Research Article https://doi.org/10.12973/eu-jer.11.2.1219

European Journal of Educational Research
Volume 11, Issue 2, 1219 - 1229.
ISSN: 2165-8714
https://www.eu-jer.com/

Surveillance in Schools Across Europe: A New Phenomenon in Light of the COVID-19 Pandemic? The Cases of Greece and France

Anastasia Karagianni*
University of Athens, GREECE

Vagelis Papakonstantinou
Vrije University of Brussels, BELGIUM

Received: October 3, 2021 ▪ Revised: February 2, 2021 ▪ Accepted: April 2, 2022

Abstract: Surveillance technology is more and more used in educational environments, which results in mass privacy violations of kids and, thus, the processing of huge amount of children's data in the name of safety. Methodology used is doctrinal, since the focus of this research was given in the implementation of the legal doctrine of data protection law in the educational environments. More than that, the cases of Greece and France regarding the use of surveillance technologies in schools are carefully studied in this article. Privacy risks that both children and educators are exposed to are underlined. In these terms, this research paper focuses on the proper implementation of the European data protection framework and the role of Data Protection Authorities as control mechanisms, so that human rights risks from the perspective of privacy and data protection to be revealed, and the purposes of the use of such technologies to be evaluated. This study is limited in the legal examination of the European General Data Protection Regulation, and its implementation in the legal orders of Greece and France, and practice pertaining to the case studies of Greece and France respectively.

Keywords: *Bio-surveillance, children's rights, data protection, privacy, video-surveillance.*

To cite this article: Karagianni, A., & Papakonstantinou, V. (2022). Surveillance in schools across Europe: A new phenomenon in light of the COVID-19 pandemic? The cases of Greece and France. *European Journal of Educational Research*, *11*(2), 1219-1229. https://doi.org/10.12973/eu-jer.11.2.1219

Introduction

Since March 2020, a global crisis has been caused by the Coronavirus disease (COVID-19) pandemic (World Health Organisation, 2020). Many people have been told to practice social distancing or self-isolate as a necessary measure to curb the spread of the virus and to protect vulnerable people. Staying indoors and completely avoiding physical contact with other people has resulted in individuals turning to online platforms to be educated, to remain in contact with family and friends, to obtain information about government responses and public health advice, and to take part in public debate and civil engagement. Consequently, this digital transformation of people's personal and professional life requires the legal framework of digital rights protection to be safeguarded, mainly when surveillance technologies are deployed and used.

Nevertheless, surveillance is not a new phenomenon since it has been apparently taken place in schools not only during the pandemic but also before that. As the COVID-19 pandemic led to massive closure of schools across Europe, many states took measures to limit the rapid spread of the virus within school environments moving to online distance learning. Not only educators, but also kids and parents have become familiar with live streaming tools and web cameras used for educational purposes. However, it is not the first time that cameras have been used in the educational context besides in the different forms of "online schools", such as "e-class" used in Greece and "Klassroom" in France. The installation of Closed-Circuit Television, known as CCTV cameras, and in general the use of video surveillance or any kind of biometric surveillance tools- such as facial recognition technology-, as it will be described in the following chapter, are measures that have been taken by many states in the face of safety, security or discipline problems in schools. Safety and health conditions in education intend to minimise accidents during school hours such as instances of mugging, bullying, and the sale or use of illegal drugs. This is the main subject that will be examined in this article.

In the first section of the article a definition of video surveillance will be given, as well as a brief overview of the surveillance-case study that will be further examined below. In the second section, the legal framework, the data protection regime, will be presented based on which the challenges set by these surveillance technologies will be further

* **Corresponding author:**
Anastasia Karagianni, PhD student at the University of Athens, Greece. ✉ karaanast@outlook.com.gr

analysed. In the third section, the cases of Greece and France will be studied in more details. In the conclusion, after examining carefully these two case studies, concluding remarks regarding the common key problems faced with the use of surveillance tools in these three countries will be presented, concerning mainly the non-proper compliance of school units and tech companies that deploy such tools with the General Data Protection Regulation, as well as the early activation of relevant protection mechanisms, such as the one of the Data Protection Authorities.

Surveillance in European Classrooms

CCTV cameras refer to a system of cameras that monitors a particular place/space and the image can be viewed on a screen and recorded in a video. The main reason for installing such a system is the supervision of a space, such as in a bank, in a government building in order to indirectly protect employees, goods and products, and space from vandalism, fires, etc. Surveillance technology, and more particularly video surveillance, can also be found in schools. The primary aims of surveillance technology in schools are to enhance the safety for students and staff, protect school property against destructive acts, such as vandalism, and contribute to the identification both of students who are not disciplined to the "schools'' codes of conduct" or "school principles/rules", and crime perpetrators.

CCTV systems should not be related with the recording of a school ceremony by the side of parents, educators and school staff, such as in a school fiesta or concert, or in instances where the lesson is recorded for educational or research purposes. However, video surveillance can be used for investigation purposes when justice is served or in a case when an authority conducts the surveillance in the context of a search warrant. This is the reason for the authorisation of CCTV system installation in school premises in Greece that will be examined below. However, it is questionable whether online distance education tools in Greece were used for massive surveillance of students and educators.

Another form of surveillance, biometric surveillance (Digital Freedom Fund, 2020) of facial recognition system was used in two high schools in France as well. In 2019, a regional authority in Marseille and Nice launched an experimental security project by installing facial recognition gates at the entrance of the school premises. The gates with the use of facial recognition technology could identify the students and distinguish them from unidentified visitors.

It is worth mentioning that facial recognition system has been recently used in the United Kingdom, in school canteens, as a more "COVID-19-secure" way of payment. More particularly, on 18 October 2021, nine schools in North Ayrshire "started taking payments for school lunches by scanning the faces of pupils, claiming that the new system speeds up queues and is more COVID-19-secure than the card payments and fingerprint scanners they used previously". North Ayrshire council states that 97 per cent of children or their parents had given consent for the new system. "Pupils often forget their PINs and unfortunately some have also been the victim of PIN fraud, so they are supportive of the planned developments and appreciate the benefits to them". However, the Biometrics Commissioner for England and Wales stated that "just because schools can use the technology does not mean they should. If there is a less intrusive way, this one should be used".

To sum up, although the justification of the use of such security measures is based on safety concerns, which is a reason that provides exceptions of the implementation of privacy and data protection regime, this does not mean that it is always acceptable. On the contrary, the acceptance of this justification is estimated under the existence of alternative, less intrusive to privacy and data protection measures.

Legal Concerns From an EU Personal Data Protection Point of View

Besides safety, security and discipline policies as legal reasons for the processing of students' and educators' personal data, schools, as State Educational Authorities, should address privacy concerns regarding the use of these surveillance technologies (European Data Protection Supervisor, 2010). The video footage or face image captured through a CCTV or web camera and used to identify that person- either directly or indirectly- is considered to be personal data. In these cases, European General Data Protection Regulation (GDPR) (declared in 2016 and came into force in 2018), hereinafter GDPR, requirements for personal data processing are enforced. GDPR has been regulated in the context of Directives 679/2016 and 680/2016 of the European Parliament and of the Council (European Parliament, Council of the European Union, 2016a and 2016b).

More specifically, according to Article 4 (1) of the GDPR, " 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person," while according to the second paragraph, "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". Consequently, all processing done by school units is regarded as data processing and as such should be taken according to GDPR safeguards. The data described in Article 4 (1) of the GDPR should be processed lawfully, fairly and in a transparent manner in relation to the data subject, based on Article 5 of the GDPR. It is crucial to stress out the

definition of "biometric data", which is based on Article 4 (14) and means "the personal data is resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images".

At this juncture, it is worth clarifying that in order for the personal data to be qualified as biometric data according to the regulations of GDPR, the measurement of the physical, physiological, or behavioural characteristics of an individual must be implied. In Article 9 of GDPR, it is stated that "there have to be a specific technical processing of that face image or video footage related to the physical, physiological or behavioural characteristics in order for it to be considered biometric data". The image or footage is not considered to be a biometric data by itself under Article 9, if it has not been specifically technically processed so that it contributes to the identification of an individual.

However, it should be highlighted that biometric data is considered to be sensitive personal data and processing of sensitive data is restricted. Processing of biometric data is prohibited unless the data subject has given explicit consent, or there are special circumstances allowing the processing. There are special circumstances under which the processing of a special category of personal data is allowed based on the GDPR. The processing of special categories of personal data is explicitly described in Article 9 of the GDPR.

Furthermore, regarding the obligations of the processing and the role of the 'controller', according to Article 4 (7) and (8) of GDPR, "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data", while "'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". According to paragraph 9, "'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not". The distinction of these three roles is of great importance for the following analysis regarding their responsibilities and legal obligations derived from the GDPR.

As such, schools having mainly the role of the controller should process students' and educators' personal data in a lawful, fair and transparent way in relation to the data subject, according to Article 5 (1) of the GDPR. Particularly when the data subjects are students and the legal processing is based on legitimate interest or the execution of a contract, in the case of a public or private school unit respectively, Articles 6 of the GDPR about the lawfulness of the processing and Article 7 of the GDPR about the conditions for consent should be enforced.

More particularly, in order for video surveillance to be legal, it should be based on a legal ground under Article 6 (1) and (2) and Recital 40 of the GDPR. Specifically, the lawful bases for data processing are consent, the performance of a contract, a legitimate interest, the protection of vital interests, the protection of a public interest- like safety and security-, and a legal requirement. However, if school units as State Educational Authorities are about to implement a video surveillance system on school premises, consent is not recommended as a lawful base. Consent is a legal ground that can be used exceptionally as a legal basis for data processing according to Article 7. As such, school units should not override the freedom and rights of an individual. Furthermore, the legitimate interest needs to be of real existence and has to be a present issue, like property protection or preservation of evidence.

Moreover, school units are not allowed to process biometric data for the purpose of uniquely identifying a student according to Article 9 (1) of the GDPR. Moreover, they should make every reasonable effort to protect the collected and processed personal data, adopt proper security management arrangements against unauthorised access to these datasets, and retain a limited number of personal data about an individual so that they can give them access according to Article 15 of the GDPR. Subsequently, based on Article 5 of GDPR school units should process the data according to the seven processing principles enshrined in GDPR, such as i. lawfulness, fairness and transparency, ii. purpose limitation, iii. data minimisation, iv. accuracy, v. storage limitation, vi. integrity and confidentiality (security) and vii. accountability.

No personal information may be collected by school units unless the collection of that information is expressly authorised under the national legislation, law enforcement purposes are served, or that information relates directly to and is necessary for an operating program or activity of the school. Furthermore, any form of surveillance is an intrusion on the fundamental rights of privacy and data protection. For this reason, it must be provided by law, be necessary and proportionate.

Moreover, school units must comply with the transparency principle and provide information about the installation and operation of surveillance by publishing a surveillance notification in advance according to Article 12 of GDPR. The notice should be easily visible in a plain language, with the appropriate camera symbol informing everyone entering the school premise about video surveillance. They should also provide contact information about the data controller and explain the reason(s) for surveillance. Other information can be made available to the data subject upon request in accordance with Article 13 and Article 14 of the GDPR.

The data subjects, namely the parents and educators, have the right to be informed by the data controller about whether their data is processed, to access to the file with their personal data and the information described in Article 15 of GDPR. Data subjects should also be informed about the purpose of the processing, the categories of processed personal data, and the recipients to whom the personal data have been or will be disclosed, as well as the period of time during which the data will be stored.

In order for privacy concerns to be counterbalanced in the case of video surveillance, a Data Protection Impact Assessment study, hereinafter DPIA, must be conducted according to Article 35 of the GDPR. Specifically, DPIA is a process that identifies and minimises risks related to personal data processing. In the case of video surveillance, a DPIA is required in instances when surveillance imposes high risk, when DPIA is imposed for a data processing activity described in Article 35 (3) of the GDPR, or when the area under surveillance is a public area.

It is important to flag that the people who are directly involved, namely the educators, students, parents and other stakeholders, according to Recital 99 of the GDPR, as well as the Data Protection Authority based on Article 36 of GDPR, should have been consulted in advance when a DPIA is conducted, while the CCTV system operators should be familiarised and be sensitive to privacy issues as well. As importantly, CCTV system should subject to constant compliance review and evaluation. Internal compliance reviews should be conducted where external independent compliance reviews are not available. In conclusion, evaluation should take into account the views of different groups of people affected by the surveillance. Results of compliance reviews and evaluations should be made publicly available.

In this context, it is notable that schools should develop an explicit policy on the use of CCTV surveillance. Sound recording is not allowed, since it represents an additional and even more significant layer of privacy intrusion, and therefore a decision to consider sound recording should be subjected to a diligent analysis.

There are certain measures that need to be taken regarding the obligations of the data controller according to Articles 24-43 of the GDPR. In brief, data controller should ensure that: i) data is processed lawfully and in a transparent manner to the data subject, ii) data is collected and processed for specific purposes, and not in a manner incompatible with original purposes, iii) collected data is accurate and up-to-date, iv) data subjects are able to demonstrate compliance.

In light of the COVID-19 pandemic and under the urgent circumstances to establish and use e-learning tools in education, schools may not have proper child safeguarding policies in place to govern student and educators' conversations via private networks and other online tools. Parents and caregivers may not be aware of school policies, if they exist, and may not be familiar with new technologies, having not the ability to discuss with their children about online child safety. Companies that are developing and deploying online educational tools should make sure that safety features are integrated, enhanced and clearly accessible to educators, parents and students.

Case Studies in Europe: The Cases of Greece and France

Instances of educational surveillance in Greece and France will be examined below. These countries are Member States of the European Union and as such are bound by EU data protection legislation. One more reason that these cases studies have been chosen is the variety of cases they offer, since almost every state has deployed a different educational surveillance technology and for different reasons. For instance, Greece has deployed online distance education tools in light of the COVID-19 pandemic, while France has deployed entrance authorisation systems.

Moreover, the case of video surveillance via CCTV cameras in Greek schools will be examined as well. More specifically, there is an interesting Opinion published by the Greek Data Protection Authority regarding the CCTV cameras operation in schools, which will be studied in more details below. It is of great importance to zoom in on whether the needs described in the authorisation of the CCTV installation were accepted or not by the Greek Data Protection Authority as justification for the installation of CCTV cameras and the process of students' and educators' data and under what circumstances.

Finally yet importantly, both cases can be categorised under the broad umbrella of bio- surveillance. The extraordinary use of bio-surveillance in schools is of great importance regarding the magnitude of the infringement and the transparent deployment and use of the surveillance technologies.

Greece: COVID-19 Class Surveillance. The Actual Processing Case.

Both primary and secondary schools were closed in Greece from March 2020 to June 2020 due to the COVID-19 pandemic, as well as from November 2020 to June 2021 (Hellenic Republic- Ministry of Education and Religions, 2021). The Ministry of Education first decided in March 2020 with the Administrative Circular 121802/ ΓΔ4/ 15-09-2020 (Hellenic Republic-Ministry of Education and Religions, 2020a) the online distance learning, modern or asynchronous as a measure for the uninterrupted operation of educational institutions, based on Article 16 of the Constitution of Greece. The tool for the online distance learning that has been approved by the Ministry of Education is the Electronic School Classroom service, or e-class. The e-Class platform supports asynchronous distance learning services without restrictions and commitments. Access to them is provided by using a simple web browser, without the requirement of specialised technical knowledge, and is addressed to educators and students, with the aim of enriching and enhancing the classic educational teaching with modern tools that empower the learning process.

The main orientation of the e-Class platform, through Webex, is the strengthening and support of the educational activity through an easy-to-use technological state-of-the-art environment. The aim is to provide and support integrated distance learning activities, offering the instructor-educator a dynamic environment for organising and disseminating knowledge, and the trainee-student an alternative channel of personalised learning independent of space-time commitments

(Hellenic Republic- Ministry of Education and Religions, 2020b). According to the Panhellenic School Network, the main objectives met by the design and the benefits derived from the use of these platforms can be summarised: i) in the integration of new information and communication technologies (ICT) in the educational activity for high quality education services through a modern technological environment, ii) in the creation of an easy-to-use means of interaction and continuous communication between the instructor-educator and the trainee-student, and iii) in the utilisation of educational material and accumulated educational experience.

Applicable Regulatory Framework- Data Protection Regime

On 26 August 2019, the Greek Parliament voted and officially published the legislation on data protection, Act no. 4624/2019 (2019), also known as the Greek Act on Data Protection. More particularly, the Act concerns the implementing measures of the European Regulation 679/2019 on the protection of individuals with regard to the processing of personal data and for the transposition of Directive 680/2016 on the protection of natural persons with regard to the processing of personal data. In addition, the Constitution of the Hellenic Republic in Article 9A provides that "everyone has the right to protection against the collection, processing and use of personal data, as provided by law (Constitution of the Hellenic Republic, 2008). The protection of personal data is ensured by an independent authority, which is established and operates as required by law."

DPA Reaction- Administrative Circular 121802/ ΓΔ4/ 15-09-2020 of the Ministry of Education About the Live Streaming Teaching

According to Article 1 of the Administrative Circular 121802/ΓΔ4/15-09-2020 of the Ministry of Education about the live streaming teaching, primary and secondary schools, both in public and private sector, are obliged to provide online distance education to students who cannot attend the classes exceptionally until the end of the academic year 2021-2022 and only if there is still a risk of spreading the COVID-19 virus (Hellenic Republic- Ministry of Education and Religions, 2021). The duration of the online courses is recommended to last from thirty to forty-five minutes, while the number of students should not exceed the maximum number of physical departments provided in the current provisions (Hellenic Republic- Ministry of Education and Religions, 2020b).

This online distance learning tool is provided to students of school units that are operating normally, namely that: i) are not in a state of temporary suspension or prohibition of operation, who cannot attend the educational process in person, as they belong to high-risk groups, ii) are living together with a person affected by COVID-19, iii) themselves have the symptoms and have undergone a molecular diagnostic test for COVID-19 and for as long as they await the outcome.

The program of the online distance education is determined by the principal of the school unit in collaboration with the relevant Teachers' Association, in accordance with the current directives of the Ministry of Education (Hellenic Republic-Ministry of Education and Religions, 2020c) and is communicated to the Director of Education. In schools of private sector, the units are set up and operate by decision of the Principal of School, which is communicated to the office of the Director of Education. The Principal of School undertakes the duty to inform all parents, guardians or caregivers and students about the processing of their personal data exclusively for the purpose of online distance education by notifying them of the update in Annex III.

However, the data protection rights of educators are not mentioned. This is very crucial, since a couple of educators in the island of Nisyros, in Greece, have complained about the exposure and violation of their intellectual and individual rights, both of teachers and students, after the online uploading and posting of photos and videos, screenshots of their digital class on social media and online networks by a portion of students (Katsikas, 2020). This had as a result their exposure to parents, other relatives or third parties who had no relation with the class. In this context, the most important element of the educational process has been disturbed, which is the uniqueness of the moment and the sanctity of the classroom.

DPA Opinion No 4/2020

In September 2020, the Greek Data Protection Authority has been requested to investigate the compatibility of online distance education tool in school units of primary and secondary education in accordance with the provisions of the GDPR and Act No 4624/2019 as well as whether its provision constitutes lawful processing of personal data or not. The possibility of primary and secondary schools to provide online distance education was also regulated by the Decision of the Ministry of Education No 57233/ Υ1, in which all relevant issues for the implementation of e-learning were provided, such as the terms and conditions of the procedure, including any organisational or technical measures for the protection of personal data of the participants etc.

For this purpose, the Ministry of Education has entered into a contract with Cisco Hellas A.E. as the executor of the processing, which included all the conditions and terms for the protection of personal data in accordance with the provisions of Article 28 of the GDPR. The legal basis for the processing of personal data by the Ministry of Education in the context of providing online distance education is the fulfilment of the obligation for the provision of public education which is at the same time a purpose of public interest according to Article 6 (1) (c) and (e) of the GDPR. A notification

was provided in advance to the subjects about the processing of their personal data in accordance with the provisions of Articles 12-14 of GDPR by the Ministry of Education.

The Greek Data Protection Authority considered the use of online distance education lawful according to Article 63 of the Act No 4686/2020 for the reasons mentioned in this Decision. In the Decision of the Greek Data Protection Authority no. 50/ 16.11.2021 (Greek Data Protection Authority, 2021), the Greek Data Protection Authority ex officio examined the compliance of the Ministry of Education with the recommendations of Opinion no. 4/2020 on the compatibility of modern distance education in primary and secondary schools with the provisions of the legislation on the processing of personal data.

The Authority identified that: a) no detailed investigation of the legality of the processing purposes has been carried out by the Ministry, in particular with regard to consent for access to information stored in a user's terminal equipment, when this is not necessary to provide the service requested by the user, b) the information provided to the data subjects is less than that required by the GDPR, while this information is not in an understandable and easily accessible form with clear and simple wording, especially if it is information that is also addressed to children, c) the applied safety measures, although in the right direction, must be completed, in a way that is available to every educator, while it must be ensured that all the educators involved in the distance education process have received minimal information, d) the Ministry violated the obligation of Article 35 (9) of the GDPR in relation to the expression of opinion of the data subjects or their representatives for the planned processing, e) no proper evaluation of data transmission to non-EU countries has been carried out (according to Art. 44-50 of the GDPR). Taken these into account, the Greek Data Protection Authority reprimanded the Ministry to address the shortcomings in the manner analysed in the decision within a period of two months.

DPA Decision No 21/2019 about the Installation of CCTV Cameras in Schools

The decision no. 21/2019 of the Greek Data Protection Authority in 2019 is a crucial decision, since it was taken after a long debate between educators' coalitions, academia and legislators. It is related with the issue of online distance learning, because it considers the installation of CCTV cameras in schools, another form of surveillance in schools.

The main point of the complaints in this Decision is that a School Principal installs CCTV cameras to deal with the problem of graffiti in school premises. According to the complainant, the purpose of these facilities was to protect the school property from graffiti vandalisms (Smith, 2004). In accordance with Article 75 of the Code of Municipalities and Communities, which stipulates that "Municipal and local Community authorities manage and regulate all local affairs, in accordance with the principles of subsidiarity and proximity, with the aim of protecting, developing and continuously improving the interests and quality of life of the local community".

The installation and operation of a video surveillance system by public authorities, for the purpose of protecting the citizens and the public property, are allowed only in the premises, which they have the responsibility to manage and in accordance with the guidelines of the Authority. As already has been defined by the Authority, the purpose is justified by the legal interest or legal obligation of the owner or manager of a site to protect the site as well as the goods located there from illegal acts. In particular, the protection of citizens and public goods with video surveillance systems may be sought by the relevant public or municipal authority or legal entity under the administrative law or that has a relevant jurisdiction in a particular area.

According to the applicable legislation, the Ministry through the school units and other services is not considered responsible for processing the audio and video data of video surveillance systems installed in school premises- that should operate exclusively after the "opening hours" of the school units. The justification is that according to the above mentioned, the Ministry of Education does not have the power to determine the purpose and manner of processing this data, nor does it actually take any relevant decision or process it, since, based on the Code of the Municipalities and Communities, the responsibilities of maintenance, cleaning and guarding of school premises belong to the Municipalities.

Moreover, in Article 204 (8) of the Act no. 4610/2019 (2019), it is stipulated that ''the recording of audio or video through such systems, installed in the premises of the above public school units by the Municipalities, is allowed in the context of exercising their responsibility for guarding the school premises, according to the Article 75 of the Code of Municipalities and Communities (Act no.3463/2003, 2003), only during the time of non-operation of the school units''.

The Data Protection Authority concludes that a public school is not allowed to use a CCT video surveillance system during the time that it operates, while during the non-operating hours of the school unit, the Municipality has the responsibility for the guarding of the place and therefore only the Municipality is competent for the processing (Directorate-General for Infrastructure, 2016). The CCTV operation should be made under the requirements set by Article 5 of the Act No. 4624/2019 about the legal basis for the data processing.

Concluding Remarks on the Greek Case

Although the use of online distance education tools has been approved as lawful by the DPA, there were privacy and data protection risks that needed to be taken into account. In the DPIA study, some of the risks had been taken into

consideration. It is worth mentioning that the Ministry of Education should ensure that "e-class" and "Webex" platforms provide a safe and favourable environment for kids and adolescents (Kaskamanidis, 2020), while a multi-stakeholder approach is needed to address this problem, including the state, civil society, academia, the tech sector, parents, caregivers and the children themselves.

It is of great importance to note that the COVID-19 pandemic has reformed children's lives in many ways exposing them simultaneously to multiple opportunities. "E-class" being properly used for educational purposes is a tool that helps kids to enhance their educational knowledge. However, the digital environment of "e-class" can also expose children to risks, including cyber bullying, online and self-exposure, which may affect their well-being and the enjoyment of human rights (Zou et al., 2020). For this reason, online distance learning could be an opportunity for the students to enhance their digital skills and familiarise with the online harms, digital safety and digital rights framework. Digital literacy has been gradually seen as a dimension of children's rights to freedom of expression, to the participation of young people and to education.

To sum up, my personal view is that children should be considered as rights holders who are entitled to protection from privacy violations and deserve a digital environment without manipulative and exploitative practices, as United Nations Children's Fund (UNICEF, 2018) has been repeatedly stating. Even though CCTV cameras' installation aims to the guarding of schools premises and thus the safety of students, children should not be under surveillance and their privacy and data protection rights should not be undermined (European Data Protection Board, 2019).

France: Facial Recognition Gates at the Entrance of the Schools. The Actual Processing Case.

A court in Marseille ruled in 2019 that authorities in Provence-Alpes-Cote d'Azur region (in France) had no power to authorise the use of facial recognition systems in two high schools in Nice and Marseille (The Administrative Tribunal of Marseille, 2020). The city's Administrative Court overturned the decision of regional authorities, ruling that only schools had the power to authorise such technology. The court ruled that the decision breached the GDPR regulation, as such systems are based on consent but students cannot give consent freely given the relationship of authority that binds them to the school's administration.

The case stems from an experiment launched at the end of 2018 to equip the Ampère high school in Marseille and Les Eucalyptus in Nice with virtual access control devices, by which cameras would recognise high school students and grant them access and be able to follow the trajectory of people (O' Murchu, 2021). The Administrative Court ruled that using facial recognition to control access to high schools was a disproportionate measure.

French advocacy group La Quadrature du Net, an advocacy organisation that promotes and defends fundamental freedoms in the digital world, brought the case in February 2019 (La Quadrature du Net, 2020). La Quadrature du Net and 80 other civil society organisations and groups signed a joint letter on December 19 calling on French authorities to ban facial recognition for any purposes of security and surveillance.

Applicable Regulatory Framework- Data Protection Regime

Act no 78-17 was adopted in France on 6 January 1978 about Information Technology, Data Files and Civil Liberties (Legifrance, 2019 and Loi no. [Act no.] 78-17, 1978), with which the French Data Protection Authority, the Commission Nationale Informatique and Libertés, hereinafter CNIL, was created. The Act of 1978 has been amended in 2004 by the Loi no. [Act no.] 2004-801 (2004) implementing the Directive 95/46/CE on protection of personal data and in 2016 by the Act for a Digital Republic. French data protection legislation includes the Act No 2018-493, which modified the Act no 78-17 of 6 January 1978 on "Data Processing, Data Files and Individual Liberties". Ordinance no. 2018-1125 was adopted in 2018, for the proper compliance and coherence of the Act No 2018-493, the main piece of the French data protection legislation, with the GDPR.

Finally yet importantly, Decree No 2019-536 was published in 2019, in order to ensure the consistency of the revised Act of 1978 with the GDPR, providing more specifications of data subjects' rights, procedural rules before CNIL, and giving a legal effect to the Act as amended by the Ordinance No 2018-1125 (République Française, 2018). This is because the Act of 1978 sets the general legal framework that applies in cases of data protection in France.

On 14 January 2020, the CNIL published their Draft Recommendations about Cookies and Other Trackers and launched a public consultation on the same issue (Commission Nationale de l'Informatique et des Libertés, 2020). The Draft Recommendations concern the practical methods regarding the obtaining of user's consent in accordance with the applicable rules and provide good practices of data processing.

Following investigations, in January 2022 CNIL issued a decision, according to which the websites facebook.com, google.fr and youtube.com do not allow users to refuse the use of cookies as easily as they accept them. In this context, it imposed a fine of 60 million euros on Facebook and 150 million euros on Google (Lawspot, 2022), ordering them to comply within three months. The reason behind is that the websites facebook.com, google.fr and youtube.com provide only one button that allows the user to accept cookies immediately. However, they do not provide an equivalent solution, button or other,

which allows the user to easily refuse to install these cookies. It takes many clicks to reject all cookies, compared to just one to accept them.

Furthermore, it should be noted that in accordance with the Ordinance the right to erasure could be invoked for journalistic, artistic or academic purposes, contrary to what was provided for in former Article 67 of the Act. Article 51 of the Act expressly refers to Article 17 of the GDPR for the implementation of the right to erasure. Moreover, Article 52 of the Act provides that "for processing operations carried out by public administrations and private sector entrusted with a public service mission whose task is to check or recover taxes, requests of the exercise of the right of deletion must be addressed to CNIL in application of Article 118 of the Act, as well as for processing relating to State security and defence".

Last but not least, as far as the age limit for consent is ranged from 15 to 16 years old, according to Article 45 of the Act. However, when consent is needed for the agreement of an online contract with a minor, for instance, Directive 98/48/EC of the European Union is enforced, since ICT services are provided. If the one part of the agreement is below 15 years old, consent will need to be provided jointly by the minor and their parent or caregiver.

Parliamentary Report on Facial Recognition and Artificial Intelligence

According to the Parliamentary Office for Scientific and Technological Assessment, and mainly their Report published in July 2019 (Parliamentary Office for Scientific and Technological Assessment, 2019), facial recognition technology is being used more and more in public and private sector and as a result, social, legal and ethical issues are raised. For this reason, a strong and effective legislative framework is required.

The supportive role of CNIL is stressed out, since CNIL could encourage "privacy by design" in the deployment of facial recognition technology and in general of all new data- driven technologies, while advocate for the protection of human rights and freedoms (Commission Nationale de l'Informatique et des Libertés, 2019). Moreover, a group of multidisciplinary experts is recommended to be established, so that the replication of bias will be avoided.

Moreover, the responsibility of all the stakeholders involved, such as the developer, integrator and controller is highlighted. Last but not least, human verification for the most sensitive uses of such technologies, like legal proceedings, is flagged that is needed.

DPA Reaction

The Administrative Court of Justice (No. 1901249), after the French Data Protection Authority's, known as CNIL, Recommendations, ordered high schools in Nice and Marseille to end their facial-recognition programs. The CNIL found that the schools' deployment of the software was not in line with the GDPR's principles on proportionality and data minimisation. CNIL concluded that less intrusive measures than facial recognition technology could have been taken "in terms of privacy and individual freedoms".

The CNIL received a request from the Provence-Alpes-Côte d'Azur region (commonly known as PACA region) for advice on the experimentation of an authorisation access by facial recognition at the entrance to two high schools in the region- lycée les Eucalyptus in Nice and Ampère high school in Marseille. After a careful examination of the project, the CNIL considered that the proposed device is contrary to the main principles of proportionality and data minimisation set by the GDPR. Indeed, the objectives of securing and facilitating entry into these high schools can be achieved by means that are much less intrusive in terms of privacy and individual freedoms, such as, for example, badge control. The Commission recalled that the processing of biometric data is particularly sensitive, justifying enhanced protection of individuals. In particular, facial recognition devices are particularly intrusive and present major risks to the privacy and individual freedoms of the persons concerned.

Concluding Remarks on the French Case

Data minimisation is a principle that states, "data collected and processed should not be held or further used unless this is essential for reasons that were clearly stated in advance to support data privacy". In Article 5 (1) of the GDPR, this is defined as "data that is adequate, relevant and limited to what is necessary for the purposes for which they are processed". Article 25 of the GDPR provides that this approach shall be applied by default to "each specific purpose of the processing". In Article 5 (1) (b) of the GDPR the 'purpose limitation' principle is also included, which states that "the purpose for the processing of personal data that must be specified, explicit and legitimate", while the storage limitation principle set out in Article 5 (1) (e) which states that personal data should be kept "no longer than is necessary for the purposes for which it is processed".

Since GDPR does not define "what is adequate, relevant and limited to what is necessary in relation to the processing", in this case the school unit should have specified the purpose for collecting and using these sensitive personal data. This is crucial, given that personal and biometric data may also differ from one individual-student to another. As such, in order for the school unit to assess whether they are holding the right amount of personal data, they should have clarified

initially the reasons of processing. For the special category of biometric data, it is particularly important the school unit make sure they collect and retain only the minimum amount of information (Jasserand, 2016).

Finally yet importantly, the school unit should have periodically reviewed the processing to check that the personal data they hold was still relevant and adequate for entrance authorisation purposes and delete everything that was no longer needed as the storage limitation principle sets (Taylor, 2010).

Conclusion

Taking these two cases into consideration, it is important to flag as a general comment that the privacy risks derived from the deployment and use of surveillance technology are real (Krivokapić & Adamović, 2016). The controversial issue is that although there is a strong European legal framework, after the adoption of GDPR, technological companies do not comply with their legal obligations about privacy and data protection standard for a simple reason, because privacy is not profitable. Their business model is based on profit. In addition, the profit is gained through the power they have to control process and analyse users' data (Karagianni, 2018).

For instance, in the case of e-class and live streaming in Greece, there is much technical vulnerability on the side of service provider, Cisco Hellas A.E, according to researchers from IBM. More particularly, in their report they mentioned that "Webex video conferencing App can allow attackers to: i) join a Webex meeting as a ghost user, invisible to others on the participant list, but with full access to audio, video, chats, and screen sharing, ii) remain in a Webex meeting as a ghost audio user even after being expelled from it, and iii) obtain information on meeting participants, such as full names, email addresses, and IP addresses". This information could also be obtained from the meeting room lobby, even before the attacker was admitted to a call. It is problematic why such risks have not been taken into account from the Greek Data Protection Authority, as potential risks, or the one who conducted the DPIA study did not remark them.

As far as the particular cases are concerned, it is very hopeful that the Data Protection Authorities have taken very seriously their role as observer and "guardians" of privacy and data protection by imposing fines to the persons responsible of GDPR violations. Last but not least, children's vulnerability is remarkable in surveillance systems and is more than ever crucial the legislators and governments take the necessary measures to provide for them a special regime of protection, respecting their age, childhood and vulnerability (European Data Protection Supervisor, 2019). The Greek DPA in the relevant case has also highlighted the special regime of children's data protection.

More than that, the French case concerned the use of facial recognition systems for entrance authorisation purposes. Nonetheless, the French DPA paid more attention on different grounds, the first one on the consent as a legal ground and the second one on data minimisation principle. Not accepting the consent as a legal ground for the processing means that the processing of personal data is not legal at all. However, the enforcement of data minimisation principle means that data processing is limited to what is necessary in relation to the purposes for which it is processed and there will be a breach only for the processing of "unnecessary" data.

To conclude, concerning the Greek case, the DPA mentioned that the school units or the Ministry of Education is not responsible to determine what could be a "menace" for the safety and security of students and school premises. Moreover, along the same lines the DPA stated that CCTV cameras is not allowed to record during the "opening hours" of the school, avoiding in this way the processing of "unnecessary" personal data.

GDPR gives motivations to the tech companies to create business models that are privacy friendly. However, tech industry and information service providers have paid little attention to privacy and data protection issues, especially when it comes to kids-users. Thus, it is important the protection of the rights of the child to be included and seriously taken into consideration in the arena of private autonomy, innovation and security (International Telecommunications Union, 2020).

As the United Nations Children's Fund highlights (Carter et al., 2020), "although the digital risks in the current COVID-19 environment are not wholly new, they are unprecedented in terms of speed, scale and invasiveness. There are more and varied players making decisions about how data, including children's data, are used and how related risks are assessed and handled. This means that we need to engage with a broader set of government and industry partners to ensure that children's rights are not overlooked".

Given that the end of the COVID-19 pandemic has not yet announced, further research should be made regarding the impact it has on the enjoyment of children's rights in the digital educational environments. Online distance learning tools have been highly used in all the European Member States, and globally. As such, it is of great importance this impact to be measured. Last but not least, since cameras are being used in children's daily life, not only in the context of online distance learning, but also in the context of security and safety in school premises, further recommendations in the relevant legislation should be made regarding the processing and analysis of selected data by the European Member States in national and European level.

Authorship Contribution Statement

Karagianni: Conceptualisation, design, analysis, writing. Papakonstantinou: Editing/reviewing, supervision.

References

Act no. 3463/2006, Ratification of the code of municipalities and communities § A'114 (2006). https://bit.ly/3KxEL3C [In Greek]

Act no. 4610/2019, Synergies of universities and TEI- access to higher education §70 8 (2019). https://bit.ly/3jvgYpi [In Greek]

Act no. 4624/2019, Legislation on personal data protection §Act 2019 § A'137 (2019). https://bit.ly/3KCYH5o [In Greek]

Carter, K., Berman, G., Garcia Herranz, M., & Sekara, V. (2020). *Digital contact tracing and surveillance during COVID-19: General and cChild-specific eEthical iIssues* (*Innocenti Working Papers, No.2020/01).* UN-iLibrary. https://doi.org/10.18356/1483e560-en

Commission Nationale de l'Informatique et des Libertés. (2019). *Facial recognition: for a debate living up to the challenges*. CNIL. https://bit.ly/3j0NHT7

Commission Nationale de l'Informatique et des Libertés. (2020). *Cookies and other tracking devices: The CNIL publishes new guidelines*. CNIL. https://www.cnil.fr/fr/node/114257

Constitution of the Hellenic Republic. (2008). *VIIIth Revisionary Parliament, Chapter II*

Digital Freedom Fund. (2020). *What is "Biosurveillance"? The COVID-19 measures getting under our skin*. Medium. https://bit.ly/38c2IiE

Directorate-General for Infrastructure. (2016). *Video-surveillance policy*. Court of Justice of the European Union. https://bit.ly/3K5mdrd

European Data Protection Board. (2019). *Guidelines 3/2019 on processing of personal data through video devices*. European Publications Office. https://bit.ly/3IVuWeg

European Data Protection Supervisor. (2010). *The EDPS video-surveillance guidelines.* European Publications Office. https://bit.ly/3NSFNJM

European Data Protection Supervisor. (2019). *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*. European Publications Office. https://bit.ly/3uNEmnc

European Parliament, Council of the European Union. (2016a, April 27). *Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data*. EUR-Lex.Europa.Eu. https://bit.ly/3tWLgqR

European Parliament, Council of the European Union. (2016b, April 27). *Regulation (EU) 2016/679 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).* EUR-Lex.Europa.Eu. https://bit.ly/3iYTlVS

Greek Data Protection Authority. (2019). *Απόφαση Αρ. 21/2019* [*Decision No. 21/2019*]. Data Protection Authority Publishing Service. https://bit.ly/3iUPGIw

Greek Data Protection Authority. (2021). *Απόφαση Αρ. 50/16.11.2021* [*Decision No. 50/16.11.2021*]. Data Protection Authority Publishing Service. https://bit.ly/3jfdwix

Hellenic Republic- Ministry of Education and Religions. (2020a). *Διοικητική Εγκύκλιος 121802/ΓΔ4/15-09-2020 του Υπουργείου Παιδείας* [*Administrative Circular 121802/ΓΔ4/15-09-2020 of the Ministry of Education*]. https://bit.ly/38assvN

Hellenic Republic- Ministry of Education and Religions. (2020b). *664.841 μαθητές και 166.949 εκπαιδευτικοί έχουν εγγραφεί στο Πανελλήνιο Σχολικό Δίκτυο* [*664,841 students and 166,949 teachers have registered in the Panhellenic School Network*]. https://bit.ly/38asrIf

Hellenic Republic- Ministry of Education and Religions. (2020c). *Joint Ministerial Decision No. Δ1α/ΓΠ.οικ. 72989*. Sheet Number 5043. FEK. https://bit.ly/3K2pLL3

Hellenic Republic- Ministry of Education and Religions. (2021). *Απόφαση No. 111525/ΓΔ4 Παροχή σύγχρονης εξ αποστάσεως εκπαίδευσης για το σχολικό έτος 2021-2022* [*Decision No. 111525/ΓΔ4 Provision of modern distance education for the school year 2021-2022].* https://bit.ly/3JXN9cq

International Telecommunications Union. (2020). *Guidelines for industry on child online protection.* ITU. https://bit.ly/3IZcBgn

Jasserand, C. (2016). Legal nature of biometric data: From 'Generic' personal data to sensitive data. *European Data Protection Law Review*, *2*(3), 297-311. https://doi.org/10.21552/edpl/2016/3/6

Karagianni, A. (2018). *UN and the rights of the child in the digital environment: data protection and privacy* [Master's thesis, Aristotle University of Thessaloniki]. Aristotle University of Thessaloniki Archive. https://bit.ly/3uRuEQH

Kaskamanidis, G. (2020). *Η τηλεκπαίδευση δεν είναι παίξε γέλασε* [*Distance learning is not a joke*] https://bit.ly/3K5ZZ8s

Katsikas, C. (2020). *Αποχή καθηγητών για παραβίαση ατομικών δικαιωμάτων από αναρτήσεις φωτογραφιών και βίντεο* [Abstention of teachers for violation of individual rights by posting photos and videos]. *Efimerida ton Syntakton.* https://www.efsyn.gr/node/268523

Krivokapić, D., & Adamović, J. (2016). Impact of General Data Protection Regulation on children's rights in digital environment. *Anali Pravnog fakulteta u Beogradu*, *64*(3), 205-220. https://doi.org/10.5937/analipfb1603205k

La Quadrature du Net. (2020). *First Success Against Facial Recognition in France*. https://bit.ly/3qXrM3n

Lawspot. (2022). *Cookies: Πρόστιμο 210 εκατομμυρίων ευρώ σε Google και Facebook από την Αρχή Προστασίας Δεδομένων της Γαλλίας* [Cookies: € 210 million fine on Google and Facebook by the French Data Protection Authority]. https://bit.ly/3uLWait

Legifrance. (2019). *Décret no. 2019-536 pour l'application de la loi no. 78-17 relative à l'informatique, aux fichiers et aux libertés (2019)* [Decree no. 2019-536 taken for the application of the Act no. 78-17 relating to data processing, files and freedoms.]. https://bit.ly/3qYSVTP

Loi no. 2004-801, Protection des personnes physiques à l'égard des traitements de données à caractère personnel [Act no. 2004-801 relating to the protection of individuals with regard to the processing of personal data] § JORFTEXT000000441676 (2004). https://bit.ly/3DzMLhK

Loi no. 78-17, A l' informatique, aux fichiers et aux libertés [Act no. 78-17 relating to data processing, files and freedoms] § JORFTEXT000000886460 (1978). https://bit.ly/35AB6mw

O' Murchu, C. (2021). Facial recognition cameras arrive in UK school canteens. *Financial Times*. https://on.ft.com/3uJwVNI

Parliamentary Office for Scientific and Technological Assessment. (2019). *Briefing 14 about Facial Recognition.* Science and Technology Briefings. https://bit.ly/37NYn4W

République Française. (2018). *Ordonnance no. 2018-1125 [Ordinance no. 2018-1125]* https://bit.ly/3Dy0aqO

Smith, P. K. (2004). Violence in Schools: A European Perspective. *Programme on Educational Building- Organisation for Economic Co-operation and Development*, 137-145. https://doi.org/10.4324/9780203006429

Taylor, E. (2010). From finger-painting to fingerprinting: The use of biometric technology in UK schools. *Education Law Journal, Vol.1(4), pp.276-288.* https://bit.ly/36KCPq2

The Administrative Tribunal of Marseille. (2020, February 27). *TA Marseille - N°1901249*. GDPRhub. https://bit.ly/3iXnsgh

United Nations Children's Fund. (2018). *Children's online privacy and freedom of expression*. https://bit.ly/3J0gK3J

World Health Organisation. (2020, January 30). *WHO Director-General's statement on IHR Emergency Committee on Novel Coronavirus (2019-nCoV)*. https://bit.ly/3uJx182

Zou, C., Zhao, W., & Siau, K. (2020). COVID-19 pandemic: A usability study on platforms to support eLearning. In C. Zou, W., Zhao, & K., Siau (Eds.), *International Conference on Human-Computer Interaction 2020. Communications in Computer and Information Science* (pp.333-340). Springer. https://doi.org/10.1007/978-3-030-60703-6_43