/mup-do-daljeg-da-obustavi-uvodenje-sistema-za-pametan-video-nadzor/>

27 Ibid.

28 Danas, Sabic: Possible Misuse Of the So-Called Smart Cameras for Video Surveillance: <https://www.danas.rs/drustvo/sabic-moguće-zloupotrebe-takozvanih-inteligentnih-kamera-za-video-nadzor/>

29 Mol, Data Protection Impact Assessment on the Use of Smart Video Surveillance: <https://www.sharefoundation.info/wp-content/uploads/MUP-Procena-uticaja-obradena-zastitu-podataka-o-licnosti-koriscenjem-sistema-video-nadzora.pdf>

30 Blic, Additional 1.000 Cameras to Record Citizens of Belgrade in the Following Years: <https://www.blic.rs/vesti/beograd/beogradane-ce-narednih-godina-na-ulicama-snimati-jos-1000-kamera/ph4m512>

31 This statement was taken by the Mondo portal, and published as news on July 30, 2019: <https://mondo.rs/Info/Beograd/a1208322/Nebojsa-Stefanovic-o-javnim-kamerama-u-Beogradu.html>

32 The Law on Personal Data Protection, Article 5 - Principles of Personal Data Processing: <https://www.paragraf.rs/propisi/zakon-o-zastiti-podataka-o-licnosti.html>



THE LACK OF LEGAL FRAMEWORK

The area of video surveillance has not been properly regulated in the Republic of Serbia. With the adoption of the new Law on Personal Data Protection, the opportunity to better regulate this area was missed, especially considering its implication on citizens' privacy. Certain provisions concerning video surveillance are scattered within laws related to the work of police and other security agencies, and, according to the Law on Private Security, the introduction of video surveillance system has been entrusted to, aside from the police, private security entities (who must obtain certain licenses).

The Authorization for Setting up and Using Video Surveillance System

According to the Law on Police, for the purpose of conducting police duties, the police can monitor and record public places, by using video-acoustic recordings and photographing equipment, in accordance with the regulation on recording and processing data in the area of internal affairs. The Law on Police does not specify what is considered video surveillance, but this definition can be found in the Law on Recording and Processing Data in Internal Affairs, where Article 5 states: *"video-acoustic recording system (video surveillance) is an electronic system for monitoring and recording situations in specific locations and transmission of camera's signal to a predefined location."*³³

33 The Law on Recording and Processing Data in Internal Affairs: <https://www.paragraf.rs/propisi/zakon-evidencijama-obradi-podataka-oblasti-unutrasnjih-poslova.html>

Article 52 of the Law on Police, which refers to recording of public spaces, states that this activity must be publicly announced by the police, and that data collected in this manner shall be kept in the prescribed records, as well as that collected data shall be destroyed within one year. The Law on Police states in a number of different provisions that data collected through video surveillance is stored in accordance with the regulations on keeping records.

By reviewing Article 47 of the Law on Recording and Processing Data in Internal Affairs, which relates to records in the area of video-acoustic recording, inconsistency in these two regulations is revealed. Namely, Article 47 states that *"all data collected by using video-acoustic recordings equipment shall be kept for a minimum of 30 days, and no longer than five years, once the analysis of the data collected helps in identifying people, events and occurrences, which require for the Ministry to take certain measures and actions"*.

In terms of data retention deadlines, these two regulations differentiate. This may be due to the unevenness of regulations, of the fact that the records prescribed in Article 47 of the Law on Recording and Processing Data in Internal Affairs, does not, in fact, refer to the records referred in Article 52 of the Law on Police. If the latter is true, it raises the question of which article regulates records kept by the police for the activity of recording of public spaces (Article 52 of the Law on Police)?³⁴

Aside from the police, the communal police are also authorized to conduct audio and video recordings within its own jurisdiction, and article 25 of the Law on Communal Police states: *"the communal police conduct audio and video recordings of public spaces,*

34 For more, see: Analysis of the MoI's Data Protection Impact Assessment on the Use of Smart Video Surveillance, pages 16-17: https://www.sharefoundation.info/wp-content/uploads/Analiza_procene_uticaja_SHARE_Partneri-Srbija_BCBP.pdf

for the purpose of performing communal-police duties, by using video-acoustic recordings and photographing equipment. For the purpose of exercising its communal-police duties, detecting and prosecuting offences, as well as controlling and analyzing the actions of communal police staff, the communal police may make audio and video recordings of their conduct.”³⁵

The authorities of the Military Security Agency (MSA) and the Military Intelligence Agency (MIA) state that MSA and MIA officials have the right to use means of surveillance, recording, navigation and communication, as well as to use any natural or legal person's means of transportation or communication, as well as that other state authorities or legal entities are obliged to provide them with the assistance necessary for performing tasks within their own jurisdiction.³⁶ The authorities of the Security Information Agency have been regulated in a similar manner, in terms of recording. Here, a distinction should be made with respect to the aforementioned authorities of the police, pertaining to the permission/possibility of setting up and using cameras in public spaces and roads, while the authorities of security agencies relate to the secret surveillance of specific persons (for which there must be an appropriate permit from the competent authority).

In addition to law enforcement agencies, video surveillance systems can only be installed and serviced by legal entities operating in the area of private security. The Law on Private Security defines private security as security that entails:

“providing services or activities related to protection of persons, property and operating with physical and technical protection, when such activities are not under the exclusive jurisdiction of the authorities, as well as affairs of transporting money, valuables and other shipments, maintaining order in public gatherings, sporting events and other public spaces (monitoring), performed by legal entities and entrepreneurs registered for performing such activities.”³⁷

35 The Law on Communal Police https://www.paragraf.rs/propisi/zakon_o_komunalnoj_policiji.html

36 The Law on the Military Security Agency and the Military Intelligence Agency, Article 33 – Special Authorities: https://www.paragraf.rs/propisi/zakon_o_vojnobezbednosnoj_agenciji_i_vojnoobavestajnoj_agenciji.html

37 The Law on Private Security: https://www.paragraf.rs/propisi/zakon_o_privatnom_obezbedjenju.html

The Law further states that these activities may be performed by legal entities, entrepreneurs and natural persons, licensed by the Ministry of Interior to carry out activities related to private security.

Thus, rules for the use of video surveillance system which have been established in such way do cause problems in practice. This means that, public institutions (for example schools), in need of video surveillance system, are obligated to contact private entities licensed by Mol. Given the lack of awareness of institutions regarding the protection of privacy, and insufficient knowledge of legislature in the area of personal data protection, and for such an important task a private firm is to be hired, there is a justifiable concern whether these entities will properly regulate contractual deadlines for storing and accessing video recordings, liabilities for leakage and misuse of those recordings, etc...

Personal Data Protection and the Use of Video Surveillance System

Despite the fact that the adoption of the new Law on Personal Data Protection was necessary, the long-awaited adoption of this regulation has provoked negative reactions from the academic community, and especially civil society organizations dealing with personal data protection.

From the aspect of video surveillance, there are no provisions regulating this area, which were foreseen by the Model of the Law on Personal Data Protection, which was developed by the Commissioner (the Model of the Law),³⁸ which was not taken into consideration by the Ministry of Justice, when drafting the new Law on Personal Data Protection. Articles 37-42 of the Model of the Law regulated the area of establishing and performing video surveillance of public spaces, business and private

38 Model of the Law on Personal Data Protection: <https://www.poverenik.rs/sr-yu/>



premises, as well as obligations relating to personal data controllers and processors.

Then, in order to align with the legal framework in the European Union, the new Law introduced the provisions of the General Data Protection Regulation (GDPR) and the Police Directive of the European Union. This resulted in a great number of exceptions related to investigative and prosecuting authorities, which makes the interpretation of the Law more difficult, and gives more freedom to these authorities when processing data. However, it was the European Commission that, in comments made to the Draft Law on Personal Data Protection, pointed out that the provisions from these two documents need to be transposed into the national legislation, through two separate laws. Furthermore, within those same comments, the European Commission also states that there is *“a problem in the way in which provisions of two important acts – the Police Directive and the General Data Protection Regulation – have been harmonized in one legal act.”* In effect, the European Commission warns that a *“great number of exceptions makes the Draft Law extremely complicated, and, thus, less transparent”*. This refers to *“more than 40 exceptions to the general rules regarding the authority of institutions in charge of preventing, investigating and detecting criminal offences, prosecuting perpetrators, imposing criminal sanctions, including the safeguarding and prevention of threats to public and national security.”*³⁹

The investigative and prosecuting institutions are also supported by the fact that Article 40 of the Law, which refers to limitation of the right to be informed on data processing, does not state that these rights can be limited only if determined by other (specific, sectoral) laws.⁴⁰ Failing to specify this article left room for public authorities or private companies dealing with personal data to possibly limit citizens' right to be informed about how their personal data is processed, without any explicit legal authorization and at their own discretion.

•••••

39 For more, see Partners Serbia Announcement: The EC Comments on the Draft of PDP Law Finally Available to Public: <https://www.partners-serbia.org/komentari-evropske-komisije-o-nacrtu-zakona-o-zastiti-podataka-o-licnosti-konacno-dostupni-javnosti/>

40 Partners Serbia, Retaining Constitutional Guarantee of Citizens' Rights in the New Law on Personal Data Protection: <http://www.partners-serbia.org/zadrzati-ustavnu-garanciju-prava-gradana-u-novom-zakonu-o-zastiti-podataka-o-licnosti/>

Taking all this into account, it is rather expected that people are quite fearful that their privacy is not sufficiently protected. That fear is further justified when public authorities use the media to announce activities that have a great impact on personal data protection; such is the case with the introduction of smart video surveillance system. Even if the new Law on Personal Data Protection does not contain special provisions relating to video surveillance, all provisions of laws governing the rules and standards for the processing of personal data relate to this area. According to the principles of the Law on Personal Data Protection, personal data must be processed *“in a lawful, fair and transparent manner”*, meaning that personal data must be processed in accordance with this Law and other laws regulating the processing of personal data. Furthermore, personal data can be processed only following the previously determined purpose, an explicit, justified and lawful purpose. The Law provides for a number of obligations for data controllers and processors, the rights of persons whose data is being processed – including the right to judicial protection, as well as sanctions for data controllers and processors, who are processing personal data contrary to the Law.

When considering the introduction of video surveillance system, especially introduction of facial recognition software, which is very invasive of the citizens' privacy, it is important to bear in mind the principle of data minimization, determined by the Law on Personal Data Protection. In particular, it is necessary to determine whether in this given case it is really necessary to install such video surveillance system, and whether the purpose for which such video surveillance system is being set up can be fulfilled by some other tool, which is less invasive of privacy. In case of smart video surveillance system, which is planned to be installed in the City of Belgrade, the purpose for setting up the surveillance, according to the documentation made available to the public, is to *increase the security of citizens and contribute to prosecuting of various cases relating to the security of traffic participants, as well as the general security.*⁴¹ It is up to the Ministry of Interior, as the enforcer of this activity, to determine whether improving the security of citizens and prosecuting

•••••

41 Mol, Data Protection Impact Assessment on the Use of Smart Video Surveillance: <https://www.sharefoundation.info/wp-content/uploads/MUP-Procena-uticaja-obrade-na-zastitu-podataka-o-licnosti-korisnjenjem-sistema-video-nadzora.pdf>



security-related cases can be accomplished by other methods that would have a smaller impact on citizens' privacy. Could the same purpose be achieved with an increased number of patrols in busier parts of town or in locations where traffic regulations are estimated to be most often violated, or even by installing "regular" cameras, meaning video surveillance which does not contain facial recognition software? A serious analysis from the Ministry of Interior, justifying the introduction of such mass video surveillance of public spaces was not presented to the public.

Officials' statements failed to reveal whether the Ministry of Interior had implemented all the procedures preceding the introduction of smart video surveillance system, which they are required to follow, according to the Law on Personal Data Protection. The Commissioner's statement⁴² indicates that the Ministry of Interior did not seek the Commissioner's opinion regarding the introduction of video surveillance, nor did it assess the impact of such data processing on the protection of personal data, prior to having announced the introduction of new video surveillance. Namely, Article 54 of the Law on Personal Data Protection states that:

In case it is likely that a certain type of processing, especially using new technologies, and taking into account the nature, scope, circumstances and purpose of processing, will cause a high risk to the rights and freedoms of individuals, data controller is under obligation to conduct an impact assessment of planned processing activities on the protection of personal data, prior to initiating the processing procedure.

Article 54 further prescribes that in case processing of personal data relates to *systematic surveillance over publicly accessible locations to a large extent*, data controller is required to conduct an impact assessment.

It was only after the Commissioner has conducted supervision (on his own initiative), that Mol had drafted and delivered the document assessing the impact of processing of personal data on the protection of personal data.⁴³


42 The Commissioner conducted supervision regarding the announcement of installation of video cameras by the Ministry of Interior: <https://www.poverenik.rs/sr/>

43 Mol, Data Protection Impact Assessment on the Use of Smart Video Surveillance: <https://www.sharefoundation.>

Therefore, when introducing video surveillance system in public spaces and on a large scale, as is the case in the above-mentioned example, it is necessary to conduct an impact assessment of such system on the rights of citizens. In case such assessment shows that the foreseen activity or project might have great consequences on citizens' right to privacy, the project initiators (in this case Mol) should make adjustments to the project, in order to diminish its impact on privacy and other citizens' rights. The fact that Mol began drafting this Assessment, after already having undertaken certain steps in implementing the Project, indicates the lack of awareness within this institution about the necessity to act in full compliance with the obligations prescribed in the Law on Personal Data Protection. This implies that, on a proactive basis, the reasons for introducing the planned surveillance system should first be clearly defined, and then the scope, based on which the purpose and means for collecting and further processing of data can be determined, followed by the identification of weaknesses of planned video surveillance system, in terms of procedures and measures for protection of data, and the removal of risks of illegal use of the data (or at least attempt to reduce them to the lowest possible level). Subsequent Mol actions in this regard are more than welcome, but whether they are sufficient, in terms of processing and protection of personal data, or whether the system will be green-lighted, should be determined by the Commissioner, as the institution responsible for monitoring the implementation of the Law on Personal Data Protection.



CONCLUSIONS AND RECOMMENDATIONS



The shortcomings of the legal regulation of video surveillance in Serbia justify the growing fear and concerns. The right to privacy – the right to personal data protection – although relatively well regulated in Serbia, is opposed to the interests regarding the protection of security, which is the reason why such surveillance systems are most often introduced. When the efforts to protect security by introducing video surveillance system are followed by equal efforts to protect citizens' privacy, these two interests need not be conflicted. Unfortunately, the practice shows that more attention is being paid to developing rules and procedures to ensure lawful and ethical use of video surveillance system. At the first glance, the hardware and software that are found within the video surveillance system's infrastructure seem "flawless" because, allegedly, the people are the ones making mistakes, not the technology. But these systems are administered by people, so irregularities are possible as the consequence of three factors: intentional misuse, ignorance or negligence. It is equally important to bear in mind that these "machines" are also made by people, who may chose to incorporate in them with certain working principles that are not necessarily ethical. These seemingly neutral surveillance systems have turned out to be a means for controlling and monitoring of specific categories of population (ethnic minorities, the poor, activists and human rights defenders, etc...)⁴⁴. Such practices challenge the assumption that surveillance systems are impartial simply because they are managed by algorithms.

In a democracy, introducing video surveillance of public spaces must meet the transparency standards, and public authorities are required to inform the public about the plans for setting up video surveillance, before actually installing them. This should also include an expert justification explaining why such system is needed and to what extent does it contribute to improving security of citizens. Studies have shown that introducing video surveillance does not necessarily have an impact on improving the security of citizens, since the criminal and violent activities "migrate" to those locations that are under no video

44 Slate, The Color of Surveillance: <https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html>



surveillance.⁴⁵ This is why it is necessary to have a professional analysis prior to introducing video surveillance, in order to determine which methods of prevention are the most suitable for increasing the level of security within a specific location. The lack of awareness regarding how important the protection of privacy in a democratic society is can easily turn us into a “police state”, where human rights are permanently suspended at the expense of the alleged protection of the security of citizens. This is why such systems must meet the standards prescribed by the Law on Personal Data Protection.

Concerns that video surveillance may have detrimental implications for the personal data protection also stems from the fact that public authorities in the Republic of Serbia have a low degree of compliance in terms of proceedings and internal procedures with domestic regulations and international standards related to personal data protection, and in this case the provisions of other laws which regulate the use of video surveillance systems. Various public authorities may use video surveillance system as a means of exercising their powers. However, much like in the mentioned case with psychiatric institutions, they do not have equitable practices, and are often dependent on the heads of their institutions.

In addition to consequences on the privacy of citizens, video surveillance has potential implications on other rights – the freedom of speech and the freedom of assembly. If we are aware that “we” are being watched, we will feel less at liberty to express our views and/or take to the streets to peacefully protest against decisions made by the public institutions and people who govern them. The information from across the world are quite worrying, since they seem to indicate that such technologies are being used as a means of mass surveillance of citizens, aimed at keeping them “under control”. Russian activists claim that facial recognition technologies are being used to identify the protesters, given that many protests are being organized without the permission of the authorities.⁴⁶ Such practice, combined with

45 T. E. Boulton, PICO: Privacy through Invertible Cryptographic Obscuration, page 3: <https://vast.uccs.edu/~tboulton/PAPERS/Boulton-PICO-preprint.pdf>

46 Radio Free Europe, Russia: Facial Recognition and Anti-Protest Technology: <https://www.slobodnaevropa.org/a/30205620.html>

the tendency to curb the regulations providing for the right to organize and take part in protests, threatens to diminish the citizens’ rights to express their dissatisfaction against decisions brought by the state and its authorities, which are guaranteed by the Constitution.

Finally, in a country where trust in institutions is not on a very high level, where personal data is often misused, certain concerns whether video surveillance system may also be misused by the state rightfully exist.

In accordance with the conclusions, the recommendations for improving rules and practices regarding the use of video surveillance system refer primarily to:

- ▶ Legal regulation of video surveillance system by adopting a law that would govern this area in great detail, including the legal regulation of facial recognition technologies.
- ▶ Harmonization of setting up and using video surveillance system with the Law on Personal Data Protection.
- ▶ Drafting of preliminary analysis, proving that the introduction of such system is necessary for improving the security of citizens and property, including a previous assessment of the impact such system might have on the protection of the citizens’ right to privacy.
- ▶ Increasing the transparency of the work of public authorities when introducing such systems.
- ▶ Providing a protection system, in order to protect the collected data from potentially being compromised, either internally or externally.
- ▶ Adequately regulate the accountability in cases of manipulation or misuse of data collected by using video surveillance in regulations issued by public authorities, and in internal policies and procedures of entities that set up and use video surveillance systems.

