TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Anar Agajev

USING CCTV CAMERAS IN SCHOOLS AND THE STUDENT'S RIGHT TO PRIVACY

Bachelor's thesis
Programme HAJB 08/14, specialisation European Union and International Law

Supervisor: Kärt Salumaa-Lepik, MA

Tallinn 2021

I hereby declare that I have compiled the thesis independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.
The document length is 8178 words from the introduction to the end of the conclusion.

Anar Agajev .....
(signature, date)
Student code: 164934HAJB
Student e-mail address: annuannu77@hot.ee

Supervisor: Kärt Salumaa-Lepik, MA:
The paper conforms to requirements in force

.....
(signature, date)

Chairman of the Defence Committee
Permitted to the defence

.....
(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

In order to process personal data, there are certain principles which have to be followed. However, there is not a specific law that deals with surveillance cameras in schools. So, the General Data Protection Regulation will be mainly used. Also, there is a big controversy still going on about using CCTV cameras in schools. The aim of this thesis is to research which kind of data protection principles do schools need to follow, whether the rights of students and teachers are being violated and which problems can interference that is very excessive cause on student's privacy.

This research uses qualitative research method where academic literature and legislation are used. The academic literature contains scientific books, articles and some other sources. The legislation contains mainly European Union legislation.

The hypothesis of this thesis is that if schools follow certain principles like lawful processing, purpose limitation and also some other conditions, then it is still illegal to use surveillance cameras; the right to privacy of students and teachers is not violated and excessive interference on students' privacy does not cause any problems.

Keywords: CCTV cameras, schools, rights, students, privacy

INTRODUCTION

Closed-circuit television cameras are an increasing presence in schools. The use of monitoring cameras rises as students move from primary to secondary school. Educational institutions that are using observation cameras generally place them in gyms, cafeterias and hallways. The use of monitoring pupils in classrooms is also increasing. Supervision technology is mainly used to expand the security and safety of the students. However, using CCTV cameras in schools can give rise to many problems, for example, the legality of using these cameras as well as the right to privacy of students.[1]

The aim of this bachelor's thesis is to find out, which principles must schools follow; are the students' and teachers' rights being violated by using these cameras and which problems can excessive interference cause on the privacy of students. In order to achieve the aim of the bachelor's thesis, the following research questions will be answered:

1. Which data protection principles do schools need to follow in order to use surveillance cameras?
2. Is the right to privacy of students and teachers being violated by using these cameras or is it not and how?
3. Which consequences can an excessive interference cause on students' privacy?

The hypothesis is that if schools follow certain principles like lawful processing, purpose limitation and also some other conditions, then it is still illegal to use surveillance cameras; the right to privacy of students and teachers is not violated and excessive interference on students' privacy does not cause any problems.

In this research qualitative research method is used including scientific books, articles, European Union legislation and some other sources.

[1] Warnick, B. R. (2007). Surveillance cameras in schools: An Ethical Analysis. *Harvard Educational Review*, 77 (3), 317, 319-320.

The thesis is divided into three parts. Chapter one is about closed-circuit television cameras in general. It starts out by explaining the development of CCTV cameras throughout time and also, what they are exactly. After that, it discusses where these types of cameras are usually used and why are schools specifically so different from them. In addition, it describes if these cameras are legal or not. Moreover, it explains why are schools using these monitoring devices and what are the negative aspects of using these cameras in schools.

Chapter two focuses on privacy and data protection law, it begins by talking about the history of privacy and data protection law, then it moves on to explaining the most important conventions and directives that deal with privacy and data protection law. Finally, it explains what is the processing of personal data and under what conditions is it legal. It also mentions sensitive personal data and the principles that need to be followed in order to process personal data.

Chapter three writes about the right to privacy of students and teachers. It begins by, first of all, defining the right to privacy, then, it moves on to the most essential law dealing with the privacy of pupils in the United States, which happens to be FERPA. Furthermore, it describes the issues that redundant interference can cause on students. Finally, it ends with teachers' right to privacy in schools.

1. CLOSED-CIRCUIT TELEVISION CAMERAS

1.1. History and definition of CCTV cameras

At the same period when the early black and white televisions started to appear, the thought of using cameras and monitors as a tool of observing a place started to take a hold but, owing to the big price of equipment, these early CCTV systems were limited to specialized activity, and to institutions that had the funds to put money into such security. These systems were of restricted use since an operator had to be observing the screen continuously.

Throughout the 1960s and 1970s, the technology of the CCTV developed at a slow pace, following in the footsteps of the broadcast industry, which had the funds to invest in modern developments. The main obstacle was in the technology of the camera, which relied enterily on vacuum tubes as a pick-up device. Tubes were large, demanded high voltages to run, were normally of no use in low light situations, and were costly. Moreover, an early colour camera demanded three of these tubes. For this reason, CCTV continued to be on the whole a low-resolution, monochrome system, which was very costly for many years.

By the 1980s camera technology was making progress, and the price of a rational colour camera lowered to a dum that was reasonably priced to smaller companies and institutions. Additionally, VHS had arrived. This had a major influence on the CCTV industry since for the first time it was possible to record video images on equipment that was priced at well beneath 1000 pounds.

From the mid-1980s onwards television technology moved forward in huge leaps. New developments like the CMOS microchip and also the charge-coupled device, which is otherwise known as the CCD chip brought about a growth in equipment capability and improved the picture quality by a considerable amount, whilst at the same time equipment costs decreased. Manufacturers like Sony and Panasonic developed digital video recording machines, and while these were planned mainly for use in the broadcast industry, they paved the way for digital video signal processing in lower-resolution CCTV and domestic video products.

For many years, CCTV had to depend on the broadcast industry to develop new technologies, and then wait for these technologies to be downgraded so that they become reasonably priced to buyers who could not afford to pay 30 000 pounds per camera and 1000 pounds per monitor.[2]

CCTV, which is otherwise known as Closed Circuit Television, is a visual surveillance technology that is designed for observing a variety of environments and activities. CCTV systems are used to monitor public areas for violent actions, vandalism, robbery, and unlawful entry, both indoors and out. CCTV recordings are used to acquire and provide proof for criminal and also other investigations; they are at times revealed to the media in the hopes of obtaining information about images of a suspect or suspects caught in or near a crime scene.

The term Closed Circuit Television can be confusing, because the word television in fact means to see at a distance, which hints at broadcast. If public broadcast is not the intent, CCTV is the right terminology, as it is not a system for broadcast to the public on the whole. As opposed to television that is used for public entertainment, a CCTV system is closed and all of its components are directly connected either by hardwire methods or wireless technologies.[3]

CCTV technology has advanced considerably beyond the camera with a cable running to a television monitor. However, fundamental questions facing decision makers involve when and how to make the switch to newer IP technology, which is otherwise known as Internet Protocol cameras, without making expensive mistakes. The direction is toward digital and away from analog. Analog signals are, for example, on a tape in original form, however with digital, analog signals are sampled, turned into numbers, and stored digitally. This is a transformation to a format enabling data to be stored and transfered through a computer network. Internet Protocol is a standard that allows computers to communicate across the Internet, which is the biggest network in the world. With IP cameras, data goes straight into the network; with analog cameras, the video must first be transformed to IP.

The advantages of IP over analog contain the transmission of almost-live video at great distances. Analog is suitable when video is viewed at only one site. In new construction, network cables are cheaper than coaxial cables for analog systems. A downside of IP is the system going down due

[2] Cieszynski, J. (2006). *Closed Circuit Television*. (3rd ed.) Oxford, UK: Elsevier Science and Technology, 1-2.
[3] Harwood, E. (2007). *Digital CCTV: A Security Professional's Guide*. California, USA: Elsevier Science and Technology, 1.

to the network issue, a hacker, or maintenance. Another drawback with IP is issues with interoperability, meaning that customers are restricted in their choice of products that work with their system; IP standards are being scheduled among manufacturers.

Elliott (2010, 48) indicates to the secret expenses of IP observation and retailers selling such systems who may not consider the correct cost when providing a quote to clients. While the price of installing an IP-based system is usually specified as being lower than an analog system, labor is needed with the IP system "to configure the corporate network, the switches and routers, to support the required Quality of Service features and bandwidth that an IP surveillance system will need." An additional concealed cost is network redundancy. When a corporate network is without unnecessary connections, switch engines, and power supplies, a defect within the network can damage the work of the IP surveillance system.[4]

1.2. The use of CCTV cameras

The ubiquity of the surveillance cameras can be seen in shopping centers, retail outlets and town centres. Also, hospitals, leisure centres and schools are progressively coming under the camera's gaze.[5] However, schools are ethically different from many other public places, like, for example, shopping malls or leisure centers, because, first of all, the people that are in schools are mostly composed of children and youngsters rather than adults. This is important, because it informs how people think about rights and obligations within schools. Also, schools are different in the way that they are public places where attendance is usually required rather than optional. Students cannot decide to leave a school in the same way that they choose to exit a shopping center. In addition, schools are not the same as some other publicly accessible places like shopping centers in that people expect public schools, or schools that accept any kind of public funds, to be at least accountable to a limited extent to the bigger community. Therefore, schools have to be clear in the formulation and assessment of their policies. Finally, schools are distinctive in that they should be places committed to learning and growth. This developmental aspect is essential to learning morals due to the fact that what may be morally acceptable outside of schools could be more troublesome inside of schools.[6]

[4] Purpura, P. P. (2010). *Security: An Introduction*. (1st ed.) Boca Raton, Florida: CRC Press LLC, 308-309.
[5] Norris, C., Moran, J., Armstrong, G. (1998). *Surveillance, Closed Circuit Television and Social Control*. (1st ed.) London: Routledge, 3.
[6] Warnick, B. R. (2007). Surveillance Cameras in Schools: An Ethical Analysis. *Harvard Educational Review*, 77 (3), 318.

1.3. Legitimacy of using CCTV cameras

Closed - circuit television cameras are legal, however, only in certain circumstances. According to article 6 of the General Data Protection Regulation, which is the GDPR, the processing of personal data is legal only if at least one of the following applies: first of all, if the data subject, which happens to be the student in a school in this case, has given permission to the processing of his or her personal data for one or more particular objectives; secondly, the processing is essential for the fulfillment of a contract to which the data subject is party or so as to take steps at the demand of the data subject before entering into a contract; in addition, if the processing is essential for accordance with a lawful obligation to which the controller is subject; also, if the processing is required so that to protect the vital interests of the data subject or of another physical person; moreover, if the processing is vital for the completion of a task carried out in the public interest; finally, if the processing is needed for the aims of the legal interests pursued by the controller or by a third party.[7]

Schools have to make sure that the system does not reasonably violate on the privacy of people and the use of a CCTV system should only be taken into account if no other suitable options have proven or are possibly to prove successful.[8]

Despite the fact that video surveillance cameras in public places like schools are not illegal, a camera in a more private area, like a locker room or bathroom, is considered to be an invasion of privacy. In schools, surveillance cameras are usually used openly, where teachers, administrators and students can easily see the camera in lunchrooms, corridors or gyms.[9]

1.4. Purposes of using CCTV cameras in schools

The main reason for why schools use surveillance cameras is to tackle bullying.[10] The most common primary argument for installing CCTV is usually the necessity to tackle vandalism and

[7] OJ L 119, 4.5.2016, art 6, p 1.
[8] Squelch, J., Squelch, A. (2005). Webcams in Schools: A Privacy Menace or a Useful Monitoring Tool. *Australia and New Zealand Journal of Law Education*, 10(2), 11(1), 56.
[9] Heintzelman, S. C., Bathon, J. M. (2017). Caught on Camera: Special Education Classrooms and Video Surveillance. *International Journal of Education Policy and Leadership*, 12 (6), 3.
[10] Taylor, E. (2011). UK schools, CCTV and the Data Protection Act 1998. *Journal of Education Policy*, 26 (1), 6.

theft. However, there are many other purposes as well. Other objectives for using monitoring cameras in schools include entrance control, behaviour control and evidence gathering.

First of all, it is to help in stopping complete strangers, who are not related to the school at all, from illegally gaining entrance to the school. There was a research done on eight schools and colleges who had installed surveillance cameras and at one particular educational institution, which is called the Priory Secondary School, visitors were kept under surveillance by CCTV at the entrance, they had to identify themselves through an intercom, and , if the person who was on duty was pleased, an electronic lock would then be activated giving them entrance into the lobby. Such kind of entrance control does not just prohibit a way in to strangers, but it also enables personnel to observe the arrival of late pupils.

Closed-circuit television cameras are also used in order to control the behaviour of students. The personnel in Olden, Priory and Quarry schools sometimes used the monitoring cameras in order to control that pupils were not hanging around in corridors when they ought to be in lessons. Video surveillance cameras engaged students in a discussion, causing them to become self-conscious about their conduct and comply with social standards. Nevertheless, all eight schools had cameras whose main aim was to observe the behaviour of pupils.

In schools monitoring cameras form part of a comprehensive policy of behaviour control working through normalising rules, exams, reports, uniform use and punishments. Although it is doubtful whether pupils think about these effects, such kind of disciplinary conversations still seek to channel and control conduct.

An important aspect of social control discussions is the promise of punishment, and in modern community the legality of taking disciplinary action is quite frequently reliant upon the production of proof. All eight schools had surveillance cameras that recorded images, which were kept for one month. These images were used to examine previous cases where the personnel were doubtful about what had happened and also to provide evidence of bad behaviour when they attempted to penalize those who were accountable.

Frequently tied into the investigative part of closed-circuit television is the use of recordings in order to hold people responsible for their actions. The technical personnel in a school is able to print the CCTV images on the screen. This necessity for proof in the form of images of those

disobeying can be seen as an answer to the pupil strategy of denying participation in problematic events. In particular situations, the images were used not only to demonstrate pupils that they had been caught but also to provide proof to parents of misbehaviour.[11]

1.5. The effects of using CCTV cameras in schools

The biggest impact that surveillance cameras could have on people is the invasion of privacy. The common argument is that using monitoring devices to observe or record the activites of someone is a search and seizure on such person. It should be considered unreasonable, and for that reason an invasion of the right of privacy, if it is carried out without any kind of judicial power or in infringement of a person's expectation of privacy.

An important question is whether the closed-circuit television camera truly decreases crime rates. Where crime rates declined in a specific area where the camera is located, it could be since the observation moves the crime somewhere else. Also, criminals and vandals have developed foolproof ways of beating the system, for example, they cover themselves with a mask and change disguises rapidly and have studied how to determine where the monitoring devices are being pointed and take action with speed and immensely increased violence in the short time the lens of the camera rotates elsewhere from them.

Another negative aspect of surveillance cameras is that they can give a wrong feeling of security. Closed-circuit television cameras cannot make anyone completely safe, because if there is a crime that is being carried out in a place, a security camera cannot jump down off the pole to save anyone. Even if the scene is being observed, mostly before the cops show up the crime is already over and the damage is done.
It is a possibility that some, or even many of the cameras are not good enough to deliver an acceptable result; this could be because of a weak picture quality, among other potential technological problems influencing usefulness and reliability.[12]

[11] Hope, A. (2009). CCTV, school surveillance and social control. *British Educational Research Journal*, 35 (6), 898-902.
[12] Akorede Yusuff, A. O. (2011). Legal Issues and Challenges in the Use of Security (CCTV) Cameras in Public Places: Lessons from Canada. *Sri Lanka Journal of International Law*, 23 (1), 55-66.

Individuals, who are against monitoring cameras and surveillance in educational institutions, point out possible negative results that increased monitoring may have on the body of the student. In particular, installing video surveillance cameras in schools could increase mistrust, fear and have negative impact on the climate of the school – mainly those with comparatively poor coherence previous to the implementation of the security camera. The use of CCTV cameras may indicate to pupils that schools are unsafe places that need to be monitored, possibly creating negative expectancy effects and increasing crime.[13]

[13] Fisher, B. W., Higgins, E. M., Homer, E. M. (2019). School Crime and Punishment and the Implementation of Security Cameras: Findings from a National Longitudinal Study. *Justice Quarterly*, 4-5.

2. PRIVACY AND DATA PROTECTION LAW

2.1. The development of privacy and data protection law

Before 1890, the right to privacy was not identified in the law as one of these fundamental rights and there was also no necessity to protect it lawfully. A lot of people think that the Bill of Rights in the Constitution of the United States places a clear basis for the right of privacy. However, the idea of privacy is not particularly stated in the first ten amendments and the word private is used just one time. It was not until 1965 that the Supreme Court discovered a method to make available for use a constitutional foundation for the existence of privacy as a right to be defended. Also, it was not until 1974 when the Congress acknowledged the right especially in a law, which was the Privacy Act of 1974.

The acknowledgment of a right to privacy was debated by Samuel Warren and Louis Brandeis. Their article argued that the person had a right to be let alone. That set the foundation for the adoption of privacy laws in the states for the next ninety years. By 1982 a right of privacy of some sort was acknowledged in 48 states and the District of Columbia.[14]

Privacy is included in article 8 of the European Convention of Human Rights and article 7 of the EU Charter for Fundamental Rights. Both of these instruments defend the right to respect for people's private and family life.[15]

Since the end of the Second World War, a necessity came into being for a more systematic defense of the private lives of the citizens. Soon after this, the United Nations and the Council of Europe laid down the right to privacy as a major human right in worldwide policy documents.

At the start of the 1980's, the Council of Europe adopted the Convention for the defense of people with regard to the automatic processing of personal data. The European Commission saw the

[14] Shank, R. (1986). Privacy: History, Legal, Social, and Ethical Aspects. *Library Trends*, 35 (1), 7-12.
[15] Gellert, R., Gutwirth, S. (2013). The legal construction of privacy and data protection. *Computer Law and Security Review*, 29 (5), 523.

adherence to the 1981 Council of Europe Convention, which is otherwise known as CoE Convention 108, for the defense of people regarding the automatic processing of personal data as a first and sufficient measure for the protection of personal data.[16]

Data protection is also enshrined in the Data Protection Directive, which is otherwise known as Directive 95/46/EC; it presented data protection principles within the law of the EU and it set the fundamentals for the protection of personal data.[17]

2.2. Privacy and data protection law in the European Union

The European Convention of Human Rights and the CoE Convention 108 are some of the most important European Union laws and principles that deal with privacy and data protection law.

After the Lisbon Treaty came into force in December of 2009, the right to the defence of personal data is officially configured as an independent major right of the EU. It is included in Article 8 of the EU Charter of Fundamental Rights, which has obtained lawfully binding force. The article states that everyone has the right to the defence of any information relating to him or her. Such kind of info has to be processed righteously for specified objectives and on the basis of the agreement of the individual involved.[18]

In 1995, the European Union legislated Directive 95/46/EC on the protection of people regarding the processing of personal information and the free movement of such kind of data, which creates an extensive regime of data protection. This law is called the Data Protection Directive. The Directive forbids the transference of personal information to countries, who are not member states to the EU which are considered to present a level of protection of personal information that is insufficient.[19]

The Data Protection Directive intends to serve the contradictory objectives of defending data subjects and simplifying free trade within the European Union. The Directive particularly indicates

[16] Kosta, E. (2013). *Consent in European Data Protection Law*. Vol 3. Leiden, The Netherlands: Martinus Nijhoff Publishers, 12-14.
[17] Gellert, R., Gutwirth, S. (2013). The legal construction of privacy and data protection. *Computer Law and Security Review*, 29 (5), 523.
[18] Gonzalez Fuster, G., Gellert, R. (2012). The fundamental right of data protection in the European Union: in search of an uncharted right. *International Review of Law, Computers and Technology*, 26 (1), 73.
[19] Bergkamp, L. (2002). EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information – Driven Economy. *Computer Law and Security Review*, 18 (1), 32-33.

to the right to privacy, alongside trade extension and the free flow of personal information.[20] The main principles in this Directive are that personal information has to be processed righteously and legally, collected for specified, clear and lawful objectives; that the data that is collected is sufficient, appropriate and not redundant relating to the intentions for which they are collected; that it is precise and, where essential, kept up to date. Additionally, personal data can be processed only under certain situations.[21]

In April 2016, the GDPR, which is otherwise known as the General Data Protection Regulation, was passed and it replaced the Data Protection Directive. The GDPR became enforceable on the 25th of May 2018. This Regulation consists of laws that are related to the defense of natural persons regarding the processing of personal information; it also protects basic rights and freedoms of physical persons and especially their right to the protection of information that relates to an identified or identifiable living individual. In addition, it defines many words, but the most important ones are the following: personal data, processing, processor, consent, genetic data, biometric data and data concerning health. Furthermore, it talks about principles that are related to the processing of personal information. Personal data has to be processed legitimately, equitably and in a manner that is transparent; it has to be collected for objectives that are clear, legal and specific; it has to be relevant, adequate and precise. There are also the rights of the data subject. Some of them include the right to acquire from the controller validation as to whether or not personal information regarding him or her are being processed and access to the data; the data subject also has the right to the correction of personal info that is imprecise; also, the person who can be identified, has the right to acquire the removal of personal data that is related to him or her and there is also the right to the limitation of processing.[22]

2.3. Legal basis for the processing of personal data

Personal data signifies any information that is related to an identified or identifiable living human being. An identifiable living person is the one who can be identified, either directly or indirectly, especially by indication to an identifier like a name, location info or to factors that are specific to the genetic, mental, physical or social identity of that individual. The processing of personal data

[20] Birnhack, M. D. (2008). The EU Data Protection Directive: An engine of a global regime. *Computer Law and Security Review*, 24 (6), 512.
[21] OJ L 281, 23.11.1995, art 6, sec. 1.
[22] OJ L 119, 4.5.2016, art 1, 4-5, 15-18, 24, 28, 45.

is any operation involving personal info, including the use, collection, organisation, storage, consultation, retrieval and disclosure as well as the removal, limitation or destruction.

Processing of personal data is legal only if the data subject, which happens to be the student in this case, has given consent to the processing of his or her personal information; in addition, if the processing is essential for the performance of an agreement or if it is required for compliance with a lawful obligation; also, if the processing is needed so as to defend the significant interests of the data subject; furthermore, if the processing is requisite for the performance of a task or for the objectives of the legitimate interests. Consent to the processing of personal data ought to be given by an obvious affirmative act that establishes a concrete, informed and freely given indication of the student's agreement to the processing of personal data that is related to him or her. Also, the consent should be either an oral or a written statement. Inactivity or silence is not considered to be consent. In addition, the student is able to withdraw his or her agreement at any time.

Sensitive personal data is a specific kind of information that has to be treated with extra security. For example, the following is considered to be sensitive info: political views, religious or philosophical beliefs, racial or ethnical background, trade union membership, biometric and genetic records, as well as data regarding health or a natural person's sex life or sexual orientation. It is forbidden to process this sort of personal data. However, personal info that is sensitive can be processed if the data subject has given clear agreement to the processing of those personal data; if the processing is essential for the objectives of carrying out the duties and exercising concrete rights of the controller or if it is requisite to defend the significant interests of the data subject; if the processing is performed in the course of its legal activities with relevant safeguards by an association, foundation or any other not – for – profit body; if processing is related to personal information which are obviously made public by the data subject; if processing is needful for the foundation, exercise or protection of claims that are legal; if processing is needed for reasons of important public interest; if processing is necessary for the objectives of anticipatory or job – related medicine; if processing is required to be done for reasons of public interest in the public health area or if processing is needful for archiving aims in the public interest, historical or scientific investigation objectives or statistical goals.

There are six principles that need to be followed to process personal data and they are the following: personal data has to be processed legally, fairly and in a way that is clear in relation to the data subject; gathered for explicit, specified and lawful objectives and not further processed in

a manner that is controversial with those aims; information also needs to be appropriate, adequate and restricted to what is needed in relation to the aims for which they are processed; data has to be precise and kept up to date; in addition, it has to be held in a way which allows identification of data subjects for no longer than is needed for the objectives for which the personal info are processed and it has to be processed in a method that ensures relevant security of the data, including defense against illegal or unauthorised processing and against random loss, damage or destruction, using suitable organisational or technical measures.[23]

[23] OJ L 119, 4.5.2016, art 4-7, 9; recital 32.

3. THE RIGHT TO PRIVACY

3.1. The right to privacy of students

The right to privacy is a basic right that ensures freedom and respect for the person's family and private life. With the evolution of technology, the defense of this right has become progressively weak and the use of such kind of devices has become danger contributing to the infringement of privacy.[24] It is frequently recognized that, as new ways of recording, monitoring and analyzing people and their information come into being with ever rising frequency, legal systems globally are incapable to keep apace.

The European Union Data Protection Directive 1995 insists that members defend peoples' right to privacy regarding the processing of personal data. In the US, constitutional explanation has developed in the courts, appearing in some laws and executive orders dealing particularly with data protection. The American Civil Liberties Union confirms that schools that are using closed-circuit television cameras are unlawfully violating the legal expectation of privacy of pupils, staff and faculty, and are becoming involved in unreasonable search without a probable cause and without a warrant. Regardless of this declaration, it is unrealistic that CCTV in educational institutions will be ruled as unlegal in the courts of the United States.[25] The legitimacy of video surveillance cameras in schools has not, to this point, been severely challenged, and the use of monitoring cameras is rapidly becoming normal school practice.

In the United States of America, the most important law that deals with the privacy of pupils is the Family Educational Rights and Privacy Act, which is otherwise known as FERPA. FERPA defends the privacy of student records; it also allows students to update their own data. This law applies to every educational institution that are given funds under an applicable program of the U. S. Department of Education. FERPA grants parents particular rights in relation to their kids'

[24] Kiral, B., Karaman Kepenekci, Y. (2017). Opinions of the Class Teachers towards "Privacy" and Its Violation. *Eurasian Journal of Educational Research*, 71, 23.
[25] Ball, K., Haggerty, K. D., Lyon, D. (2012). *Routledge Handbook of Surveillance Studies*. London: Routledge, 228.

education data. These rights are transferred to the pupil when she or he becomes 18 or goes to school beyond the high school level. The pupils who receive these rights are called "eligible students". Eligible students or parents have the right to review and control the education data of the students that are maintained by the educational institution. They also have the right to demand that a school corrects data if they think that it is misleading or not accurate.[26]

FERPA enables educational institutions to disclose pupil's education data, without permission, to the following parties or under the following conditions: school officials who have lawful academic interest; other educational institutions to which a pupil is going to; specified officials for assessment aims; suitable parties in connection with monetary aid to a pupil; institutions who are conducting specific studies on behalf of the school; accrediting organizations; to follow a legally issued subpoena or a judicial order; suitable and relevant officials in cases of safety and health emergencies and local and state authorities according to particular law within the state.[27]

There have been cases in the US regarding the proccesing of students' data. For example, one such case was Jackson vs McCurry, which was about if administrators in an educational institution may search the contents of a pupil's cell phone without their permission. Two high school receptionists searched a pupil's mobile phone without any kind of warrant or the student's permission during their investigation of alleged threats made against the student. On the basis of this and some other events, the parents of the student filed suit, claiming that the school infringed the pupil's Fourth Amendment rights. The Court decided that defendants had reasonable grounds to have a suspicion that a search of EDJ's text messages would uncover proof that she was infringing school rules against harassment. The receptionists searched the mobile phone believing that she was sending negative messages about M to other pupils. This belief was based on info provided by other pupil interviews. And since the conduct alleged constituted harassment under school policy, the Court decided that the administrators had reasonable grounds to search the mobile phone.[28]

Another example of a case was Chicago Tribune Co. v. University of Illinois. In 2009 the Chicago Tribune was carrying out an investigation into allegations that the University of Illinois had a particular recruitment track for well-connected families. So as to acquire info about the scope of this program, the Tribune used state freedom of information requests to seek data related to the

[26] 20 US Code. Sec. 1232 g; 34 C. F. R. Part 99. Family Educational Rights and Privacy Act of 1974.
[27] 20 US Code. Sec. 1232 g; 34 C. F. R. Part 99. 31. Family Educational Rights and Privacy Act of 1974.
[28] United States Court of Appeals, 18-10231, *Jackson v. McCurry*.

program. The educational institution said that revealing data about scholarships would infringe FERPA. The Tribune sued, and the U. S. District Court for the Northern District of Illinois consented that FERPA did not forbid the publication of the data in question. The University of Illinois appealed to the U. S. Court of Appeals for the Seventh Circuit. In 2011, the First Amendment groups and a coalition of media filed a brief supporting the Tribune, arguing at educational institutions constantly use FERPA to cover up misuses of the public trust and to undermine the clear objective of state open data laws. In 2012, the Seventh Circuit eventually remanded the case to the district court with an order to dismiss the case for a lack of subject-matter jurisdiction.[29]

The right to privacy can be thought of as a welfare right. A lot of people have an interest in privacy; that is, in controlling access to their bodies and info about themselves. Unwished exposure of our body or our private info can give rise to severe monetary, psychological or even physical harm. We desire privacy not due to the fact that it is something good in itself, but for the reason that we want to avoid the external damage caused when we cannot control access to ourselves. Both adults and children can be damaged via privacy infringements – the physical and psychological damage that is caused by sexual predation is one clear example that both kids and grown-ups would wish to keep from happening. As a result, it appears to be that privacy actually can be regarded as a welfare right that both adults and children share, and privacy rights serve to defend that interest.

Understanding youngster's right to privacy as a prosperity right does not seem to give us a strong right to privacy in educational institutions. A right to privacy that is founded on well – being interests does not stand up very well when compared to other essential welfare considerations that conflict with privacy. Because of this, monitoring practices usually seem to create less damage than the infringements these practices aim to keep from happening. Certainly, safety over privacy is nearly always the rallying cry of those who would limit privacy, however, in educational institutions the tradeoff appears to be more justified. Pupils are lawfully required to be in schools, but people are not for instance legitimately required to fly the airlines. Since schools are compulsory, there is less of a chance to opt out and exercise an option to avoid risk. Because of this, educational institutions have a special duty to reduce risk. Pupils cannot decide to remain home; also, schools have a responsibility to make them secure.

[29] United States Court of Appeals, Seventh Circuit, 680F. 3d 1001, *Chicago Tribune Co. v. University of Illinois*.

Another method of thinking about children's rights is to take into account a dissimilar kind of right. There are rights that we give to kids in the interests of grown-ups they will one day become, which are called rights that are developmental. These kind of rights are granted to the youngster so as to make possible the exercise of particular liberty rights as a grown-up. These sort of rights are named the "right to an open future". The exercise of a freedom right demands the capability to select, and the growth of the power to pick insists an environment that enables kids to acquire knowledge about dissimilar chances of life and allows them to practice rising levels of self-governance founded on their own justification that is free from outside control. The theoretical presence of the coming grown-up who will one day be given the chance to exercise opportunity and autonomy proves or shows a set of rights to be correct for the kid that is presently existing. The youngster has a right to be ready to live a life that is independent.

The right to privacy is related to the right to an open future. Enabling people to do something independently and to decide on their own is how we honor them. We infringe on the freedom of a person when we exercise control that is parental and demand on checking and being in charge of our access to the activities of him or her. When we continously look at what other people do, we do not make them more confident so that they can do something for their own reasons; rather, we hearten them to act as we want them to.

Take into account what people would think of a grown-up who continually watches the every action of her teenage daughter. Depending on the matureness and the age of the girl, the majority of people would think of such actions as objectionable. The teenager would constantly act like her parent were observing. A person who is being constantly kept an eye on undergoes social pressure such that the ability to act autonomously and individually is vanished.

Placing the value of liberty into a developmental context hints that privacy ought to be realized as a section of a developmental right and not just a well-being right. Observation in educational institutions is in tension with the practice of independent activity. It does not permit pupils to do something on their own. While youngsters are under observation, they know that others are the ones who tell people what to do and that they are not being honored as actors who are able to decide their own way. This is basically the same as the teenage child of the mom situation. If the kid is not able to break free from the observant eye of the parent, she cannot learn to decide based on her own reasons. Some sort of privacy is necessary for her so that she can develop the powers of self-governance.

Educational institutions have to recognize that pupils have a well-being interest as well as a developmental interest in privacy based on their right to a future that is open. Just as a kid has got a lot of dissimilar well-being interests, some of which could conflict with the interests that assist the privacy right, in addition, there looks to be much aspects of the growth of independence that are incompatible with agreeing to give pupils privacy that is strong. Besides, security and safety are preconditions for an open future as well. For instance, a kid who is bullied, is not being permitted to practice liberty. To the extent that safety in educational institutions is maintained by observation, supervision might be needed as well as part of pupils' larger right to an open future. An additional example is that, it can be disputed that a proper education appears to be a precondition for an open future. If observation can decrease the disturbing chaos of an academic environment and enable pupils to obtain a satisfactory education, then it appears to promote an open future as well.

There are strong reasons to give kids privacy in schools, however these causes do not support any inviolable or absolute right to privacy in educational institutions. The right to privacy that pupils enjoy has to be balanced with maintaining other rights that are justifiable in the same manner. Taking into account the advantages of privacy, observation should only be used if there is proof of an active danger to the other well-being interests of students, developmental interests, or rights as present and future citizens, and it should end if there is no proof of a continued danger. The level of monitorization should not be more than what is necessary to settle problems that are specific and still going on.[30]

3.2. The right to privacy of teachers

The most common reasoning for using CCTVs in educational institutions is the security and safety of pupils. However, there were 27 interviews carried out with Israeli school principals and there were indications to monitoring practices targeting teachers. In order to realize the surveillance of teachers a little bit better, 55 interviews were carried out with Israeli teachers, 28 of them said that school surveillance cameras targeted them.

[30] Warnick, B. R. (2007). Surveillance cameras in schools: An Ethical Analysis. *Harvard Educational Review*, 77 (3), 321-327.

A survey was carried out by NASUWT in 2014, which is the biggest teachers' union in the United Kingdom and it declared that the monitoring of teachers was actually a common occurrence. The results revealed that one third of teachers felt that surveillance cameras in educational institutions was a violation of their privacy.

The principals in schools are the ones who control the majority of video surveillance cameras. The usage of Closed-Circuit Television is usually motivated by risk anxiety. The subjects of this kind of anxiety are the students, and the objects of observation are malicious external parties, or pupils who could hurt their peers. The typical use of monitoring cameras is to examine minor disciplinary infringements. While the teachers are bystanders in this situation, they are still caught in the eye of the cameras, and they also become the objects of observation.

In their relationships with pupils, teachers are educators; however, in their relationship with principals, teachers are employees. Employers observe workers in many work-related contexts, like Internet usage and email, biometric technologies, and location tracking, normally as a means of identification. Employers' interests are categorized into three fundamental groups: observing productivity, defending the interests of the company and defending the organization from lawful obligations. Workers are interested in preserving a proper workplace environment that honors and defends them.

The courts in the United States have ruled in many cases that teachers do not have reasonable expectation of privacy in special education classrooms, or in a break room. Then again, European law demands on a proportional balance, as reflected in formal opinions of the European Union's data protection expert group, and in European Court of Human Rights jurisprudence. When it comes to the video surveillance cameras, lower courts ruled that hidden cameras infringed the privacy of the employees.

The educational institution as a workplace has its own unique features. The school's interest in using video surveillance cameras to observe teachers is mainly to defend it from legal liability, like negligence in cases of pupil injury. Furthermore, the school is a dual environment, which means that it operates simultaneously as a workplace for teachers and as a teaching institution for students. In addition, educational institutions are distinctive in that they are meant to be places that are devoted to development and learning.

The interviews revealed many forms of teachers' observation: keeping an eye on the participation of teachers, examining teaching and disciplining of pupils, viewing on-duty teachers at the time of school recess and observing non-classroom time management.

The law could have offered a toolkit to address the monitorization of teachers by video surveillance cameras. Using the principles that are developed in Israeli privacy and employment law would demand a set of measures in educational institutions, like showing a lawful school interest that can justify the observation of teachers, letting the teachers know about the use of CCTVs and their actual use, asking for their free and informed consent and more. No evidence of any of these measures was found in the interviews. In addition, the interviewees did not indicate to the potential unlawfulness of the principals' practices.[31]

[31] Perry-Hazan, L., Birnhack, M. (2019). Caught on camera: Teachers' surveillance in schools. *Teaching and Teacher Education*, 78, 193-203.

CONCLUSION

The aim of the paper was to investigate which data protection principles do educational institutions have to comply with and whether the rights of pupils and teachers are being infringed by using surveillance cameras as well as which problems can redundant interference cause on the privacy of students. The hypothesis of the paper was that if schools have to comply with specific principles like purpose limitation, lawful processing and some other conditions, then it is still unlawful to use video surveillance cameras; students' and teachers' rights are not violated and unreasonable interference on students' privacy does not cause any issues.

In the first chapter of the paper, the birth and the development of CCTV cameras was talked about. In addition, it was found out that CCTV is a visual observation technology that is designed for monitoring a variety of environments and activities. Also, the difference between CCTV and IP cameras was discussed. Furthermore, the places that use these types of surveillance cameras like town centres, retail outlets and shopping centers as well as hospitals and schools were mentioned. Also, the reasons why schools are ethically different from many other public places and the conditions under which CCTV cameras are legal; moreover, the reasons for why schools use these cameras, like for example to tackle vandalism, bullying and theft was talked through. Finally, the effects of using monitoring cameras in schools, the biggest impact being the invasion of privacy was written about.

The second chapter of the paper examined privacy and data protection law. Since there is no specific law that deals with data protection principles schools must follow and the processing of personal data in schools specifically, then the GDPR was used. The processing of personal data is legal only if the data subject who happens to be the student in this case, has given permission to the processing; if the processing is important and necessary for the performance of an agreement or if it is required for compliance with a lawful obligation; also, if the processing is needed so as to defend the significant interests of the data subject; furthermore, if the processing is requisite for the performance of a task or for the objectives of the legitimate interests. Educational institutions have to follow the next principles: personal data has to be processed legitimately, fairly and in a

way that is clear in relation to the data subject; gathered for explicit, specified and lawful purposes and not further processed in a way that is controversial with those aims; info also needs to be appropriate, adequate and limited to what is needed in relation to the aims for which they are processed; data has to be precise and kept up to date; in addition, it has to be held in a way which allows identification of data subjects for no longer than is needed and it has to be processed in a method that ensures relevant security of the information.

In the third part of the paper, the right to privacy of students and teachers was examined. Redundant exposure of the body of people or their private info can give rise to very serious financial, psychological or even physical harm. Furthermore, when we constantly monitor what others do, we do not encourage them to act for their own reasons; rather, we hearten them to act as we want them to act.

LIST OF REFERENCES

Scientific books

1. Ball, K., Haggerty, K. D., Lyon, D. (2012). *Routledge Handbook of Surveillance Studies*. London: Routledge.

2. Ciescynski, J. (2006). *Closed Circuit Television*. 3rd ed. Oxford, UK: Elsevier Science and Technology.

3. Harwood, E. (2007). *Digital CCTV: A Security Professional's Guide*. California, USA: Elsevier Science and Technology.

4. Kosta, E. (2013). *Consent in European Data Protection Law*. Vol 3. Leiden, The Netherlands: Martinus Nijhoff Publishers.

5. Norris, C., Moran, J., Armstrong, G. (1998). *Surveillance, Closed Circuit Television and Social Control*. 1st ed. London: Routledge.

6. Purpura, P. P. (2010). *Security: An Introduction*. 1st ed. Boca Raton, Florida: CRC Press LLC.

Scientific articles

7. Akorede Yusuff, A. O. (2011). Legal Issues and Challenges in the Use of Security (CCTV) Cameras in Public Places: Lessons from Canada. *Sri Lanka Journal of International Law*, Volume 23, Issue 1, 33-76.

8. Bergkamp, L. (2002). EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information – Driven Economy. *Computer Law and Security Review*, Volume 18, Issue 1, 31-47.

9. Birnhack, M. D. (2008). The EU Data Protection Directive: An engine of a global regime. *Computer Law and Security Review*, Volume 24, Issue 6, 508-520.

10. Fisher, B. W. Higgins, E. M., Homer, E. M. (2019). School Crime and Punishment and the Implementation of Security Cameras: Findings from a National Longitudinal Study. *Justice Quarterly*, 1-25.

11. Gellert, R., Gutwirth, S. (2013). The legal construction of privacy and data protection. *Computer Law and Security Review*, Volume 29, Issue 5, 522-530.

12. Gonzalez Fuster, G., Gellert, R. (2012). The fundamental right of data protection in the European Union: in search of an uncharted right. *International Review of Law, Computers and Technology*, Volume 26, Issue 1, 73-82.

13. Heintzelman, S. C., Bathon, J. M. (2017). Caught on Camera: Special Education Classrooms and Video Surveillance. *International Journal of Education Policy and Leadership*, Vol. 12, No. 6, 1-16.

14. Hope, A. (2009). CCTV, school surveillance and social control. *British Educational Research Journal*, Vol. 35, No. 6, 891-907.

15. Kiral, B., Karaman Kepenekci, Y. (2017). Opinions of the Class Teachers towards "Privacy" and Its Violation. *Eurasian Journal of Educational Research*, No. 71, 21-40.

16. Perry-Hazan, L., Birnhack, M. (2019). Caught on camera: Teachers' surveillance in schools. *Teaching and Teacher Education*, Vol. 78, 193-204.

17. Shank, R. (1986). Privacy: History, Legal, Social, and Ethical Aspects. *Library Trends*, Vol. 35, No. 1, 7-18.

18. Taylor, E. (2011). UK schools, CCTV and the Data Protection Act 1998. *Journal of Education Policy*, Volume 26, Issue 1, 1-15.

EU and international legislation

19. 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, OJ L 281, 23.11.1995, p. 31-50.

20. 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), OJ L 119, 4.5.2016, p. 1-88.

Other countries' legislation

21. 20 US Code. Sec. 1232 g; 34 C. F. R. Part 99. Family Educational Rights and Privacy Act of 1974.

Other court decisions

22. United States Court of Appeals, Seventh Circuit, 680 F. 3d 1001, *Chicago Tribune Co. v. University of Illinois*.

23. United States Court of Appeals 18 – 10231, *Jackson v. Mccurry*.

Other sources

24. Squelch, J., Squelch, A. (2005). Webcams in Schools: A Privacy Menace or a Useful Monitoring Tool. *Australia and New Zealand Journal of Law Education*, Volume 10, Issue 2 and Volume 11, Issue 1, 55-66.

25. Warnick, B. R. (2007). Surveillance cameras in schools: An Ethical Analysis. *Harvard Educational Review*, Volume 77, Issue 3, 317-343.

Appendix. Non-exclusive licence

A non-exclusive licence for reproduction and for granting public access to the graduation thesis

I Anar Agajev

1. Give Tallinn University of Technology a permission (non-exclusive licence) to use free of charge my creation
"Using CCTV cameras in schools and the student's right to privacy",

supervised by Kärt Salumaa-Lepik,

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of Taltech library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of Taltech library until the copyright expires.

2. I am aware that the author will also retain the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection act and other legislation.