Asst. Prof. Mišo Dokmanović, PhD

WATCHING THE WATCHERS: LEGAL REGULATION OF CCTV IN MACEDONIA

Keywords: Macedonia, law, data protection, CCTV, video, surveillance

Introduction

Over the last several years there has been rapid and continuous expansion in the collection, usage and transmission of personal data all over the world. Government institutions, organizations and companies have dramatically increased the volume of personal data that they collect, process, analyze and further transmit as part of their everyday activities. This process has inevitably jeopardized and eroded privacy. In January 1997, the "new environment" was best described in the famous statement of SUN Microsystems' executive, Scott McNealy: "You have zero privacy anyway! Get over it!"[1] Having in mind the recent developments, it seems that during the last decade this statement had a strong visionary power. At the same time, it proved to be more than accurate.

The revolution in personal data processing has affected many areas of everyday life. One of the emerging issues in this global process was the usage, development and legal regulation of closed circuit television (CCTV). As a result of that, this paper will make an attempt to analyze the latest trends in the CCTV expansion and its regulation on global level and, consequently, to compare it with the Macedonian experiences. Furthermore, the paper will analyze the current legal regulation of CCTV in Macedonia as well as its implementation practice. Equally, it will offer recommendations how to cope with the potential challenges in this area in future.

The "Surveillance" Revolution

The so-called "surveillance revolution" has begun in the United Kingdom (UK) in the 1960's. The beginning was quite different from the current trends: the number of cameras in operation was very low and the analog technology was used. Undoubtedly, given its extensive experience, UK could be considered as the homeland of CCTV. However, it was during the 1990's that this technology began to expand, as a result of the overall development of digital technology and several other factors (new approaches in crime prevention policy, traffic control etc). In the 1990's the developed countries in Europe and overseas gradually commenced to install surveillance systems in public areas. Again, the leading role was played by the UK. For instance, in 1995, 78% of the UK Home Office budget for crime prevention was spent on open street CCTV and by 1999 the funding has been allocated to 530

[1] Gene K. Landy, *The IT/Digital Legal Companion: A Comprehensive Business Guide to Software, IT, Internet, Media and IP Law.* Syngress: Burlington, 2008. p.453.

town centre schemes operating or scheduled for establishment across UK.

This trend was also evident in the other parts of Europe. Countries such as France, Germany and Belgium have played a pivotal role in the establishment of surveillance systems in the EU. Besides, in the beginning of the 1990's, the major cities in United States and Australia have established CCTV systems. For example, the city of Perth established Australia's first open street closed circuit television system in July 1991.

The process of installation of surveillance systems in Macedonia has accelerated in the last decade. In the beginning, this process was led by private entities that installed CCTV systems with the sole purpose to increase their security and the security of their property. However, in the last few years public entities became involved in the process as well. In that direction, several government institutions and organizations have installed surveillance cameras. CCTV systems were installed on major crossroads, border checkpoints, squares, as well as on other facilities. Generally, the use of CCTV in the country, as elsewhere in the world, was justified with the raising levels of crime and the need for security improvement.

In 2008, the Customs administration of Macedonia has announced the installation of the centralized system for video surveillance composed of 240 video cameras including 44 high speed cameras with zooming options positioned at the border crossing points and the customs branch offices in the country. The main objective of the surveillance system was the prevention of smuggling and corruption.[2]

Besides that, since 2009 the number of surveillance cameras placed by the Ministry of Interior began to grow in particular in the capital Skopje. Over 100 surveillance cameras have been installed on major streets and crossroads in Skopje. In certain parts of the city over 5 cameras have been placed at one spot. However, according to the statement of the spokesman of the Ministry of Interior from June 2011, the surveillance cameras in downtown are still not operational due to the economic crisis.[3] As a result of that, the planned fusion center for the managing of the system of video cameras in the capital has not yet been established in the last two years.

Why is CCTV so important? What makes it so powerful?

Privacy rights are very difficult to define especially in terms of their operation in public and semi-public spaces. Most of us accept that we surrender a certain level of privacy once we leave the premises of our homes. In other words, as we will later point out, we all have *a reasonable expectation of privacy* in the public space. As a result of that,

[2] Презентација на централизираниот систем за видео надзор. Presentation of the centralized system for video surveillance.[Available at http://mk.sectron.com/news/45]. Accessed 20 June 2011.

[3] Newspaper Vest, 21 June 2011, p. 13. [Available from http://daily.mk/cluster3/a94745ae83b000b686b3c20e3c762323/787983]. Accessed on 23 June 2011.

few would concede that we have no expectations of privacy when we walk in the street or ride on a bus.[4]

An additional element is represented by the fact that the number of operating CCTV systems is rapidly growing and that their features are developing. For instance, nobody knows how many surveillance cameras are installed in United Kingdom (some authors consider the number between 2 and 6 million cameras installed in the UK only)[5]. Having in mind the numbers mentioned, it becomes extremely difficult to control and monitor the performance of surveillance.

However, the true importance of CCTV surveillance lies in the ability to watch and especially in the discretion afforded to the watcher in this respect. CCTV surveillance, which involves interaction between the human and the machine, is perhaps best regarded as a hybrid—neither automatic, nor entirely manual.[6] The problem with such CCTV recordings, as far as the agencies such as the police are concerned, is that although cameras may be directed according to the discretion of the operator, video recordings always contain a continuous and unsorted stream of both relevant and irrelevant images. In that direction, Goold argues that the "use of CCTV represents a significant threat to anonymity and therefore privacy in public space"[7]. The latest developments in CCTV technology have considerably increased the capabilities of surveillance cameras including high speed recording, development of smart cameras (for instance, with software for automatic car plates recognition), advanced digital image quality as well as improved zooming capabilities. Therefore, the new surveillance features have expanded the possibilities for potential misuse or violation of the citizens' right of privacy in the public space.

There are many examples how this technology could be (mis)used. For example, the surveillance camera zooming features may allow government employees to focus cameras on individuals/groups assembling in public places, or zoom in on pamphlets or other literature that people carry, effectively obstructing the willingness of the people to exercise their right to assemble or carry and distribute literature and therefore representing a potential violation not only of the right of privacy but of the freedom of expression or association, as well.

Moreover, video surveillance includes camera operators zooming on individuals even though they are not doing anything to attract attention. Usually persons are unaware that they are being watched. Besides, the presence and performance of surveillance systems is frequently unannounced and the surveillance cameras are concealed. As a result of that, the surveillance setting is likely to be ignored by the citizens, which is not the case with the regular police monitoring. Another significant issue is the access to the video – recordings from the

---

[4] Benjamin J. Goold, 'Privacy Rights and Public Spaces: CCTV and the Problem of the "Unobservable Observer"', In: *Criminal Justice Ethics*, Winter/Spring 2002, Vol. 21 Issue 1, p. 23.

[5] Martin Courtney, Public Eyes Get Smart', In: *Science and Technology*, February 2011, p.38.

[6] Thomas Murphy, 'Teeth but a Questionable Appetite: The Information Commissioner's Code of Practice and the Regulation of CCTV Surveillance', in: *International Review of Law Computers & Technology*, Vol.21, No.2, p.138.

[7] Benjamin J. Goold, 'Open to All? Regulating Open Street CCTV and the Case for "Symmetrical Surveillance' in: *Criminal Justice Ethics*, Winter/Spring 2006, p. 8.

surveillance and their storage, which may also be considered as an opportunity for misuse.

These examples, as well as the abovementioned trends in the development of surveillance technology affect the general public perception that CCTV is subject of inadequate control. In that direction, von Hirsch urges that the violation is the exposure of individuals to "the prolonged scrutiny from unobservable observers". As a result of that, Hirsch recommends at least two suggestions to prevent the potential misuse of CCTV: (1) restriction of access to video tapes and other recording instrument, as well as existence of some kind of legitimate interest and justification for the access and (2) placement of notifications in areas where surveillance takes place with the sole purpose to familiarize citizens with the process and to improve their awareness.

Another important issue in the overall process of CCTV regulation is whether the placement of surveillance systems actually prevents crime. Consequently, it is still questionable *whether the use of CCTV decreases crime*. The main argumentation for installation of CCTV anywhere in the world is the prevention of crime. The experience of major cities in this field is biased, as these issues have been widely discussed.

This research has examined the efficiency of surveillance systems in respect of crime prevention in UK and US. Research on CCTV systems initially focused on the question of whether it actually reduced offences. Recent studies in UK suggest that in well-defined spaces such as shops, buses, car parks, underground transportation systems and sports grounds, CCTV system could be a valuable tool for prevention of specific offences. Such results reflect the general findings of the situational crime prevention programs which reveal that success is the most evident in the cases when clearly identified problems in specific locations are targeted.[8] Although there is clear evidence that the use of surveillance cameras affects crime at specific sites, it is still questionable whether the implementation of CCTV generally decreases crime rates in particular in public space areas.

US practice in the field of CCTV regulation has experienced different challenges. According to 2006 New York Civil Liberties Union Report on Video Camera Surveillance in New York, a clear position could not be reached on the issue whether the usage of surveillance cameras in public space decreases crime. Surveillance cameras in New York were installed in 1997 and during the following year, according to the testimony of a law enforcement officer, the monitored buildings experienced on average 36 percent less crime in comparison with the year before installation. At the same time, the report underlines that during the same period the police force was expanded and re-structured. One may conclude, then, that the role of the surveillance cameras was not the only factor that influenced crime prevention in New York.[9]

On the other hand, the experience with installation of surveillance systems in Baltimore was different. Baltimore has developed a CCTV system composed of a small number of cameras

[8] Dean Wilson, Adam Sutton, 'Watched Over or Over – watched', in: The Australian and New Zealand Journal of Criminology, Vol. 37, No. 2, 2004, p. 221.

[9] New York Civil Liberties Union, A Special Report, '*Who's Watching? Video Camera Surveillance in New York City and the Need for Public Oversight',* Fall 2006, p.5.

concentrated in the city's downtown economic and tourist districts. The research conducted after the installation of surveillance cameras has showed that the overall crime rates did not decrease dramatically. However, the positioning of the cameras in the city center has displaced crime to the other parts of the city.[10]

To conclude, foreign practice demonstrated that the use of CCTV is more effective in smaller and specifically defined areas. Furthermore, CCTV has strongly affected displacement of crime from the public areas under surveillance. However, it remains a serious challenge to produce conclusive evidence that surveillance cameras deter crime in general.

In addition to the discussed developments in the practice of CCTV implementation, it is important to emphasize that the courts have created considerable practice and a specific approach concerning the issue of privacy and CCTV surveillance, especially in US.

US courts in several cases have addressed the issue of CCTV and privacy. However, according to Xenakis, they have shown a distinct unwillingness to treat public area surveillance as a search for the purposes of the Fourth Amendment[11], or as violation of any constitutionally protected right to privacy.

In *1983 United States v. Knotts,* for instance, the Supreme Court rejected any suggestion that the electronic tracking of a vehicle could be regarded as a search. As far as the fact of the case are concerned, Tristan Armstrong was frequent buyer of chloroform, substance for manufacturing of illegal drugs. Thus, the Minnesota law enforcement officers arranged with the seller to place a beeper inside the chloroform container and used the beeper together with visual surveillance to trace movement of the respondent which eventually led to his cabin in Wisconsin. The Supreme Court concluded that the beeper signals did not invade "any legitimate expectation of privacy" and in that direction, a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements.[12] As a result of the fact that tracking consisted primarily of visual surveillance upon such routes, this surveillance did not violate his Fourth Amendment rights.

Another important case in the development of the practice concerning surveillance was the decision in *1967 United States v. Katz.* Numerous lower courts and academic commentators believe that, according to this case, the use of covert CCTV surveillance in public spaces—and presumably, therefore, overt surveillance is lawful. Consequently, no person moving about public spaces has a reasonable expectation of privacy. A concurring opinion by John Marshall Harlan introduced the idea of a 'reasonable' expectation of Fourth Amendment protection. According to this case, reasonable expectation of privacy exists in the cases where (1) you actually expect privacy, and (2) your

---

[10] Scott Weaver, '*Looking into Baltimore. London Cameras',* CHARLOTTESVILLE NEWS & ARTS, July 10-16, 2007, [Available from http://www.c-ville.coin/index.php?cat=141404064434008&ShowArticle_ID=l 1430907073691218] Accessed 15 May 2011.

[11] The Fourth Amendment of the US Constitution guarantees the right of the people to be secure in guards against unreasonable searches and seizures, along with requiring any warrant to be judicially sanctioned and supported by probable cause.

[12] United States vs. Knotts, 460 U. S. 276 (1983). [Available from http://supreme.justia.com/us/460/276/case.html]. Accessed on 21 May 2011.

expectation is one that society as a whole would consider legitimate. In other words, the decision of the Supreme Court holds that when a person enters a telephone booth, shuts the door, and makes a call, the government could not record what that person says on the phone without a warrant.[13]

The Main Challenges of CCTV Regulation

Having in mind the abovementioned main characteristics of the development, as well as the future challenges of CCTV, we arrive to the issue of the legal regulation of CCTV.

CCTV represents a new stage of the law enforcement technology. By definition, its usage decreases money spending and reaction time. At the same time, it is a fact that CCTV technology develops more quickly than the law. Obviously, Gelbstain's comparison of the development of information technology and the relevant legislation for its regulation as a race between a rabbit and a turtle is even more applicable in the case of CCTV development and its regulation.[14]

Is it possible to regulate this new emerging technology? What is the legal regulation of CCTV?

Basically, it is a set of legal norms that regulate the use of surveillance cameras and, in particular, their use to record the individuals in public space. Several countries have made a considerable progress in CCTV's legal regulation. At the same time, several international organizations have adopted acts that regulate certain aspects of CCTV.

According to Slobogin, the CCTV regulation should be composed of four key-elements: prior justification for establishment of any CCTV system, clear policy governing the use of cameras, clear rules regarding the storage and dissemination of recorded materials, as well as establishment of accountability procedures and external oversight of all open street CCTV.[15]

Besides that, it should be emphasized that the legal regulation of CCTV is closely related to the issue of data protection. In most cases, the CCTV related issues are regulated by the data protection law of many countries, as well as by several acts of international organizations. In practice, CCTV images are readily involved within the definition of personal data, namely 'data which relate to a living individual who can be identified from those data, or from those data and other information which are in possession of, or are likely to come into possession of, the data controller'.

In general the definition of personal data includes the words "those data from which a living person could be identified". In that direction, according to Article 2 of the Directive 95/46/EC, personal data is defined as "any information relating to an identified or identifiable natural person. Consequently, an identifiable person is defined as a

[13] Katz v. United States 389 U. S. 347 (1967). [Available from http://supreme.justia.com/us/389/347/case.html]. Accessed on 19 May 2011.

[14] Gelbstain, Eduardo. *Crossing the Executive Digital Divide.* Malta: DiploFoundation, 2006, p. 297-301.

[15] Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity', *Mississippi Law Journal 72* (2002), pp. 270-292.

person that can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[16]

Therefore, CCTV cameras produce an amount of images by which any identifiable individual is depicted on screen. Furthermore, the produced images could be used for cross-referencing and image-matching which could lead to identification of the individual (for instance, identification of a person sitting in a theatre or identification of a person in a shop through matching of records of credit card transactions and images from video surveillance). Finally, any filming, recording, storing, viewing, editing etc. falls within the framework of "data processing" and the appropriate provisions of the data protection legislation are applied.

Bearing in mind the close correlation between CCTV and data protection regulation, it should be underlined that there are two groups of sources of data protection legislation: international and domestic. Given the fact that the nature of global economy unavoidably includes transfer of large amounts of data on daily basis, several intergovernmental organizations have attempted to harmonize the data protection legislation. Several acts have been adopted with the sole purpose to discourage organizations and individuals from avoiding data protection control and, at the same time, to guarantee a free flow of information across borders.

Since 1970's the Council of Europe has played a pivotal role in the development of legislation in this field. In 1981 the Council of Europe has adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[17], which laid out a number of principles for data protection which were expected to be incorporated in the national law of the signatories.[18] Besides that, the Organization for Economic Cooperation and Development (OECD) has adopted Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data[19] in 1980, an act that included the principles envisaged in the abovementioned Council of Europe convention. Moreover, in 1990, United Nation's General Assembly adopted the Guidelines for the Regulation of Computerized Personal Data Files[20] which represented the

[16] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [Available from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML]. Accessed on 29 May 2011.

[17] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm] Accessed on 30 June 2011.

[18] By 2011, 43 out of 46 member – states have ratified the convention. The Convention was amended in 1999 and additional protocol was adopted in 2001.

[19] OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data. [Available at http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html]. Accessed 28 June 2011.

[20] UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, 14 December 1990, [Available at: http://www.unhcr.org/refworld/docid/3ddcafaac.html]. Accessed 22 July 2011.

next step in the development of data protection legislation.[21] Finally, through the Parliament and the Commission, the European Union has prepared several acts that deal with the issue of data protection. In 1976 the European Parliament adopted a Resolution on the Protection of the Rights of Individuals in Connection with Data Processing. However, it was only in 1990 when the Commission proposed adoption of a directive addressing the issue of data protection[22]. The Directive was eventually adopted by the European Parliament and Council in 1995 and, consequently, the member – states were obliged to implement the Directive in the national legislation by 1998.[23]

The adoption of the EC Directive represented a major breakthrough in the development of data protection legislation. In a confined period of time the member – states adopted national legislation harmonized with the provisions of the Directive. It should be mentioned that the Directive offered a comprehensive definition of personal data, as well as reference for the processing of sound and image data that was included for the first time.[24]

Finally, given the close connection of CCTV regulation and privacy, any data controller should bear in mind the provisions of Article 8 of the European Convention on Human Rights. This article guarantees the right for respect of the private and the family life of every person, as well as his correspondence. The exercise of the right to privacy could not be derogated by public authority except in cases when it is in accordance to the law and it is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, prevention of disorder or crime, protection of health or morals, or for the protection of the rights and freedoms of others.[25]

How do these recent developments affect the rights of the individuals in Macedonia? Is there a legal framework for regulation of the usage of CCTV systems in the country?

Legal regulation of CCTV in Macedonia

As it was the case with the other countries in the world, the legal regulation of CCTV in Macedonia is closely connected to the general regulation of data protection. At the same time, the adoption of several

[21] The UN guidelines incorporated the existing principles of the Council of Europe Convention and OECD Guidelines, as well as included three additional terms: principle of non-discrimination, power to make exceptions and supervision and sanctions.

[22] EC Council Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. [Available from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML]. Accessed on 24 May 2011.

[23] Chris Reed, John Angel, *Computer Law: The Law and Regulation of Information Technology*, Oxford University Press, 2007, pp. 464 – 469.

[24] In that direction, the processing of sound and image data, such as in cases of video surveillance, did not come within the scope of the Directive, if it is carried out for the purposes of public security, defense, national security or in the course of state activities relating to the area of criminal law, or of other activities which do not come within the scope of Community law.

[25] European Convention of Human Rights. [Available at http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/ENG_CONV.pdf]. Accessed 22 June 2011.

previously mentioned acts by the intergovernmental organizations had a suitable impact on the development of data protection legislation, including CCTV regulation.

The development of data protection legislation in Macedonia commenced in 1994 when the Law for Personal Data Protection was adopted[26]. The Law provided the legal framework for protection of personal data of the citizens. However, the provisions of 1994 Law for Personal Data Protection were not completely implemented. Besides that, it is important to emphasize that the Law did not establish a special body for the implementation of the legislation, in particular for the monitoring of the personal data processing. Moreover, the 1994 Law for Personal Data Protection has been adopted before Directive 95/46/EC was passed by the European Council and Parliament.

The next phase in the development of data protection legislation in Macedonia began in 2005 when the Macedonian Parliament adopted the new Law for Personal Data Protection.[27] It was to a large extent drafted under the influence of Directive 95/46/EC, as part of the Macedonian efforts to harmonize its legislation with the European standards in this field.[28]

The 2005 Law for Personal Data Protection established the Directorate for Personal Data Protection as a state body with the sole purpose to monitor and supervise "the legality of undertaken activities in the personal data processing on the territory of the Republic of Macedonia".[29] Besides that, provisions concerning personal data processing, data protection and secrecy, development of registry of personal data, as well as data transfer were included in the text of the law. It should be emphasized that according to Article 2 of the Law for Personal Data Protection, personal data is defined as any information pertaining to an identified or identifiable natural person, the identifiable entity being an entity whose identity can be determined directly or indirectly, especially according to the personal identification number of the citizen or on the basis of one or more characteristics, specific for his/her physical, mental, economic, cultural or social identity. The definition of "personal data" in the law is almost identical with the definition incorporated in the Directive 95/46/EC.

The first complaint to the Directorate was submitted in the beginning of 2006 and as a result of that the Directorate adopted several rulebooks in order to define and specify certain aspects of the procedure.[30]

---

[26] Закон за заштита на личните податоци. (Сл. весник на РМ бр. 12/1994). [Law for Personal Data Protection. Official Cazette of the Republic of Macedonia No. 12/1994].

[27] Закон за заштита на личните податоци. (Сл. весник на РМ бр. 7/2005). [Law for Personal Data Protection. Official Cazette of the Republic of Macedonia No. 7/2005].

[28] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [Available from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML]. Accessed on 29 May 2011.

[29] Член 37, Закон за заштита на личните податоци. (Сл. весник на РМ бр. 7/2005). [Article 37, Law for Personal Data Protection. Official Cazette of the Republic of Macedonia No. 7/2005].

[30] The first submitted complaint was MD vs. Stopanska Banka Skopje.

Amendments and supplements to the law were adopted in 2008 and 2010. The amendments were attended to further align the domestic legislation with the *acquis communautaire,* in particular to strengthen the position of the Directorate for Personal Data Protection and improve the implementation of the law. According to the European Commission Progress reports on Macedonia, the overall performance of the Directorate for Personal Data Protection was evaluated as satisfactory.[31]

One of the issues that were addressed in the amendments was the *regulation of video surveillance*. The issue of video surveillance was included in the Macedonian legislation with the adoption of the Law for Amendment and Supplement of the Personal Data Protection Law in 2008[32]. As it was already emphasized, this was a result of the changing nature as well as the accelerated introduction of CCTV in the country, both by private and public entities.

The amendments adopted a general and at the same time explicit position that the provisions of the Law for Personal Data Protection should also be applied to personal data processing by video surveillance, unless otherwise determined by another law.

Furthermore, the amendments regulated the issue of signage or notification of video surveillance performance. Consequently, each controller that performs video surveillance is obliged to display a notification. The notification should be (1) comprehensive; (2) visible and (3) displayed in a manner which enables the personal data subject to be informed about the performance of video surveillance. Moreover, the amendments clarified the content of the notification which should include: (1) information that video surveillance is being performed; (2) information regarding the name of the controller that performs the surveillance and (3) the manner for obtaining information regarding the place and period of preserving the videos of the surveillance system.[33]

Another issue that was addressed in the amendments to the law was the purpose of the surveillance and time framework for storage of video recording. Consequently, according to the amendment, "the controller may perform video surveillance solely in an area necessary for fulfilling the aims of its setting". However, in the implementation of this provision, the controller should bear in mind the effect that the use of surveillance systems might have on individual privacy. In particular, the controller should choose a location that minimizes the recorded area to extent which is necessary for the purpose to be achieved and on the other hand, a location that will provide images of sufficient quality.[34] Finally, Article 9-a clearly defined the duration of the preservation of the videos

---

[31] European Commission, FYR Macedonia 2010 Progress Report. [Available from http://www.delmkd.ec.europa.eu/en/bilateral-relations/pdf/mk_rapport_2010_en.pdf]. Accessed on 15 June 2011; European Commission, FYR Macedonia 2008 Progress Report. [Available from http://ec.europa.eu/enlargement/pdf/press_corner/keydocuments/reports_nov_2008/the_former_yugoslav_republic_of_macedonia_progress_report_en.pdf]. Accessed on 15 June 2011.

[32] Закон за измени и дополнување на Законот за заштита на личните податоци. (Сл. весник на РМ 108/2008). [Law for Amendment and Supplement of the Personal Data Protection law. (Official Gazette of the Republic of Macedonia No. 108/2008)].

[33] Article 9-a, Law for Amendment and Supplement of the Personal Data Protection Law. (Official Gazette of the Republic of Macedonia No. 108/2008).

[34] Peter Carey, *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, 2009, p. 231.

made by video surveillance. The video should be preserved until fulfilling the purposes of its performance, not exceeding 30 days, unless longer period is envisaged by another law. European experiences in this field show that all storage media (a video cassette, CD –ROMs, hard disk drives etc.) should be purged of footage containing personal data on regular basis. If the footage was necessary for criminal proceedings, it should be kept during the procedure including appeals. On the other hand, Carey argues that if some of the images on the tape or other storage media are not related to an incident, they should be erased at earlier stage.[35]

Furthermore, the Law for Personal Data Protection has included restrictions regarding stipulated rights in the text. Some restrictions of the rights of the personal data subjects were envisaged in Article 15 of the Law for Personal Data Protection. In that direction, the rights of the personal data subject stipulated in the provisions of articles 10-14 could be restricted in some special cases when their application could endanger the fulfillment of controller's obligations envisaged by law[36]. These special cases include: protection of the security and defense of the state; detection and prosecution of the perpetrators of criminal acts; protection from infringement of ethic rules of a certain profession; protection of important economic or financial interests of the state or the European Union and protection of the rights and freedoms of the personal data subject or the rights of the natural persons. As far as the restrictions in EU Data Protection Directive are concerned, the processing of sound and image data, such as video surveillance, do not come within the scope of the Directive, if it was performed for the purposes of public security, defense, national security or in the course of state activities relating to the area of criminal law, or other activities which do not come within the scope of the Community law.

In addition, the amendments to the Law for Personal Data Protection also incorporated some special provisions for particular cases such as video surveillance of business premises and single and multiple-quarters buildings. Accordingly, the amendments defined the conditions under which the controller may perform video surveillance in official or business premises. The performance of video surveillance was possible only if it was necessary for protection of human life and health, property, protection of the life and health of the employees, due to the nature of the job and control over the entry and exit from the official and business premises. Besides that, the controller should notify the employees about the performance of video surveillance. Moreover, the controller should refrain from placing surveillance equipment in areas where subjects expect a higher level of privacy. For that reason, the performance of video surveillance in dressing rooms, fitting rooms, toilets and bathrooms, elevators and other similar areas is prohibited.

As far as the video surveillance in single and multiple-quarters buildings is concerned, the amendments defined that in order to perform video surveillance of the buildings, a written consent of all owners

[35] Ibid, p. 232.

[36] The following rights of the personal data subject could be restricted: the right for notification of data processing, the right to request freezing of the subject's personal data processing, the right to ask supplementing, amending, deletion or prevention of the use of the personal data etc.

should be provided[37]. However, this general provision is limited with the prohibition of transmission of the footage on cable television (public or internal network), via the internet or via other electronic means for data transfer and the prohibition of recording of footage of entrances in personal apartments of other owners and lessees.[38] Finally, the controller is obliged to regulate the manner of performing the video surveillance with a special act.

The amendments of the Law for Personal Data Protection adopted in 2010 further strengthened the position of the Directorate for Personal Data Protection. The law instructed each organ of the state administration, public institutions or other legal entities that keep official registers to submit, upon request of the Directorate, all data from the registers and data obligations. Moreover, the Directorate was authorized to request aid by the state administration body competent for internal affairs during the implementation of the executive decision. These provisions were included in the text of the law in an effort to overcome the setbacks that occurred in the practice of the Directorate.[39]

Macedonian Practice in the Implementation of the Legislation concerning CCTV

The monitoring of the implementation of legislation concerning video surveillance in Macedonia has begun in 2008. According to the 2008 Annual Report of the Directorate for Personal Data Protection of Republic of Macedonia, violation of Art. 9-a and 9-b was registered in 8 cases. In these 8 cases the following violations were conducted: the controller of personal data did not inform the personal data subject about the personal data processing, the controller performed video surveillance in an area that was not necessary for fulfilling the aims of its setting, the videos made while performing video surveillance were kept for over 30 days, performance of video surveillance in single and multiple quarters buildings without consent as specified in the law etc.[40] The 2008 Annual Report concludes that 2/3 of the inspected personal data controllers did not fully implement the provisions of the Personal Data Protection Law. Finally, the report underlined the need for further inspection control especially in the fields of personal data processing by video surveillance, biometric data and personal data processing by use of information technology.

The Directorate for Personal Data Protection has increased the number of inspections in 2009. According to the 2009 Annual Report of the Directorate, the violations of the Personal Data Protection Law

[37] In 2010 this provision was expanded with the requirement to request a written consent of all owners and all leases. Law for Amendment and Supplement of the Personal Data Protection Law. (Official Gazette of the Republic of Macedonia No. 124/2010).

[38] Article 9-c, Law for Amendment and Supplement of the Personal Data Protection Law. (Official Gazette of the Republic of Macedonia No. 108/2008).

[39] Articles 4-c and 4-d, Law for Amendment and Supplement of the Personal Data Protection Law. (Official Gazette of the Republic of Macedonia No. 124/2010).

[40] Годишен извештај за работењето на Дирекцијата за заштита на личните податоци за 2008 година. [2008 Annual Report of the Directorate for Personal Data Protection]. [Available from http://dzlp.mk/FILES/1164/PUBLIC/CONTENT/729553489483110104081405 1_FILES/Godisen_izvestaj_DZLP_08.pdf]. Accessed on 15 June 2011, p. 14.

persisted in 2009. The Directorate has registered 59 data controllers that violated Art. 9-a, 9-b and 9-c, concerning almost the same issues as it was the case in 2008[41].

However, it should be emphasized that in 2009 the Directorate has partly prohibited video surveillance in the centers for drugs addiction treatment and decreased the number of video cameras in the corridors and waiting rooms of the public health institutes. Besides that, the Directorate has prohibited the continuous surveillance of the employees with the purpose of monitoring their efficiency.[42] Finally, the Directorate has noted a growing number of cases of setting surveillance cameras to record public space (streets, squares, parking lots etc.) with the purpose of vehicles recording or transmission of the recording through their websites in order to increase the number of visitors. The Directorate has concluded that this practice is not in accordance with the provisions of the law.[43]

Having in mind the provisions of the Article 9-b of the Law for Personal Data Protection, in 2010 the Director of the Directorate has enacted the Rulebook on the form and content of the act on the manner of performing video surveillance[44]. The enactment of the Rulebook represented a major step in practical regulation of the video surveillance in Macedonia. In particular, article 3 regulated the main elements of the act that every controller in the country should adopt when performing video surveillance. In that direction, the act should include the following elements: legal basis for surveillance, aims for personal data processing, transfer of personal data processed through the surveillance system, technical and organizational instruments for providing secrecy and protection of personal data, the deadline for keeping the records, technical specifications of the equipment, plan for using CCTV cameras.

Furthermore, the controller of personal data is obliged to carry out an analysis of the reasons and aims for setting video surveillance, as well as to conduct periodical evaluation of the results achieved by the surveillance system. Besides that, the controller should prepare a report that includes a statistical overview concerning the access to the video records and their use.[45] Finally, in order to monitor the access and usage of video records, the provisions of Article 9 created an obligation for the

---

[41] Годишен извештај за работењето на Дирекцијата за заштита на личните податоци за 2009 година. [2009 Annual Report of the Directorate for Personal Data Protection]. [Available from http://dzlp.mk/FILES/1164/PUBLIC/CONTENT/729553489483110104081405 1_FILES/GODISEN%20IZVESTAJ%20za%202009.pdf]. Accessed on 15 June 2011, p. 20.

[42] The Personal Data Protection Directorate has concluded that, according to the European regulations and practice, the continuous video surveillance of the employees in order to monitor their efficiency constitutes a direct violation of the right for personal data protection and privacy. (2009 Annual Report of the Directorate for Personal Data Protection, p.19).

[43] The 2010 Annual Report of the Directorate has not been published during the preparation of the paper.

[44] Правилник за содржината и формата на актот за начинот за вршење на видео надзор. (Сл. весник на РМ бр. 158/10). [Rulebook on the form and content of the act on the manner of performing video surveillance. (Official Gazette of the Republic of Macedonia No. 158/10)].

[45] Член 7, Правилник за содржината и формата на актот за начинот за вршење на видео надзор. (Сл. весник на РМ бр. 158/10). [Article 7, Rulebook on the form and content of the act on the manner of performing video surveillance. (Official Gazette of the Republic of Macedonia No. 158/10)].

controller to keep a registry. The registry should include: name of the authorized person, date and time of access, reasons for access, date and time when the video record was made, date, time and name of the user that was given access to the video records, type of media where the video record is kept etc. Finally, the person authorized for personal date protection should sign a statement for secrecy and protection of personal data protection. It is evident that the Rulebook has incorporated several significant elements from the international practice and to conclude, its enactment has considerably improved the legal framework for CCTV in the country.

Conclusion

It could be concluded that the CCTV regulation in the country is from recent date. As it is the case with the considerable number of countries, the issues of CCTV regulation are mainly addressed in the Law for Personal Data Protection. In that direction, it is evident that Macedonian data protection law has been harmonized with the EU legislation to a large extent. Furthermore, the CCTV regulation was strongly influenced by the development of video surveillance technology and international data protection legislation and on the other hand, the growing tendency to install surveillance systems by both private and public entities in Macedonia. Adoption of the amendments to the Law for Personal Data Protection in 2008 has set the basic framework for CCTV regulation in the country.

The position of the Directorate for Data Protection has continuously been strengthened through several amendments of the Law for Data Protection in 2008 and 2010. It is of a great importance to emphasize the adoption of the Rulebook which permitted further operationalisation of the procedure for video surveillance. In particular, the obligation of every data controller to adopt an act which should include several elements selected under influence of the international experience is of a key-importance for the CCTV control and monitoring in the country. Furthermore, the adoption of several decisions in 2008 and 2009 to prohibit video surveillance in centers for drug addiction, decrease the number of cameras in corridors and waiting rooms in health institutions or CCTV transmissions through websites is very important. Given the fact that the Directorate is in charge of monitoring and supervision of undertaken activities in the personal data processing, it should continue this practice and further improve the control and assessment audit of data controllers in public and private entities.

In that direction, the Directorate should pay a special attention to the control and monitoring of the video surveillance system within the Ministry of Interior. Although this surveillance system is still not operational, the considerable number of cameras installed on major roads and squares suggest that it might be a challenging issue for the privacy of the citizens, once the cameras become operational. As it was already mentioned, there are several examples of inappropriate and inadequate setting of CCTV systems which could possibly be contrary to the obligation provided by the Law for Personal Data Protection that the controller may solely perform video surveillance in an area necessary for

fulfilling the aims of its setting. Having in mind the number of installed cameras, as well as the fact that the cameras will perform surveillance of the public space, the Directorate should work closely with the Ministry of Interior, in particular with regard to the plan for camera setting (article 14 of the Rulebook), as well as the development of system for monitoring and supervision of the staff. Nevertheless, international experience should be implemented in the work of the Ministry in order to prevent any potential "prolonged scrutiny of unobservable observes".

Besides that, CCTV legislation in the country should be further supplemented with provisions that will prohibit targeting or observing individuals solely because of their race, gender, ethnicity, sexual orientation, disability or other classifications protected by law. Also, the use of audio recording in conjunction with CCTV should be explicitly prohibited, unless appropriate court orders are provided. Further efforts for advancement independent regulatory framework based on clear rules and external auditing for video surveillance performance by public entities should be encouraged.[46] Finally, in order to improve the transparency of the overall process, an effort should be made to involve representatives of local communities/councils in the crucial phases of the surveillance performed by public entities in public space, such as the definition of the viewing areas of cameras, control and monitoring of the performance of video surveillance, storage of video footage, periodic audits etc.

[46] Aileen B. Xenakis, 'Washington and CCTV: It's 2010, Not Nineteen Eighty Four'. In: *Case Western Reserve Journal of International Law*; 2010, Vol. 42 Issue 3, p. 584.

Abstract

This article reconsiders the legal and normative questions raised by the spread of CCTV, particularly in light of recent writings on both privacy and the regulation of surveillance technologies. The author analyzes the recent trends in the installation on CCTV systems and its regulation in several countries, with special emphasis on UK and US. In the second part of the paper, the author explores the current situation in Macedonia. In that direction, the relevant legislation for CCTV regulation has been analyzed. Finally, the paper provides recommendations to supplement the current CCTV legislation, in particular with regard to the improvement of monitoring and transparency during video surveillance process, as well as further advancement of the right to privacy of citizens.

REFERENCE LIST

- Aileen B. Xenakis, 'Washington and CCTV: It's 2010, Not Nineteen Eighty Four'. In: *Case Western Reserve Journal of International Law*; 2010, Vol. 42 Issue 3.
- Benjamin J. Goold, 'Open to All? Regulating Open Street CCTV and the Case for "Symmetrical Surveillance'. In: *Criminal Justice Ethics*, Winter/Spring 2006.
- Benjamin J. Goold, 'Privacy Rights and Public Spaces: CCTV and the Problem of the "Unobservable Observer"', In: *Criminal Justice Ethics*, Winter/Spring 2002, Vol. 21 Issue 1.
- Chris Reed, John Angel, *Computer Law: The Law and Regulation of Information Technology*, Oxford University Press, 2007.
- Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity', *Mississippi Law Journal 72* (2002).
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm] Accessed on 30 June 2011.
- Dean Wilson, Adam Sutton, 'Watched Over or Over – watched', In: The Australian and New Zealand Journal of Criminology, Vol. 37, No. 2, 2004.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [Available from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML]. Accessed on 29 May 2011.
- EC Council Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. [Available from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML]. Accessed on 24 May 2011.
- European Commission, FYR Macedonia 2010 Progress Report. [Available from http://www.delmkd.ec.europa.eu/en/bilateral-relations/pdf/mk_rapport_2010_en.pdf]. Accessed on 15 June 2011; European Commission, FYR Macedonia 2008 Progress Report. [Available from http://ec.europa.eu/enlargement/pdf/press_corner/key-documents/reports_nov_2008/the_former_yugoslav_republic_of_macedonia_progress_report_en.pdf]. Accessed on 15 June 2011.
- European Convention of Human Rights. [Available at http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/ENG_CONV.pdf]. Accessed 22 June 2011.
- Gelbstain, Eduardo. *Crossing the Executive Digital Divide.* Malta: DiploFoundation, 2006.

- Gene K. Landy, *The IT/Digital Legal Companion: A Comprehensive Business Guide to Software, IT, Internet, Media and IP Law*. Syngress: Burlington, 2008.
- Katz v. United States 389 U. S. 347 (1967). [Available from http://supreme.justia.com/us/389/347/case.html]. Accessed on 19 May 2011.
- Martin Courtney, Public Eyes Get Smart', in: *Science and Technology*, February 2011.
- New York Civil Liberties Union, A Special Report, '*Who's Watching? Video Camera Surveillance in New York City and the Need for Public Oversight',* Fall 2006.
- Newspaper Vest, 21 June 2011, p. 13. [Available from http://daily.mk/cluster3/a94745ae83b000b686b3c20e3c762323/787983]. Accessed on 23 June 2011.
- OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data. [Available at http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html]. Accessed 28 June 2011.
- Peter Carey, *Data Protection: A Practical Guide to UK and EU law*, Oxford University Press, 2009.
- Scott Weaver, '*Looking into Baltimore. London Cameras',* CHARLOTTESVILLE NEWS & ARTS, July 10-16, 2007, [Available from http://www.c-ville.coin/index.php?cat=141404064434008&ShowArticle_ID=l1430907073691218] Accessed 15 May 2011.
- Thomas Murphy, 'Teeth but a Questionable Appetite: The Information Commissioner's Code of Practice and the Regulation of CCTV Surveillance', In: *International Review of Law Computers & Technology*, Vol.21, No.2.
- UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, 14 December 1990, [Available at: http://www.unhcr.org/refworld/docid/3ddcafaac.html]. Accessed 22 July 2011.
- United States vs. Knotts, 460 U. S. 276 (1983). [Available from http://supreme.justia.com/us/460/276/case.html]. Accessed on 21 May 2011.
- Годишен извештај за работењето на Дирекцијата за заштита на личните податоци за 2008 година. [2008 Annual Report of the Directorate for Personal Data Protection]. [Available from http://dzlp.mk/FILES/1164/PUBLIC/CONTENT/72955348948311010408140 51_FILES/Godisen_izvestaj_DZLP_08.pdf]. Accessed on 15 June 2011, p. 14.
- Годишен извештај за работењето на Дирекцијата за заштита на личните податоци за 2009 година. [2009 Annual Report of the Directorate for Personal Data Protection]. [Available from http://dzlp.mk/FILES/1164/PUBLIC/CONTENT/729553489483 1101040814051_FILES/GODISEN%20IZVESTAJ%20za%202009.pdf]. Accessed on 15 June 2011, p. 20.

- Закон за заштита на личните податоци. (Сл. весник на РМ бр. 12/1994). [Law for Personal Data Protection. Official Cazette of the Republic of Macedonia No. 12/1994].
- Закон за заштита на личните податоци. (Сл. весник на РМ бр. 7/2005). [Law for Personal Data Protection. Official Cazette of the Republic of Macedonia No. 7/2005].
- Закон за измени и дополнување на Законот за заштита на личните податоци. (Сл. весник на РМ 108/2008). [Law for Amendment and Supplement of the Personal Data Protection Law. (Official Gazette of the Republic of Macedonia No. 108/2008)].
- Правилник за содржината и формата на актот за начинот за вршење на видео надзор. (Сл. весник на РМ бр. 158/10). [Rulebook on the form and content of the act on the manner of performing video surveillance. (Official Gazette of the Republic of Macedonia No. 158/10)].
- Презентација на централизираниот систем за видео надзор. Presentation of the centralized system for video surveillance.[Available at http://mk.sectron.com/news/45]. Accessed 20 June 2011.