Original scientific paper
UDK: 340.134: 308(497.4/.7)
DOI: 10.5937/jrs16-27170
Received: 20 June 2020 / Accepted: 30 December 2020

Comparative Analysis of Video Surveillance Regulation in Data Protection Laws in the Former Yugoslav States*

ĐORĐE KRIVOKAPIĆ**
Faculty of Organisational Sciences, University of Belgrade, Serbia / Masaryk University, Czechia

DANILO KRIVOKAPIĆ***
Share Foundation, Serbia

JELENA ADAMOVIĆ****
Share Foundation, Serbia

ALEKSANDRA STEFANOVIĆ*****
Faculty of Law, University of Belgrade, Serbia

Abstract: Video surveillance, the monitoring of a specific area, event, activity or person through an electronic device or a system for visual monitoring is already established as a central tool of public security policy. Video surveillance represents a starting point for implementing advanced technologies such as automatic number plate recognition (ANPR) and automatic facial recognition (AFR), which tend to become standards in many urban areas. Based on the increased use of video surveillance technologies, governments and private actors' capabilities in terms of monitoring of the population and potentially violating fundamental human rights are colossally increased. The article will provide a comparative analysis of national regulatory frameworks of video surveillance in public spaces in former Yugoslav states and its compliance with standards provided by new data protection regulatory framework, particularly General Data Protection Regulation (GDPR). The article will also give an overview of the major violations of the right to privacy by video surveillance and insight into and potential impact of new projects and technologies currently under deployment in the observed countries.

Keywords: surveillance, facial recognition, privacy, regulatory framework, former Yugoslav states

* This article is supported by the European Regional Development Fund (ERDF) project "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).
** *krivokapic@fon.rs*
*** *danilo@sharedefense.org*
**** *jelenaa@sharedefense.org*
***** *aleksandra.stef97@gmail.com*

Video Surveillance Fundamentals

The digital revolution in the 21st century brings a paradigm shift in the way we use technology, approach everyday problems and responsibilities, and change the essence of the industries and public services. For governments, it usually means the development of digital service delivery across government and making services available digitally from start to finish. The ongoing trend of the digital transformation of the public sector requires the deployment of various information technologies in the work of public bodies. These processes may contribute to make governments more efficient but also create privacy risks and information harm.[1]

Video surveillance, the monitoring of a specific area, event, activity, or person through an electronic device or system for visual monitoring,[2] is already established as a central tool of public security policy[3] and it is expected that the police use of integrated and highly sophisticated video surveillance platforms will continue to increase.[4] The blurring of boundaries between public and private operations will continue, as many actors from the private sector are using video surveillance for their daily operation, and the overlap between police use will become more entangled with that of private and commercial organizations.[5] Also, video surveillance represents a starting point for implementing advanced technologies such as automatic number plate recognition (ANPR) and automatic facial recognition (AFR) which tend to become standards in many urban areas.

Based on the increased use of video surveillance technologies, governments' capabilities in terms of monitoring of its population are colossally increased. It was estimated that London, which was for an extended period known as the CCTV capital of the world, had around 627,000 surveillance cameras in 2019 and that an average person commuting to work and back with a one-hour lunch break walking around London could be captured by as many as 300 CCTV cameras during their standard working day.[6] However, with 68.40 cameras per 1,000 people, London is far behind Chinese cities Chongqing and Shenzhen estimated as having 168.03 and 159.09 cameras per 1,000 people.[7] The increasing expansion of video surveillance is the most visible in China. It has been reported that 176 million cameras operate across China, and by 2022, China could have one public CCTV camera for every two people.[8] Police forces on the outskirts of Beijing are trialing facial recognition sunglasses, a programme known as 'Sharp Eyes' in the province of Xionping

1 Niculescu-Dinca 2012, 104.

2 Definition provided by the *Glossary* of the European Data Protection Supervisor. Accessed April 4, 2020. https://edps.europa.eu/node/3116#video_surveillance.

3 Heilmann 2011, 369.

4 UK Surveillance Camera Commissioner 2019, 1.

5 *Ibid.*

6 CCTV Installer 2019.

7 Bischoff 2019.

8 *Ibid.*

which combines video surveillance technology and AFR.[9] In combination with the already established country's social credit system, these infrastructures could soon restrict individuals' freedom of movement and other rights.

The surveillance technology market is also rapidly developing, creating a new type of economy.[10] It is estimated that the world market for Video Surveillance products in 2018 was $17.57 billion. It will grow much faster than previously expected to reach $32.64 billion in 2023, due to the more innovative and better products and increased demand for AI Video Analytics.[11] We are witnessing a race where numerous manufacturers and solution providers are offering their cutting edge video surveillance solutions across the globe. The ECU-911 system which has been deployed in Ecuador was manufactured jointly by China's state-backed C.E.I.E.C and Huawei, and consists of as many as 4,200 cameras, monitored by 16 centers and around 3,000 employees. The system lets the government track phones, and may soon be upgraded with facial-recognition capabilities.[12]

The article will review national regulatory frameworks applicable to video surveillance in public spaces in former Yugoslav states in order to assess regulatory approaches, compliance with newly adopted data protection standards and practical implications of deployment of such technology. It will start with the assessment of the impact of video surveillance on fundamental rights, continue with relevance of GDPR for video surveillance and then present comparative analysis and overview of the major violations of the right to privacy by video surveillance in former Yugoslav states.

Impact of Video Surveillance on Fundamental Rights

The establishment of surveillance infrastructures could decrease undesired behavior and sometimes increase pro-social behavior.[13] Still, it could also limit our personal freedoms, e.g. the cameras are reminding citizens of the human surveyor potentially influencing behavioral change.[14] Considering that at the present stage of social and technological development data collected about us are used as a resource controlled by surveilling parties, we should restrict our behavior to keep control over ourselves, our identity and reputation.

There is clear evidence that video surveillance, even in its basic form like CCTV, is a substantial threat to fundamental human rights, raising concerns primarily regarding the right to privacy but also freedom of expression and assembly.[15] These concerns are espe-

9 UK Surveillance Camera Commissioner 2019, 5.

10 Schneier 2015, 46; Zuboff 2019, 8–12.

11 Memoori Research 2019.

12 Porter 2019.

13 Jansen *et al.* 2018, 10.

14 Oulasvirta *et al.* 2012, 49.

15 Goold 2010, 27.

cially justified regarding video surveillance of publicly available spaces. Although our expectation of privacy is somehow limited in public, there are strong social conventions that help us enjoy a reasonable level of privacy on the streets, in public transport, restaurants, leisure spaces etc. which enable us to feel anonymous and lose oneself in the crowd.[16] Special consideration should be paid to political freedoms in the context of protests and other forms of execution of freedom of assembly and expression. It is unlikely that citizens are going to freely express their views and oppose the system if they are aware of the capacity of CCTV networks to precisely document their actions.

The development and deployment of advanced technological systems, capable of collecting a vast amount of data, is happening at an increasing pace – with design decisions concerning personal data models and flows, categories and processing algorithms largely closed from public debate.[17] Therefore, it is necessary to pay more attention to balancing the interest of public safety and citizens freedoms. These systems should only be used to prevent crime, promote public safety, and never gather information about citizens' political views or activities.[18] Democratic states respecting human rights have already established a strict regulatory framework about video surveillance. They are under debate on how to efficiently regulate the employment of connected technologies such as ANPR, AFR and others.

At first sight, the former Yugoslav states promote the use of video surveillance rather than regulate it. Video surveillance is perceived as an effective tool to make public and private spaces safer, reduce the level of criminal activity, optimize the work of security apparatus and mitigate ongoing "security deficit". In Serbia, Huawei's surveillance system with 1,000 high-definition cameras, which could use ANPR and AFR, will be installed in 800 locations across the Serbian capital over the next two years.[19]

Video surveillance of public and publicly available private spaces should be consistent with human rights standards. The public should be fully informed about the purpose, operation, and regulation of the systems and trust that the systems will not be abused and that over time they will not be used in a political context.[20]

16 *Ibid.*

17 Niculescu-Dinca 2012, 104.

18 Goold 2010, 32.

19 Stojkovski 2019.

20 Goold 2010, 33.

Video Surveillance and GDPR

In May 2018, a General Data Protection Regulation (GDPR) came into force, placing personal data under unprecedented protection. It was the finale of a six-year-long process, with 4,000 amendments submitted to the text itself. Simultaneously, almost all relevant actors from the public, private and civil sectors participated in the public debate. GDPR sets new standards in personal data protection and is directly applicable in all 28 EU Member States. Its significance goes far beyond EU borders since, after 2016, many countries modelled their data protection framework after GDPR.

GDPR General Principles

Without making specific reference to video surveillance, but having in mind that this kind of footage often contains images that can be used to identify natural persons either directly or indirectly, GDPR qualifies them as personal data which means that all rules and principles laid down in GDPR apply to video surveillance. More precisely, this means that six principles relating to the processing of personal data laid down in Article 5 of GDPR must be respected by any entity deploying video surveillance. European Data Protection Board has issued Guidelines regarding the processing of personal data through video devices (EDPB Guidelines), which deal with many relevant aspects of such processing, including the application of principles in practice.

1. Lawfulness, fairness and transparency – This principle means that before video surveillance begins, the legal basis for this kind of data processing needs to be established by the new rules.[21] Every natural person whose data is processed needs to be informed about the data controller's identity and the purpose of data processing. Contact of data controllers must be publicly available. There needs to be an announcement, poster or mark that a particular place or object is under video surveillance around every system or even a camera. Natural persons should be made aware of risks, rules, safeguards and rights about processing personal data and how to exercise their rights concerning such processing. According to EDPB Guidelines, the most essential information should be displayed on the warning sign itself (first layer). In contrast, the further mandatory details may be provided by other means (second layer).[22]

2. Purpose limitation – For every kind of video surveillance, there needs to be a legitimate purpose for which data is collected. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined when collecting personal data.[23] The position taken in the EDPB Guidelines is that the mere purpose of "safety"

21 The GDPR, Article 6, states that in order for the processing to be lawful, personal data should be processed on the basis of consent or if processing is necessary for the performance of a contract, compliance with a legal obligation, for protecting a vital interest, for the performance of a task in the public interest or for the purposes of the legitimate interests.

22 EDPB Guidelines, paras 111–119.

23 GDPR 2016, 39.

or "for your safety" is not sufficiently specific.[24] Besides, data collected for particular purposes cannot be used for any other incompatible purpose.

3. Data minimization – This principle means that one should only collect personal data necessary for the specified purpose. There is no need for setting up cameras everywhere around the monitored place or object. It is enough to define a target that is at risk and the spot covering enough angles for everything to be seen to achieve the purpose of using video surveillance.[25] This principle should be kept in mind when choosing between black box solutions and real-time monitoring and the possibility to rely on the intervention of security personnel.[26]

4. Accuracy – This principle means that personal data shall be accurate and, where necessary, kept up to date. It is most relevant about facial recognition technology that promises precise identification of natural persons regarding video surveillance. Nevertheless, studies have highlighted how the algorithms trained on racially biased data sets misidentify people.[27] This is particularly worrying if it results in unlawful arrests or leads public agencies and private companies to discriminate.

5. Storage limitation – This principle means that personal data need to be kept in such form that identification of data subject is no longer possible after the purpose for data processing is achieved. Even if installing cameras is justified for security purposes, the timely and automatic deletion of video footage is crucial. The standard for retaining video footage would be "as long as necessary, as short as possible", although sometimes legal framework imposes fixed periods. According to EDPB Guidelines, in general, it could be said that in the vast majority of cases data should be erased after a few days since within that period, the purpose will be fulfilled. The longer the storage period is set, and especially when beyond 72 hours, there should be more argumentation for the legitimacy of the purpose and the necessity for such storage.[28] Video surveillance systems that constantly record and store images indefinitely will be in breach of this provision.

6. Integrity and confidentiality – In video surveillance system integrity can be referred to using a robust system because the ability to connect a camera to the internet is considered as smart technology. Still, it also provides additional points of access for hackers. For ensuring that there will not be personal data leaks and hacks, it is best to stay updated with the latest cybersecurity practices and, also, to ensure that the system is updated and adequately maintained. These kinds of practices are helping data subjects gain trust in data processors and feel that their privacy will not be violated. The respect for "privacy by design" and "privacy by default" rules is also of the utmost importance when complying

24 EDPB Guidelines, para 15.

25 Genetec 2017.

26 EDPB Guidelines, para 29.

27 Snow 2018.

28 EDPB Guidelines, para 121.

with this principle. When it comes to technical measures, data protection, and privacy safeguards should be built into the technology's design specifications. When it comes to organizational practices, appropriate management framework, policies, and procedures should be in place from the outset.[29]

Specific Rules – DPIA and DPO

One of the most important novelties of GDPR is the obligation for data controllers to carry out data protection impact assessment (DPIA) in situations when the use of new technologies, as well as context and purpose of data processing, are likely to result in the high risk to the rights and freedoms of natural persons. Many video surveillance systems can cause this risk, such as facial recognition technology for profiling purposes or monitoring large scale publicly accessible areas like squares, parks, airports etc.[30] In these situations, every data controller must determine risks associated with their system through DPIA. GDPR prescribes the minimum content of DPIA.[31]

Designation of data protection officer (DPO)[32] is also an obligation in any case where the processing of personal data, by virtue of their nature, their scope and their purposes, requires regular and systematic monitoring of data subjects on a large scale which often happens with video surveillance systems.

State of Affairs in the Former Yugoslav States

To map and compare the standards of personal data processing in video surveillance, laws, policies and practices in six former Yugoslav states were examined: Serbia, Croatia, Slovenia, Montenegro, Bosnia and Herzegovina and North Macedonia.[33] It should be noted that two countries, i.e. Slovenia and Croatia, are the EU Member States and that the General Data Protection Regulation (GDPR) applies directly on their territory. While Croatia has adopted a national law implementing the GDPR, Slovenia is one of the few remaining EU Member States yet to adopt a new data protection law and incorporate the GDPR rules in their national legal system.

29 *Ibid*., paras 126–127.

30 GDPR Article 35(3)(c) explicitly states that DPIA will be required in case of systematic monitoring of publicly accessible areas on a large scale.

31 Article 35 (7) of GDPR prescribes that DPIA shall contain at least: a systematic description of the envisaged processing operations and the purposes of the processing, an assessment of the necessity and proportionality of the processing, an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph and the measures envisaged to address the risks.

32 Article 37 of GDPR.

33 The research has been performed with the support of the Share Foundation and associates.

For this comparative research, the authors have studied the national legal frameworks, i.e. data protection laws and bylaws about video surveillance, national data protection authorities (DPAs) and their practice in matters relating to data processing in the context of video surveillance, relevant opinions and decisions of DPAs, cases of abuse of video surveillance reported on by the media, case law before the national courts and the European Court of Human Rights, etc. Outside the scope of this research are rules on video surveillance not regulated by data protection laws but by sectoral regulation, particularly relevant internal affairs legislation which usually regulates video surveillance use by the police.[34]

Country	**Laws complied with GDPR**	**Laws (and abbreviations)**
Slovenia (EU Member State)	GDPR applies directly, national law in procedure[35]	ZAKON O VARSTVU OSEBNIH PODATKOV (**ZVOP-1**)[36] (DRAFT) ZAKON O VARSTVU OSEBNIH PODATKOV (**ZVOP-2**)[37]
Croatia (EU Member State)	Yes (GDPR applies directly)	ZAKON O PROVEDBI OPĆE UREDBE O ZAŠTITI PODATAKA (**ZPOUZP**)[38]
Serbia (EU Candidate)	Yes	ZAKON O ZAŠTITI PODATAKA O LIČNOSTI (**ZZPLS**)[39]
North Macedonia (EU Candidate)	Yes	ЗАКОН ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ (**ZZLPNM-1**)[40] ЗАКОН ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ (**ZZLPNM-2**)[41]

34 The second part of this article, which is in a process of drafting, will focus on a comparative review of internal affairs legislation which regulates video surveillance in countries of the former Yugoslavia.

35 An omnibus law compliant with the GDPR is in legislative procedure (PDPA 2).

36 Personal Data Protection Act is in Slovene language: Zakon o varstvu osebnih podatkov. ZVOP-1 is its official acronym in Slovene language. This Act was published in: Official Gazette of the Republic of Slovenia, No. 86/2004, as of 5 August 2004 and was partly annulled and corrected by the Information Commissioner Act which was published in: Official Gazette of the Republic of Slovenia, No. 113/2005, as of 16 December 2005. Accessed May 18, 2020. https://rm.coe.int/16806af30c.

37 ZVOP-2 draft. Accessed May 18, 2020. https://www.gov.si/assets/ministrstva/MP/ZVOP-2-14.8.19.pdf.

38 ZPOUZP in Croatia was promulgated on April 26, 2018 and entered into force May 25, 2018. Accessed May 18, 2020. https://www.zakon.hr/z/1023/Zakon-o-provedbi-Op%C4%87e-uredbe-o-za%C5%A1titi-podataka.

39 PDPA applies in Serbia as of August 21, 2019. Accessed May 18, 2020. http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2018/87/13/reg.

40 ZZLPNM-1 came into effect during 2005 and was updated several times („Службен весник на Република Македонија" бр. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015, 99/2016 и 64/2018). Accessed May 18, 2020. https://dzlp.mk/sites/default/files/u4/zakon_za_zashtita_na_lichnite_podatoci.pdf.

41 ZZLPNM-2 was adopted in the latter part of February 2020, but the application has been delayed for 18 months. Accessed May 18, 2020. https://dzlp.mk/sites/default/files/u4/zakon_za_zastita_na_licnite_podatoci.pdf.

Montenegro (EU Candidate)	No	ZAKON O ZAŠTITI PODATAKA O LIČNOSTI (**ZZPLM**)[42]
Bosnia and Herzegovina	No	ZAKON O ZAŠTITI LIČNIH PODATAKA (**ZZLPBH**)[43]

Table 1: *Data Protection Laws (and Drafts)*

In terms of DPAs, three countries have institutions that oversee both personal data protection and freedom of information (Slovenia, Serbia and Montenegro), while the other three have institutions exclusively dealing with data protection matters (Croatia, North Macedonia, Bosnia and Herzegovina).

Country	**Institution**
Slovenia	Information Commissioner[44]
Croatia	Personal Data Protection Agency[45]
Serbia	Commissioner for Information of Public Importaance and Personal Data Protection[46]
North Macedonia	Directorate for Personal Data Protection[47]
Montenegro	Agency for Personal Data Protection and Free Access to Information[48]
Bosnia and Herzegovina	Personal Data Protection Agency[49]

Table 2: *Data Protection Authorities*

42 ZZPLM came into effect during 2008 and was updated several times ("Službeni list Crne Gore", br. 079/08 od 23.12.2008, 070/09 od 21.10.2009, 044/12 od 09.08.2012, 022/17 od 03.04.2017). Accessed May 18, 2020. http://www.azlp.me/docs/zastita/Ustav%20i%20zakoni/Zakon%20o%20ZLP.docx.

43 ZZLPBH came into force during 2006 with amendments and additions from 2011 ("Sl. glasnik BiH", br. 49/2006, 76/2011 i 89/2011 - ispr.). Accessed May 18, 2020. https://www.paragraf.ba/propisi/bih/zakon-o-zastiti-licnih-podataka.html.

44 Information Commissioner of the Republic of Slovenia. Accessed May 18, 2020. https://www.ip-rs.si/.

45 The Croatian Personal Data Protection Agency. Accessed May 18, 2020. https://azop.hr/data-protection-agency.

46 Commissioner for Information of Public Importance and Personal Data Protection, Serbia. Accessed May 18, 2020. www.poverenik.rs.

47 The Directorate for Personal Data Protection, North Macedonia. Accessed May 18, 2020. https://dzlp.mk/.

48 Agency for Personal Data Protection and Free Access to Information, Montenegro. Accessed May 18, 2020. www.azlp.me.

49 Personal Data Protection Agency in Bosnia and Herzegovina. Accessed May 18, 2020. http://azlp.ba.

All countries except Serbia have video surveillance regulated at least in a general sense. Namely, in Serbia, video surveillance is regulated with general data protection provisions while other countries have specific norms in that respect. Review of applicable legislation provided that specific provisions on video surveillance, mainly identified within the data protection laws, could cover: general video surveillance in any context; video surveillance of public spaces; video surveillance of access to official premises and business premises; video surveillance within work areas; video surveillance within residential buildings or within work areas.

Country	Special provisions about video surveillance	Public place	Access to business premises	Within residential buildings	Within work areas[50]
Slovenia	+	-	+	+	+
Croatia	+	+	-	+	+
Serbia	-	-	-	-	-
North Macedonia	+	-	+	+	/
Montenegro	+	+[51]	+	+	+
Bosnia and Herzegovina	+	-	-	-	-

Table 3: *Availability of specific provisions on video surveillance*

Scope of specific rules applicable to all forms of video surveillance varies in different jurisdictions. These rules could be derogated by other laws (for example, by-laws regulating police operations). However, these regulatory solutions usually aim to clarify how data protection principles apply to the implementation of video surveillance.

50 Interpretation of the GDPR and Labor Act by Several surveillance Institutions in the opinions and decisions in certain cases (see in the text below – 1.i. and 3.c. responses) where they interpreted that according to GDPR there could not be surveillance of people for the purpose of measurement of a working performance but there could be video surveillance for safety reasons (e.g. in factory hall). E.g. Croatian GDPR application Act regulates obligatory notice of employees before deciding upon installation of video surveillance and appropriate notice in advance of the employees that will be in the reach of cameras' lenses. In Montenegro's PDPA it is explicitly stated that video surveillance is allowed if there is a risk for employees due to the nature of work.

51 Other norms accordingly applied to regulation of video surveillance in a public place.

Principle	Specific Provisions	Laws reference	Analysis
Lawfulness and Fairness	A special written decision on deployment of a video surveillance system has to be enacted by the Controller in the case that legal basis is not provided by the Law.	ZVOP-1 - / ZVOP-2 Art.108(1) ZPOUZP - / ZZPLS - / ZZLPNM-1 Art. ZZLPNM-2 Art.90(2,4) ZZPLM Art. 35(2,3), 36(3,4) ZZLPBH Art. 21a (2)	At the moment, this principle is regulated in 2 out of 6 state laws (3 after the adoption of ZVOP-2).
Transparency	Mandatory notification that video surveillance is being carried out should be published in a manner that enables the individual to become familiar with the implementation of video surveillance. The notification should include: 1) Identity of Controller and 2) Contact info for citizens to get informed where and how long the recordings are stored and how to execute data subject's rights.	ZVOP-1 Art. 74(2,3) ZVOP-2 Art. 108(2,3) ZPOUZP Art. 27 ZZPLS - / ZZLPNM-1 Art. 9-a ZZLPNM-2 Art. 89 (3,4) ZZPLM Art. 39 ZZLPBH Art. 21a(3)	The principle is regulated in 5 out of 6 state laws.
Purpose limitation	Video surveillance is permitted only about the purpose which is: • necessary and justified related to the security of persons and property (ZPOUZP) • security of persons and property + reducing risks for employees (access to premises and public space) + protection of trade secrets (workspace) (ZZPLM)	ZVOP-1 - / ZVOP-2 - / ZPOUZP Art. 26(1) ZZPLS - / ZZLPNM-1 - / ZZLPNM-2 - / ZZPLM Art. 35-40 ZZLPBH - /	The principle is regulated in 2 out of 6 state laws.
Data minimization	Video surveillance may not be carried out in lifts, toilets, changing rooms and other similar premises, whose individual may reasonably expect a higher level of privacy. (ZVOP-2) Video Surveillance is limited to the premises, parts of premises, outdoor space of premises and indoor space in public transportation (ZPOUZP) The controller may perform video surveillance only on the space that is sufficient for meeting the goals for which it is set. It is prohibited to conduct video surveillance in wardrobes, locker rooms, toilets and other similar premises. ZZLPNM-1 + ZZLPNM-2	ZVOP-1 - / ZVOP-2 Art.108(8) ZPOUZP Art. 26(2) ZZPLS - / ZZLPNM-1 Art. 9-a (5) 9-b(4) ZZLPNM-2 Art.89(6), 90(3) ZZPLM - / ZZLPBH - /	At the moment, this principle is regulated in 3 out of 6 state laws (4 after the adoption of ZVOP-2).
Accuracy	Collection of video surveillance systems shall contain a recording of the individual (picture), the date and time of the shot (+ audio if allowed by the Law). (ZVOP-2) Special records on video surveillance have to be kept which has to include: video and audio record, date and time of the record if needed personal data of recorder person (name, address, employment data, ID number, etc.) (ZZPLM)	ZVOP-1 - / ZVOP-2 Art.108(5) ZPOUZP Art. ZZPLS - / ZZLPNM-1 - /. ZZLPNM-2 - / ZZPLM Art. 37(2)[52] ZZLPBH- /	At the moment, this principle is regulated in 1 out of 6 state laws (2 after the adoption of ZVOP-2).

52 This rule is limited to the video surveillance of entrances to official and business premises, within the working areas and public spaces.

Storage limitation	Maximum 6 months (ZVOP-2) Maximum 6 months (ZPOUZP) Maximum 6 months (ZZPLM) Maximum 30 days (ZZLPNM-1 + ZZLPNM-2)	ZVOP-1- / ZVOP-2 Art.108(7) ZPOUZP Art. 29 ZZPLS - / ZZLPNM-1 Art. 9-a (5) ZZLPNM-2 Art.89(8) ZZPLM Art. 37(3) ZZLPBH /	At the moment, this principle is regulated in 3 out of 6 state laws (4 after the adoption of ZVOP-2).
Integrity and confidentiality	The video surveillance operator shall ensure the possibility of an ex-post for each viewing or use of the recordings determining which recordings were viewed, when, and how they were used or transmitted, by whom has performed these processing acts, when, for what purpose, or on what legal basis, and such it retains the audit trail for five years unless otherwise provided by law. (ZVOP-2) + (ZPOUZP) Protected from unauthorized access (all except Serbia & BIH).	ZVOP-1 Art. 74(5) ZVOP-2 Art. 108(6) + (9) ZPOUZP Art. 28 ZZPLS - / ZZLPNM-1 - / ZZLPNM-2 - / ZZPLM Art. 39(1) ZZLPBH - /	The principle is regulated in 3 (4) out of 6 state laws.

Table 4: *Data protection principles and special provisions related to video surveillance*

Video surveillance of public spaces is covered by legislation in two countries - Croatia and Montenegro - while the latest version of the draft of the Slovenian ZVOP-2 does contain such provision also. The regulatory approach differs, and while in Montenegro it calls for application of the norms related to the access to business premises,[53] in Croatia it limits this activity solely to state authorities in a case it is prescribed by the law and necessary for their operation or protection of life and health of citizens or property.[54] Slovenian ZVOP-2 determines that video surveillance in public areas is only allowed when absolutely necessary and purpose cannot be achieved by less intrusive means.[55] Specified purposes are the existence of serious and reasonable threats to human life or health, property security, protection of classified information, protection of persons, facilities and neighborhoods of facilities protected by the police or the protection of others premises, buildings, or areas protected by law. Video surveillance is only allowed for the public sector officials or authorized security personnel and authorized private security personnel for the private sector.

Two countries, Slovenia[56] and Montenegro,[57] have more detailed provisions on video surveillance of access to official and business premises which mainly limit the purpose of such processing, impose more specific rules on notification of employees and establish rules about technical and organizational measures.

53 ZZPLM Art. 40.

54 ZPOUZP Art. 35.

55 ZVOP-2 Art. 112.

56 ZVOP-1 Art. 75; ZVOP-2 Art. 109.

57 ZZPLM Art. 35.

Four countries (Croatia,[58] Slovenia,[59] Montenegro[60] and North Macedonia[61]) have more detailed provisions on video surveillance within work areas that limit permitted purposes, require notice to employees in advance, and add layers of technical and organizational measures. Laws of Slovenia and Montenegro also require that the opinion of the labor union is taken into account.

Four countries have more detailed provisions for installation of video surveillance within residential buildings, usually with the requirement that the majority of owners must consent to the installation (70% of residents in Slovenia[62] and Montenegro[63] and 2/3 of residents in Croatia[64] and North Macedonia[65]). Video surveillance of access to individual apartments is usually prohibited.

Some of the data protection authorities (DPA) in the six regional countries have had more activities than others in publishing opinions and other documents related to video surveillance data. For example, the Slovenian Information Commissioner published detailed guidelines on data processing by video surveillance in the form of a manual[66] that explains the rules on the introduction of video surveillance and calls attention to the most frequent violations of law in its implementation. The Croatian DPA recently published guidelines for applying the GDPR in preschool institutions,[67] where they specifically prescribed this aspect of video surveillance. It should be highlighted that the Montenegrin DPA issued several positions on different aspects of video surveillance, such as on the recording of employees in official premises,[68] video surveillance of natural persons on their private property,[69] video surveillance in residential buildings,[70] etc.

58 ZPOUZP Art. 30.

59 ZVOP-1 Art. 77; ZVOP-2 Art. 111.

60 ZZPLM Art. 36.

61 ZZLPNM-1 Art. 9-b, ZZLPNM-2 Art. 90.

62 ZVOP-1 Art. 76; ZVOP-2 Art. 110.

63 ZZPLM Art. 38.

64 ZPOUZP Art. 31.

65 ZZLPNM-1 Art. 9-c, ZZLPNM-2 Art. 91.

66 Slovenian Information Commissioner 2015.

67 Croatian Personal Data Protection Agency n.d.

68 The Council of the Agency for Personal Data Protection and Free Access to Information, Montenegro 2019.

69 The Council of the Agency for Personal Data Protection and Free Access to Information, Montenegro 2017.

70 The Council of the Agency for Personal Data Protection and Free Access to Information, Montenegro n.d.

Obligation to Undertake a Specific Assessment of the Video Surveillance System

Among the observed countries, only the North Macedonian legislation prescribes explicit obligation to undertake a particular analysis of surveillance systems usage. According to ZZLPNM-2, the controller is obliged to periodically evaluate the achieved results from the system for performing video surveillance every two years, and especially for: (i) further need to use the system for performing video surveillance, (ii) the purpose, i.e. the goals for performing video surveillance, and (iii) possible technical solutions for replacing the video surveillance system.[71]

Slovenian ZVOP-1 and ZVOP-2 do not generally require special assessment for video surveillance. But they do prescribe one additional checkpoint in case of video surveillance in the employment context. According to ZVOP-2, before introducing video surveillance in a public or private sector, the employer must consult with representative trade unions and the works council, or the workers' confidant, if they exist. The consultation must take place a minimum of 30 days before the intended instalment of the cameras. Upon receipt of any opinion, the employer shall decide on the introduction or non-introduction of video surveillance.[72]

Cases of Abuses

There were numerous cases of abuse of video surveillance which the media from the six countries have reported on. Most cases reported to the public concerning illegal installation and usage of cameras, in violation of principles of purpose limitation and data minimization. In cases when data were leaked to the public, there was also an apparent violation of the principle of integrity and confidentiality.

One of the cases attracting considerable attention was the "Belgrade Arena affair", where a police traffic camera was used to zoom in on a young couple having sexual intercourse in the vicinity of the Belgrade Arena, a large sports and concert hall. The video in question was then uploaded to pornographic websites.[73] Another bizarre case from the Serbian DPA practice concerns the installation of cameras in toilets of the Belgrade Bus Station, under the excuse of fear of a possible terrorist attack.[74] As early as 2006, the Slovenian media reported on the case of security cameras that were installed in a clothing store in a way that changing booths were also visible, so the Information Commissioner had to react and prohibit this practice.[75] Montenegro has also had numerous cases of abuse of

71 Article 92 of ZZLPNM-2.

72 Article 111(5) in ZVOP-2.

73 Mondo 2011.

74 Petrović 2017.

75 Dnevnik 2006.

video surveillance during the past several years. There were even doubts that members of organized crime groups have illegally installed surveillance cameras for their surveillance purposes in many public spaces in the city of Kotor.[76]

Setting up the surveillance system by the Serbian Ministry of Interior (MoI) is one of the most significant ongoing surveillance projects in the region. However, this project from the outset has some serious problems, starting with the principle of lawfulness. Namely, MoI announced the placement of 1,000 Huawei cameras equipped with facial and license plate recognition software on 800 locations in Belgrade at the beginning of 2019. Later, this information was updated many times, and the last document says there will be 8,100 cameras (including body cams and eLTE terminals). However, much of the information regarding the purpose and scope of the surveillance and the use of facial recognition remains unknown to date. Many information given to the public came through media statements by MoI officials. In contrast, the only official documents are two Data Protection Impact Assessments (DPIA) provided by MoI to the Serbian Commissioner[77] (which were prepared mostly under the pressure of Serbian digital rights NGOs).[78] The First DPIA prepared in September of 2019 did not meet formal requirements prescribed by the national legal framework. As noted in the Commissioner's Opinion regarding this respective DPIA,[79] and as analyzed by a number of legal and technology experts from leading Serbian NGO's that have expertise on surveillance topics,[80] DPIA did not provide relevant answers to many of the outstanding issues. It is also not valid from the legal standpoint, as it does not contain the minimum requirements for DPIAs prescribed by the Serbian Personal Data Protection Act, especially in relation to the 'smart' aspect of the video surveillance system. Many practical and technical problems with this system were not sufficiently covered by the DPIA: no comprehensive description of the intended actions on processing personal data in the case of smart video surveillance; no risk assessment regarding the rights and freedoms of the data subjects; no description of the measures that are to be taken in relation to the existence of risks identified; no clarification regarding technical, organizational and personnel measures for data protection. However, the lack of clear legal basis to even begin collection of personal data by using this technology seems to be the most difficult to overcome by MoI. After such response from the Commissioner, MoI prepared a second, updated DPIA[81] in March 2020. This document more closely follows the formal requirements prescribed by the Serbian Personal Data Protection Act and contains more information on how this project will be implemented. Despite this, the Commissioner issued the opinion that using this video surveillance system for the purpose of biometric data processing is not legal at the moment since there is no legal

76 Monitor Online 2016.

77 Ministry of Interior, Serbia 2019; Share Foundation 2020.

78 The project's timeline is provided in English in: Share Foundation 2019b.

79 Serbian Commissioner for Information of Public Importance and Personal Data Protection 2019a.

80 Share Foundation, Partners Serbia, Belgrade Centre for Security Policy 2019.

81 Ministry of Interior, Serbia 2020.

basis for such processing in the national legal framework and MoI did not assess proportionality and necessity of such data processing.[82] In other words, such a system could become legal in Serbia only if changes to the relevant laws are introduced to establish a legal basis for MoI to use this 'intelligent surveillance' in specific situations.

The principle of lawfulness, paired with the principle of purpose limitation, i.e. an obligation to use surveillance only when there is a clear purpose that is allowed, is interpreted in the important European Court of Human Rights (ECtHR) case *Antović and Mirković v. Montenegro*.[83] It was decided in late 2017, and the court ruled in favour of the applicants, meaning that the Montenegrin Government had indeed infringed upon their right to private and family life, guaranteed under Article 8 of the European Convention on Human Rights.[84] The case concerned two professors of the Faculty of Mathematics at the University of Montenegro, who brought a compensation claim against the University of Montenegro, the Montenegrin DPA and the State of Montenegro before the court in Podgorica. They claimed their right to a private life was infringed by an unauthorized collection and processing of their personal data without their consent through the use of video surveillance on school premises. The opinion of the European Court of Human Rights, in this case, was that, in accordance with Article 36 of the Montenegrin PDPA, "[…] video surveillance equipment can also be installed in official or business premises, but only if the aim s[...], notably the safety of people or property or the protection of confidential data, cannot be achieved in any other way. The Court observes that video surveillance was introduced in the present case to ensure the safety of property and people, including students, and for the surveillance of teaching. It is noted that one of those aims, notably the surveillance of teaching, is not provided for by the law at all as a ground for video surveillance."[85]

The illegitimate purpose has also been found to exist by the Croatian Personal Data Protection Agency, in case that concerned surveillance in the workplace. In a case that concerned surveillance systems in municipality building, the Agency took the position that having cameras in the offices where municipality employees work and recording them throughout the day is the processing of personal data without a legitimate purpose.[86] In Slovenia, the Information Commissioner found that the video surveillance owner who installs cameras to record the entrances to his premises along a public road (and thus may also capture part of that road) must ensure that the purposes for which the video surveillance is carried out (security of assets, control of entrances and exits) are fulfilled. If the cameras also capture a passer-by, thereby interfering with their privacy, the Information Commissioner took the position that the controller can only review videos in accordance

82 Serbian Commissioner for Information of Public Importance and Personal Data Protection 2019b.

83 *Antović and Mirković v. Montenegro* no. 70838/13. 2017.

84 *European Convention on Human Rights.*

85 *Antović and Mirković v. Montenegro* no. 70838/13. 2017. Para 59.

86 Croatian Personal Data Protection Agency 2016.

with the purposes laid down by ZVOP-1 for the introduction of video surveillance. This means that in the event of an incident (such as damage or theft of property), the controller may access the video archive, which must be appropriately recorded, but continuous live monitoring is not allowed (because it is not within the purpose of the surveillance). Moreover, it is not in accordance with the allowed purpose to give the recorded video footage of the theft that happened on the public road to the damaged party (who has in a particular case published the video of the theft on Facebook to get information from the public on the identity of the thief).[87]

As the analysis shows, video surveillance is a highly controversial and complicated issue in the former Yugoslav states, with many personal data protection implications. Even with the national DPAs best efforts, cases of abuse occur often. It seems that even with the help of modern legal protection frameworks, such as the GDPR and the national laws which were based upon it, it would be challenging to improve the practice and ensure a higher level of privacy protection, at least for the time being. Certain developments, such as the installation of Huawei facial recognition cameras in Belgrade,[88] raise additional issues, especially since the Serbian PDPA does not contain provisions specifically regulating video surveillance. In such situations, citizens must engage in public discussion regarding this topic, since these kinds of practices can have detrimental effects on young Balkan democracies. In Serbia, citizens took active participation in monitoring the MoI video surveillance projects, among other things, with an effort to map the cameras deployed in Belgrade.[89]

Conclusion

The GDPR text is established as the standard for modern data protection laws, especially in Europe. Therefore, the fact that most ex-Yugoslav states have implemented its rules into their national laws is a step in the right direction, relevant also for video surveillance regulation. Montenegro and Bosnia and Herzegovina should follow this lead. In addition to GDPR, the newly adopted Protocol amending the Convention for the Protection of Individuals about Automatic Processing of Personal Data,[90] i.e. Council of Europe Convention 108+ is relevant as a reaffirmation of the high expectation in the area of data protection for all Council of Europe member countries. Serbia and Croatia have already ratified its text, and it is expected that the other former Yugoslav states should do the same soon.

Video Surveillance should be specifically regulated in a general sense regardless of the purpose and type of controllers performing surveillance including police, businesses, public

87 Slovenian Information Commissioner 2017, 20.

88 Share Foundation 2019a.

89 Citizen initiative hiljade.kamera.rs has mapped more than 1000 cameras on more than 450 locations. Accessed June 18, 2020. https://hiljade.kamera.rs/sr/pocetna/.

90 Council of Europe 2018.

administration or civil sector. Such provisions are lacking only in Serbia. Special rules related to specific spaces/premises are desired to improve legal certainty and facilitate implementation by controllers and processors. Such rules are provided in 4/6 states regarding residential buildings, 3/6 within work areas and business premises and 2/6 regarding public spaces. Also, when regulating video surveillance legislators should put special attention to the implementation of data protection principles and EDPB Guidelines could help. The comparative research shows that the most popular principle for implementation is "Transparency" which can be found in 5/6 states followed by "Data minimization", "Storage limitation" and "Integrity and confidentiality" which are present in the legislation of 4/6 states. "Lawfulness and Fairness" can be found in 3/6 states while the rarest is the implementation of "Purpose limitation" and "Accuracy" principles present in 2/6 states. Additionally, the quality of implementation of data protection principles should be improved based on the EDPB Guidelines. Finally, all countries should follow global (EU) trends and focus on the regulation of implementation of facial recognition technologies related to video surveillance due to its higher risks to human rights and potential for misuse.

Data protection laws aligned with GDPR are requiring DPIA in the case of implementation of video surveillance in public spaces or the use of technologically advanced systems. DPIAs prepared by the Ministry of Interior were only substantial documents officially published about the implementation of the Huawei project in Belgrade, providing at least minimal level of transparency. The supervisory authorities should clarify situations when DPIA is mandatory and provide guidance on its execution as they could provide important safeguards for citizens. Similar guidance should clarify in which situation controllers and processors must appoint data protection officers. Finally, relatively novel data protection regulations should impact sector-specific regulations which establish video surveillance systems, particularly in the security sector.

In conclusion, complex technological solutions and novel regulations will not be easy to implement in accordance with human rights standards. Building capacities of the controllers of video surveillance systems in the public sector should be a priority in areas of data protection, information security and data management. On the other hand, Serbia's example demonstrates that the implementation of major projects by governments in collaboration with global companies is hard to subject to oversight. Therefore, further development of the supervisory authorities' independence and competences, building capacities of digital watchdogs from the civil society sector and raising awareness of the general public are prerequisites for safeguarding our digital rights in the future.

Finally, in order to have comprehensive understanding of impact of video surveillance technologies in public spaces on society and fundamental human rights it would be recommended to collect and analyze data about application of such systems, its technical functionalities, internal procedures with controllers, implemented safeguards for citizens, success of law enforcement processes and crime rates. Such cross-disciplinary analysis could provide solid basis to assess necessity and proportionality of video surveillance systems in years to come.

References

Bischoff, Paul. 2019. "Surveillance camera statistics: which cities have the most CCTV cameras?" *Comparitech*, August 15. Accessed April 4, 2020. https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

CCTV Installer. 2019. "How many CCTV Cameras are there in London?" May 29. Accessed April 4, 2020. https://www.cctv.co.uk/how-many-cctv-cameras-are-there-in-london/.

Council of Europe. 2018. "Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data." Accessed June 19, 2020. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf#globalcontainer.

Croatian Personal Data Protection Agency. 2016. "Decision on surveillance system in offices of a municipality building." December 9. Accessed May 19, 2020. https://azop.hr/images/dokumenti/490/videonadzor-radno-mjesto.pdf.

Croatian Personal Data Protection Agency. n.d. "Guidelines for application of the GDPR in preschool institutions." Accessed May 19, 2020. https://azop.hr/info-servis/detaljnije/primjena-opce-uredbe-o-zastiti-podataka-u-predskolskim-ustanovama.

Dnevnik. 2006. "Security guards peeked into the locker rooms of the Emporium." June 27. Accessed May 19, 2020. https://www.dnevnik.si/186409.

European Convention on Human Rights. Accessed May 19, 2020. https://www.echr.coe.int/documents/convention_eng.pdf.

European Court of Human Rights. 2017. *Antović and Mirković v. Montenegro* no. 70838/13. November 28, 2017. Accessed May 19, 2020. http://hudoc.echr.coe.int/eng?i=001-178904.

European Data Protection Board. 2020. "Guidelines 3/2019 on processing of personal data through video devices Version 2.0, Adopted on 29 January 2020." Accessed October 26, 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices.pdf.

GDPR. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR)." Accessed May 18, 2020. https://gdpr-info.eu/recitals/no-39/.

Genetec. 2017. "What the GDPR means for Video Surveillance. General Data Protection Regulation (GDPR) for video surveillance applications." Whitepaper, 12. Accessed May 18, 2020. https://resources.genetec.com/i/894178-gdpr-video-surveillance/11.

Goold, Benjamin J. 2010. "CCTV and Human Rights." In *Citizens, Cities and Video Surveillance: Towards a Democratic and Responsible Use of CCTV*, 27–35. Paris: European Forum for Urban Security.

Gov.uk. 2019. "UK Surveillance Camera Commissioner's annual report 2019." Accessed on July 10, 2020. https://www.gov.uk/government/publications/surveillance-camera-commissioner-annual-report-2018-to-2019.

Heilmann, Eric. 2011. "Video surveillance and security policy in France: From regulation to widespread acceptance." *Information Polity* 16 (4): 369–377.

Jansen, Anja M., Ellen Giebels, Thomas J. L. van Rompay, and Marianne Junger. 2018. "The Influence of the Presentation of Camera Surveillance on Cheating and Pro-Social Behavior." *Front. Psychol*. 9:1937. doi: 10.3389/fpsyg.2018.01937.

Memoori Research. 2019. "Major Trends in the Video Surveillance Market 2018 to 2023." January 22. Accessed April 4, 2020. https://memoori.com/major-trends-video-surveillance-market-2018-2023/.

Ministry of Interior, Serbia. 2019. "Data Protection Impact Assessment of video surveillance system." Accessed May 19, 2020. https://www.sharefoundation.info/wp-content/uploads/MUP-Procena-uticaja-obrade-na-zastitu-podataka-o-licnosti-koriscenjem-sistema-video-nadzora.pdf.

Ministry of Interior, Serbia. 2020. "Data Protection Impact Assessment of video surveillance system II." March. Accessed November 19, 2020. https://www.sharefoundation.info/Documents/Procena_Uticaja%20_2_0.pdf.

Mondo. 2011. "The Yanks investigate 'sex at the Arena' too." April 27. Accessed May 19, 2020. https://mondo.rs/Info/Drustvo/a205507/I-Ameri-istrazuju-seks-kod-Arene.html.

Monitor Online. 2016. "Abuse of video surveillance: Criminals and police officers like Big Brother." April 29. Accessed May 19, 2020. https://www.monitor.co.me/zloupoterba-video-nadzora-kriminalci-i-policajci-kao-veliki-brat/.

Niculescu-Dinca, Vlad. 2012. "Managing Suspicion and Privacy in Police Information Systems." In *European Data Protection: In Good Health*, edited by Serge Gutwirth, Ronald Leenes, Paul de Hert, Yves Poullet, 104. Dordrecht: Springer Netherlands.

Oulasvirta, Antti, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio and Petri Myllymäki. 2012. "Long-term effects of ubiquitous surveillance in the home." In *UbiComp'12 – Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 41–50. doi: 10.1145/2370216.2370224.

Petrović, Zlatko. 2017. "Recording in progress!" Accessed May 19, 2020. https://resursi.sharefoundation.info/sr/resource/pazi-snima-se/.

Porter, Jon. 2019. "The NYT investigates China's surveillance-state exports." *The Verge*, April 29. Accessed April 4, 2020. https://www.theverge.com/2019/4/29/18522248/china-surveillance-state-exporting-ecuador-senain-ecu-911-privacy-facial-recognition-tracking.

Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* New York: W. W. Norton & Company.

Serbian Commissioner for Information of Public Importance and Personal Data Protection. 2019a. "Opinion on MoI DPIA." November 12. Accessed May 19, 2020. https://praksa.poverenik.rs/predmet/detalji/FB967E2A-AE57-4B2C-8F11-D2739FD85A9B.

Serbian Commissioner for Information of Public Importance and Personal Data Protection. 2019b. "Opinion on MoI DPIA II." November 12. Accessed November 19, 2020. https://www.sharefoundation.info/Documents/Mi%c5%a1ljenje_Poverenika_2_0.pdf.

Share Foundation. 2019a. "Huawei knows everything about cameras in Belgrade – and they are glad to share!" March 29. Accessed May 19, 2020. https://www.sharefoundation.info/en/huawei-knows-everything-about-cameras-in-belgrade-and-they-are-glad-to-share/.

Share Foundation. 2019b. "Serbian government is implementing unlawful video surveillance with face recognition in Belgrade." Accessed May 19, 2020. https://www.sharefoundation.info/wp-content/uploads/Serbia-Video-Surveillance-Policy-brief-final.pdf.

Share Foundation. 2020. "Kamere bez upotrebne dozvole / procena uticaja 2.0." July 31. Accessed November 19, 2020. https://www.sharefoundation.info/sr/kamere-bez-upotrebne-dozvole-procena-uticaja-2-0/.

Slovenian Information Commissioner. 2015. "Guidelines on Video Surveillance." Accessed May 19, 2020. https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Guidelines_videosurveillance_eng.pdf.

Slovenian Information Commissioner. 2017. "Information Commissioner of the Republic of Slovenia Annual Report 2017." Last accessed February 17, 2021. https://www.ip-rs.si/fileadmin/user_upload/Pdf/letna_porocila_ang/Annual2017.pdf.

Snow, Jacob. 2018. "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots." *The American Civil Liberties Union*, July 26. Accessed May 18, 2020. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

Stojkovski, Bojan. 2019. "Big Brother Comes to Belgrade." *Foreign Policy*, June 18. Accessed May 18, 2020. https://foreignpolicy.com/2019/06/18/big-brother-comes-to-belgrade-huawei-china-facial-recognition-vucic/.

The Council of the Agency for Personal Data Protection and Free Access to Information, Montenegro. 2017. "Conclusion on video surveillance of natural persons on their private property." Accessed May 19, 2020. http://www.azlp.me/docs/zastita/Stavovi%20Savjeta/Zaklju%C4%8Dak%20o%20nenadle%C5%BEnost%20za%20video%20nadzor%20fizi%C4%8Dkih%20lica.doc.

The Council of the Agency for Personal Data Protection and Free Access to Information, Montenegro. 2019. "Position on recording of employees on official premises." Accessed May 19, 2020. http://www.azlp.me/docs/zastita/Stavovi%20Savjeta/Stav%20Savjeta%20snimanje%20slu%C5%BEbenih%20lica.docx.

The Council of the Agency for Personal Data Protection and Free Access to Information, Montenegro. n.d. "Position on video surveillance in residential buildings." Accessed May 19, 2020. http://www.azlp.me/docs/zastita/Stavovi%20Savjeta/video-nadzor-u-stambenim-zgradama.doc.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism.* London: Profile Books, 8–12.