ПРЕГЛЕДНИ НАУЧНИ РАД
10.5937/zrpfn0-48197

Carmen Oana Mihăilă, LL.D.,
Associate Professor,
Faculty of Law, University of Oradea, Republic of Romania
***Mircea Mihăilă, PhD** (Comp.Sc.),*
University Lecturer,
Faculty of Electrical Engineering and Information Technology,
University of Oradea, Republic of Romania

UDK: 621.397.4:004.8:[347.77:342.738

Рад примљен: 12.12.2023.
Рад прихваћен: 15.12.2023.

VIDEO SURVEILLANCE AND ARTIFICIAL INTELLIGENCE: HOW DOES IT AFFECT PRIVACY AND INTELLECTUAL PROPERTY RIGHTS?

Abstract: *The protection of individual privacy is increasingly questioned in the context of today's high-tech video surveillance by using superior technologies, such as Artificial Intelligence (smart cameras and video surveillance systems, biometrics and facial recognition) which is capable of analyzing a huge amount of data, identifying links between that data and de-anonymizing them. Technology is synonymous with evolution. Yet, the advantages of using new technology are combined with great risks. The use of video cameras for surveillance raises important privacy issues. Biometric remote identification can only be performed under certain safeguards, in the context of a justified interest and with respect for the principle of proportionality. In recent years, facial recognition technology has become increasingly widespread, and highly controversial, as it is omnipresent (at airport check-in lines, police departments, pharmacies, etc.). While it may add a sense of security and comfort for businesses implementing it, such technology has been widely criticized by privacy advocates, especially for its built-in racial bias and potential for abusive use. "Real-time" biometric identification of individuals in public-accessible spaces for law enforcement purposes is seen as highly intrusive on the rights and freedoms of the individuals concerned, but it also evokes a sense of constant surveillance and indirectly discourages the exercise of freedom of assembly and other fundamental rights. Another important issue is the use of video surveillance in a context where it can cause problems in terms of intellectual property.*

* mejl
* mejl

The unauthorized use of recordings may affect confidential business operations. Trade secrets and confidential information are often an essential part of a company's intellectual property portfolio. Thus, companies have to take extra steps to ensure that images captured by cameras are stored securely and accessible only to authorized personnel. Cameras can capture images of artistic works, performances, exhibitions, and uncontrolled access can lead to infringement of copyright and related rights. As captured videos can be uploaded to platforms, such use of intellectual property can lead to copyright infringement, especially when the video entails the use of copyrighted material without the owner's permission, which constitutes an infringement of intellectual property rights.

Keywords: *video surveillance, facial recognition technology, Artificial Intelligence, intellectual property, General Data Protection Regulation (GDPR).*

1. Introduction

The aim of the EU is *"to create a single European data space [...] where both personal and non-personal data, including sensitive commercial data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data [...]"* (EC, 2020a: 4)[1]. In this objective, we may observe multiple advantages but we cannot ignore the possible risks. In the context of today's very efficient high-tech video surveillance by using superior technologies, the protection of the private life of an individual is increasingly called into question. Technology is synonymous with evolution. Yet, when it comes to using new technologies, such as Artificial Intelligence (smart cameras and video surveillance systems, biometrics and facial recognition), the advantages may come together with great risks.

Digital technologies are essentially a tool of social control, with individuals becoming increasingly transparent (De Gregorio, 2022: 217). Given the fact that **personal data** and sensitive information can be captured through video surveillance, the systems must comply with the regulations imposed by the General Data Protection Regulation (GDPR)[2]. Artificial Intelligence (AI) can analyze a

1 European Commission/EC (2020a). *A European strategy for data*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2020)66, Brussels, 19.02.2020; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066

2 The General Data Protection Regulation (2016): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), JO L 119, 4.5.2016; https://gdpr-info.eu/

huge volume of data, identify the links between these data, de-anonymize them, and thus create great risks. The use of video cameras for surveillance raises important privacy issues. When using AI technologies, the way data subjects express their free and informed consent is clearly questionable, given that the data controller cannot transparently explain the purpose of the data processing and the data subject does not know what risks he/she is exposed to (Paal, 2022: 297)[3]. In case of absence of consent, the right to be informed to consent to data processing and to have access to the stored data are almost non-existent. In this context, the limitation of these rights must be well justified, whereas the obligation of the responsible operator to implement adequate technical and organizational measures to comply with data protection is essential.[4]

Another important aspect of video surveillance is related to interference with **intellectual property**. In the modern era, video monitoring (video-conferencing, social media, etc.) is present in homes, businesses, public institutions or public places as an important tool in daily life. Yet, there is an increased concern about the abusive use of video recordings for purposes such as invading a person's privacy or spying on employees. Another problem that can affect video monitoring systems is **computer piracy.** To address all these issues, additional security measures are needed to ensure encryption, passwords, and controlled access.

Unauthorized use of these recordings may affect confidential business operations (plans, prototypes). Trade secrets and confidential information are often an essential part of a company's intellectual property portfolio. That is why companies find themselves in a position to take extra measures to ensure that the images captured by the cameras are stored securely and accessible only to authorized personnel. Cameras may capture images of artworks, performances, exhibitions, and uncontrolled access may result in infringement of copyright and copyright-related rights. Captured videos can be uploaded to platforms, and this use of intellectual property can lead to copyright infringement, especially when the video uses copyrighted material without permission. Using video record-

3 The processing of personal data is lawful only if the data subject has given consent, which means that the person must give consent for one or more specific purposes. In this context, there is probably no way for the controller to know or predict for which purposes personal data will be processed by autonomous and self-learning artificial intelligence systems (Paal, 2022: 297).

4 Art. 25 para. (2) of GDPR (2016): "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons".

ings without the owner's permission may constitute a violation of intellectual property rights. Regarding the ownership of video recordings, in principle, the one who makes the recording is the owner of copyright on it. Yet, if a person is hired to make the video, the employer may own the copyright. Moreover, if the video recording captures images of other people, their right to privacy must be taken into account.

As early as 2005, when the Article 19 Data Protection Working Party (WP)[5] drafted a document on the applicability of data protection in the field of intellectual property, attention was drawn to the relationship between the two branches and the need to implement measures to protect the rights and legitimate interests of intellectual property rights holders against alleged fraud. The document addresses the digital rights management (DRM), including the legitimate use of technologies for the purpose of protecting works (e.g. DRM may provide for identifying persons accessing legally protected information: songs, software, etc.), but also the possibilities available to copyright holders to enforce their rights against individuals suspected of copyright violation. On the other hand, the document addresses the DRM, which could be detrimental to the processing of personal data of natural person. In applying data protection principles to digital rights management, there is a growing gap between the protection of individuals in the offline and online worlds, especially given the widespread tracking and profiling of natural persons (WP, 2005: 3).

The EU Directive no. 2019/790 on Copyright and related rights in the Digital Single Market[6] states that "any processing of personal data under this Directive should be carried out with respect for fundamental rights, including the right to respect for private and family life and the right to protection of personal data set out in Articles 7 and 8 (respectively) of the Charter, and must be in compliance with Directive no. 2002/58/EC and Regulation (EU) no. 2016/679" (Preamble § 85). Art. 28 of the Directive even has the marginal title "Protection of personal data". Specialists in the field of data protection appreciate that this Directive offers a new framework, adapted to technical developments on the personal data protection (Şandru, 2019: 21-31).

5 Article 29 Data Protection Working Party/WP (2005). Working document on data protection issues related to intellectual property rights, WP 104, 18 January 2005 (the Working Party set up under Article 29 of Directive 95/46/EC, Directorate E (Services, Copyright, Industrial Property and Data Protection) of the European Commission, Internal Market Directorate-General, Brussels, 2005; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp104_en.pdf

6 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, **Official Journal of the EU, L** 130, 17.5.2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790

In Romania, surveillance systems can be installed in open spaces (streets, national roads), provided that they are mounted in visible places, and it is forbidden to hide them. Article 6 § 1c) of the GDPR stipulates that the processing is necessary in order to fulfil a legal obligation incumbent on the operator. In this context, Article 2 of Romanian Law 333/2003 on the protection of objectives, goods, values and persons[7] provides that "ministries and other specialized bodies of central and local public administration, autonomous administration, national companies and societies, national institutes of research and development, companies regulated by Law no. 31/1990, republished, with subsequent amendments and additions, regardless of the nature of the social capital, as well as other organizations that hold assets or values of any title, referred to in this law as units, are obliged to ensure their protection" (Article 2 § 1 of Law 333/2003).

According to Romanian legislation, there are several types of operators that have the legal obligation to install CCTV, including *inter alia* loan institutions in the category of banks, companies specialized in currency exchange, units profiled for activities with jewellery made of metals or precious stones, arms and ammunition stores, pawnshops, fuel stations, gambling halls and premises, institutions of public interest (Article 68 of Methodological norms of 11 April 2012 for the implementation of Law no. 333/2003 on the protection of objectives, goods, values and persons).

Under Law no. 190/2018 on measures to implement Regulation (EU) 2016/679[8] on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, commercial companies have the right to install video surveillance cameras, but only if they can prove that other methods were ineffective and did not allow the proper functioning of the business. According to Decision no. 301/2012[9] on the approval of the Methodological Norms for the application of Law no. 333/2003, which refers to the security of goods and people, commercial companies that have surveillance cameras are obliged to display warning signs regarding their presence. If the video images

7 Romanian Law 333/2003 on the protection of objectives, goods, values and persons, with subsequent additions and amendments, *Official Gazette of Romania*, no.189/18 March 2014; https://legislatie.just.ro/Public/DetaliiDocument/156432

8 The Romanian Law no.190/2018 on measures to implement Regulation (EU)2016/679 of the E. 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 repeal of Directive 95/46/CE (GDPR), *Official Gazette* no. 651/2018; https://legislatie.just.ro/Public/DetaliiDocument/203151

9 Government Decision no. 301 of 11 April 2012 on the approval of the Methodological Norms for the application of Law no. 333/2003, *Official Gazette* no. 335/17 May 2012, https://legislatie.just.ro/Public/DetaliiDocument/138059

are used for the purpose of processing sensitive data such as biometric data, the operator shall apply Article 6 (lawfulness of processing) and Article 9 (processing of special categories of personal data) of the GDPR.

In Law no. 363/2018 on the protection of natural persons regarding the processing of personal data by the competent authorities for the purpose of prevention, discovery, investigation, prosecution and combating of crimes or the execution of punishments, educational and safety measures, as well as regarding the free circulation of these data[10], the processing of biometric data is prohibited, with some exceptions: a) if the processing is expressly provided by the law; b) if it is necessary to prevent an imminent danger at least to life, bodily integrity or health of the person concerned or of another natural person; or c) if it refers to personal data that is openly made public by the data subject, with the adoption of appropriate measures to protect the rights, freedoms and legitimate interests of the data subject (Articles 10 and 11 of Law no. 363/2018).

According to Decision no. 174 of 18 October 2018[11], operators are obliged to carry out an impact assessment on the protection of personal data. Thus, the **Data Protection Impact Assessment** (**DPIA)** is mandatory, particularly in case of "[...] e) large-scale processing of personal data through innovative use or the implementation of new technologies, especially if the respective operations limit the ability of data subjects to exercise their rights, such as the use of facial recognition techniques to facilitate access to different spaces" (Article 1 of Decision no. 174 of 18 October 2018). Although the use of these technologies can be perceived as effective, the EDPB Guidelines 3/2019 on processing personal data through video devices (§73)[12] note that operators must first assess the impact on fundamental rights and freedoms and consider less invasive means to achieve the legitimate aim of processing (EDPB, 2020:19).

The use of biometric data and in particular facial recognition entail heightened risks for data subjects' rights. It is crucial that recourse to such technologies

10 The Romanian Law no. 363/2018 on the protection of natural persons regarding the processing of personal data by the competent authorities for the purpose of prevention, discovery, investigation, prosecution and combating of crimes or the execution of punishments, educational and safety measures, as well as regarding the free circulation of these data, *Official Gazette* no. 13/7 January 2019, https://legislatie.just.ro/Public/DetaliiDocument/209627

11 Decision no. 174 of 18 October 2018 on the list of operations for which a personal data protection impact assessment is obligatory, National Supervisory Authority for the Processing of Personal Data, *Official Gazette* no. 918/31 October 2018, https://legislatie.just.ro/Public/DetaliiDocument/206331

12 European Data Protection Board/EDPB (2020). Guidelines 3/2019 on processing of personal data through video devices, 29 Jan. 2020; https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices.pdf

takes place with due respect to the principles of lawfulness, necessity, proportionality and data minimisation as set forth in the GDPR. Whereas the use of these technologies can be perceived as particularly effective, controllers should first of all assess the impact on fundamental rights and freedoms and consider less intrusive means to achieve their legitimate purpose of the processing.

2. Video surveillance: Benefits greater than risks?

Facial recognition has evolved from face detection to the implementation of sophisticated methods: face segmentation, shape or texture description (Onufreiciuc, 2020: 95-103). In the early days of facial recognition technology (in 1990s), university researchers photographed volunteers to develop their algorithms. Later, they accessed cameras from campuses or cafes, or even photos posted online. In 2014, *Yahoo* announced "the largest public multimedia collection ever published" (a dataset of 100 million photos and videos) (Thome, Shamma, Friedland, Elizalde, Ni, Poland, Borth, Li (2016: 3).[13] However, users were not notified that their photos and videos were included in the dataset (although the photos were not shared directly but as links via American hosting service for images and video). In 2015, over four million Flickr photos were used in creating a database called Megaface to help test and refine facial recognition algorithms (*New York Times:* Hill, Krolik, 2019).[14]

Video surveillance, i.e. "systematic automated monitoring of a specific space by optical or audio-video means" (EDPB, 2020:5), is considered to be in accordance with the law only if there is a **legitimate interest of the operator/controller or a third party**, unless the interests or rights and freedoms fundamental rights of the data subject prevail over these interests.[15] The legitimate interest must not be fictitious or speculative but must be real and up to date (WP, 2014:24).[16] The GDPR stipulates that the processing and collection of personal data shall be legal,

13 Thome, B., Shamma D.A, Friedland G., Elizalde B., Ni K., Poland D., Borth D., Li L-J. (2016). YFCC100M: The New Data in Multimedia Research, *Communications of the ACM*, vol. 59|no.2|Feb. 2016; Retrieved 22 March 2023 from https://dl.acm.org/doi/pdf/10.1145/2812802; https://arxiv.org/pdf/1503.01817v2.pdf

14 *The New York Times*: Hill, K., Krolik, A. (2019). How Photos of Your Kids Are Powering Surveillance Technology, The New York Times, https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html

15 Article 6 §1f) of GDPR: "Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child […]".

16 Article 29 Data Protection Working Party (2014): Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 9 April 2014; https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp217_en.pdf

transparent and fair, and that the data shall be collected for a specific purpose, so that individuals have the right to access and control their data (Preamble § 39 GDPR). Therefore, individuals must be informed about the presence of the cameras and their purpose. If they are smart cameras, which are not visible, the persons concerned must be informed in detail about the monitored places (EDPB, 2020:28). Thus, there should be warning signs, a link to a website detailing surveillance information, a phone number, or a map of the application.[17]

The provisions of Article 5 (§ 1) of the GDPR contain obligations regarding the legality, fairness and transparency of data processing, compliance with and compatibility with determined, explicit and legitimate purposes, the principle of data minimization, accuracy, limitation of storage, integrity and confidentiality of data. In this context, a data protection impact assessment procedure (DPIA procedure) is necessary because, according to Article 35 (§ 1) and recitals 89 and 91 of the GDPR, the use of a new technology "in accordance with the achieved level of technological knowledge" may trigger the need to carry out a DPIA procedure.

Article 22 of the GDPR also stipulates in that "the data subject has the right not to be subject to a decision based exclusively on automatic processing, including profiling, which produces legal effects concerning the data subject or similarly affects him to a significant extent". Therefore, a natural person cannot be transformed into a simple object of computer-assisted programs (Paal, 2022: 293). It remains to be seen how the complex processes involved in AI can be explained.

Data collected by video cameras must be stored securely and deleted when no longer needed. Individuals have the right to access their data, and video recordings cannot be used without consent for purposes other than those originally intended. The EC Communication *A European Data Strategy* (EC, 2020a:20) states that individuals "can be empowered to be in control of their data through tools and means that allow them to decide at a granular level" how their data can be used ("personal data spaces").[18] Under Article 13(§ 2 f) GDPR, in order to ensure fair and transparent data processing, controllers must provide data subjects

17 Similarly, when individuals interact with an AI system, or when their emotions or characteristics are recognised by automated means, individuals must be made aware of these circumstances, unless AI is used by law to detect, prevent, investigate and prosecute criminal offences.(Title IV(Art. 52)-Transparency obligations for certain AI systems, EP/EC Proposal for Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (*Artificial Intelligence Act*) and amending certain Union legislative acts, COM(2021)/0106(COD)/206; Brussels, 21.4.2021).

18 "This could be supported by strengthening individuals' right to data portability under Article 20 of the GDPR, giving them more control over who can access and use automatically generated data, for example through stricter interface requirements for real-time data access

with further information about the presence of automated decision-making.[19] The strategy also envisages effective access to justice, liability of operators, and compensation for sustained damage or harm (EC, 2020b: 22).[20]

In the European Union, the use of **facial recognition technology** is governed by rules on data protection, privacy, fundamental rights and non-discrimination. *Facial recognition* is "the automatic processing of digital images containing the faces of individuals for the purpose of identifying, authenticating/verifying or classifying those individuals" (WP, 2012a: 2).[21] Facial recognition technologies are biometric technologies, starting from the simple detection of the presence of a face in an image to the verification, identification and classification or more complex classification of people (Buolamwini, Ordóñez, Morgenstern, Learned-Mill, 2020: 2-6). To be used in a face recognition system, a face must be photographed by a camera or photo camera, or recorded by a video camera (Buolamwini *et al.,* 2020: 9). Although facial recognition algorithms have advanced a lot in recent years, facial recognition systems can generate errors (at least at the current level, algorithms are prone to errors, especially in difficult environments such as poor lighting or crowded spaces); thus, they generate high risks and affect fundamental rights.

The collection and analysis of biometric data by facial recognition software, for the purpose of identifying a person, may represent an interference with the rights to privacy and data protection, as envisaged in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU)[22]. Article 7 CFREU stipulates that "every person has the right to respect for private and family life, home and the secrecy of communications". Article 8 (§1) of the CFREU and Article 16 §1) of the Treaty on the Functioning of the European Union (TFEU) regulate every person's right to the protection of personal data concerning him/

and by introducing mandatory machine-readable formats for data from certain products and services, e.g. data from smart home appliances or smart wearable devices"(EC, 2020a:20).

19 Article 13 §2(f) of the GDPR envisages that such information should include "the existence of automated decision-making, including profiling, referred to in Art. 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."

20 European Commission/EC (2020b). *White paper on Artificial Intelligence: European approach to excellence and trust,* 19.2.2020, COM(2020)65, https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf

21 Article 29 Data Protection Working Party (2012a). *"Opinion 02/2012 on facial recognition in online and mobile services"*, 00727/12/EN, WP 192, Brussels, 22 March 2012 (2), Retrieved 1 March 2023 from https://www.pdpjournals.com/docs/87998.pdf.

22 The Charter of Fundamental Rights of the European Union (CFREU), Official Journal of the European Communities C 2000/C 364/01); https://www.europarl.europa.eu/charter/pdf/text_en.pdf

her. Similarly, Article 8 of the European Convention on Human Rights (ECHR) ensures the right to respect for private and family life.[23] As shown in the GDPR, "the processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity" (Preamble § 4 GDPR).[24]

This right must be balanced with other fundamental rights, according to the principle of proportionality. Article 52 of the CFREU also requires that "any restriction of the exercise of the rights and freedoms recognized by this charter must be provided by law and observe the substance of these rights and freedoms. By observing the principle of proportionality, restrictions may be imposed only if they are necessary and only if they effectively respond to the objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others". The jurisprudence on these issues may be illustrated by some cases of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU).[25]

23 In *Gaughran v. the United Kingdom (Appl. no 45245/15, Judgment 13.02.2020), t*he ECtHR has ruled that the implementation of facial recognition tools, using photographs captured during a person's arrest and subsequently stored in a police database interferes with the right to respect for private life under Article 8 ECHR. The Court pointed out that keeping photographs of an arrested person for an indefinite period is a violation of the same right. (ECtHR case: *Gaughran v. the United Kingdom, Appl.no 45245/15, Judgment 13.02.2020, Strasbourg,* https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-12731%22]}; accessed on 5 March 2023

24 *See:* CJEU case: Volker und Markus Schecke GbR and Hartmut Eifert Joined cases C-92/09 and C-93/09, Judgment of the Court (Grand Chamber) of 9 November 2010, para. 48.

25 Under Article 8, personal data protection plays a fundamental role in an individual's exercise of the right to respect for private and family life. Domestic law must provide adequate guarantees to prevent any use of personal data that might be incompatible with the Article 8 guarantees (ECtHR case: *S. and Marper v. the United Kingdom*, Appl. no 30562/04, Strasbourg, Dec. 2008, para. 103).
In *Digital Rights Ireland*, the CJEU has invalidated Directive 2006/24 (of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2006 O.J. (L 105) 54), which is no longer in force, on the grounds that it infringes fundamental rights to privacy and data protection. The Directive obliged telecom and Internet service

Article 8 (§2) of the ECHR specifies the conditions in which there may be an interference with the exercise of the protected right. In order to be justified, the interference must be "in accordance with law", must pursue a "legitimate aim", and must be "necessary in a democratic society". Any interference must be justified by a legitimate aim, and the reasons justifying the interference must be relevant and sufficient.[26] As previously shown, when the fundamental right to private life interferes with the right to protection of personal data, the analysis of the balance of proportionality must be done,[27] and it is important that the fundamental rights are not called into question (Brkan, 219: 864-883).

The Protocol (no.223/2018) amending the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (108/1981)[28] emphasizes that the purpose of the Convention is to protect every person, regardless of his/her nationality or residence, with regard to the processing of personal data, thus contributing to respect for fundamental human rights and freedoms and, in particular, the right to private life/privacy (Article 2 of Protocol 2018).[29]

providers to retain data on their users: name, address, date, time, duration and type of communication, as well as the IP addresses of Iinternet service users. (CJEU case: *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, joined Cases C-293/12 and C-594/12, Judgment of the Court (Grand Chamber), 8 April 2014).

In the case *Maximillian Schrems v Data Protection Commissioner*, the CJEU ruled that mass surveillance measures compromise the essence of the fundamental right to privacy, stating that "regulation which allows public authorities to access the content of electronic communications on a general basis must be regarded as undermining the substance of the fundamental right to respect for private life as guaranteed by Article 7 of the Charter" (CJEU case: *Maximillian Schrems v Data Protection Commissioner*, Request for a preliminary ruling from the High Court (Ireland), C-362/14, Judgment of the Court (Grand Chamber) of 6 October 2015, para. 94).

26 Council of Europe/European Court of Human Rights (2022). *Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence*, 31 August 2022, Retrieved 7 March 2023 from https://www.echr.coe.int/documents/guide_art_8_eng.pdf

27 As the CJEU has already stated: "two separate rights are here invoked: a classic right (protection of privacy under Article 8 ECHR) and a more modern right (the data protection provisions of Convention No 108). Similar rights are identified respectively in Articles 7 and 8 of the Charter. The Court has recognised the close link between the fundamental rights to privacy and the right to data protection" (CJEU case: *Volker und Markus Schecke and Eifert GbR and Hartmut Eifert*, joined cases C-92/09 and C-93/09, Opinion of Advocate General Sharpston, 17 June 2010, para. 71).

28 Council of Europe/CoE (2018). Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (108/1981), Council of Europe, CETS No. 223, Strasbourg, 10.X.2018; https://rm.coe.int/16808ac918

29 In Romania, the 2018 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was ratified by Law no. 290/2021,

The European Court of Human Rights has shown that "the rapid development of increasingly sophisticated techniques that allow, among other things, facial recognition and facial mapping techniques to be applied to people, to photos of people, makes their photography, as well as the storage and the possible diffusion of the resulting data, problematic" (ECtHR, 2020: 86).[30]

In the case *Antović and Mirković v. Montenegro,*[31] the ECtHR considered that there had been a violation of Article 8 of the Convention, finding that the camera surveillance did not comply with the law. The application was filed by two professors at the School of Medicine, who said that the surveillance was illegal and that they had no effective control over the collected information. The domestic courts rejected a claim for damages, finding that privacy was not at issue because the halls where the applicants taught were public spaces. Noting that private life can include professional activities, the ECtHR held that the surveillance by cameras constituted an interference with the applicants' right to private life. In another case, *Bărbulescu v. Romania*[32], the ECtHR held that there was a violation of Article 8 of the Convention, finding that the Romanian authorities did not adequately protect the plaintiff's right to respect for his private life and correspondence. The plaintiff complained that his employer's decision to fire him after monitoring his electronic communications and accessing their contents was based on a violation of his privacy rights. He had not been informed of the nature or extent of the monitoring, nor of the degree of intrusion into his private life and correspondence. In the case *Peck v. the United Kingdom,*[33] a footage filmed in a street where the plaintiff was cutting his veins was released. The images were filmed using a closed-circuit television camera (CCTV) installed by the local council and have been posted in several articles about the positive impact of CCTV cameras and subsequently on TV shows about crime in the UK. The Court established that Article 8 of the Convention was violated because the disclosure of the records by the city council was not accompanied by sufficient safeguards and constituted a disproportionate and unjustified interference in

Official Gazette of Romania, no.1171,10 December 2021.

30 ECtHR (2020). "*Guide to the Case-Law of the of the European Court of Human Rights, Data protection"*, 31 August 2022, 86; https://www.echr.coe.int/documents/d/echr/Guide_Data_protection_ENG

31 ECtHR case: *Antović and Mirković v. Montenegro*, Application no 70838/13 Judgment 28 November 2017. (See: ECtHR Factsheet: *Personal data protection*, December 2022, p.14; https://www.echr.coe.int/documents/d/echr/fs_data_eng).

32 ECtHR case: *Bărbulescu v. Romania* Application no 61496/08, Judgment 5 September 2017. (ECtHR Factsheet, 2022: 12)

33 ECtHR case: *Peck v. the United Kingdom,* Application no 44647/98, Judgment 28 January 2003; https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-687182-694690%22]}

the applicant's private life. The Council did not seek the plaintiff's consent when it released these photographs.

In 2020, the Human Rights Council (HRC) adopted Resolution A/HRC/44/L.11 on "The Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, including the Right to Development"(2020),[34] through which the HRC condemned the use of facial recognition technology alongside other digital tracking tools. In 2021, the HRC adopted Resolution 47/23 on "New and Emerging Digital Technologies and Human Rights"(2021),[35] which obliged the High Commissioner to convene an expert consultation on "the relationship between human rights and technical standard-setting processes for new and emerging digital technologies" (OHCHR, 2023).[36] Among the proposed issues was the influence of technical standards for new and emerging digital technologies, related risks and opportunities or common obstacles to the effective integration of human rights considerations into technical standard-setting processes for new and emerging digital technologies. As experts point out, the protection of private life and access to personal data are "two complementary notions that have evolved as inclusion and understanding, which were permanently under the impact of technological innovation and easier access to information, especially the information transmitted in electronic format" (Manescu, 2020: 102-114).

3. Artificial Intelligence (AI) and real-time surveillance

Elaborating on the AI Strategy for Europe (EC, 2018a),[37] the European Commission attempted to define the concept of Artificial Intelligence (AI) and presented a coordinated plan to promote the development and use of AI in Europe (EC, 2018 b).[38]

34 UN Human Rights Council (HRC): Resolution A/HRC/44/L.11 on "The Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, including the Right to Development**"**, 13 July 2020; https://documents-dds-ny.un.org/doc/UNDOC/LTD/G20/178/26/PDF/G2017826.pdf?OpenElement

35 UN Human Rights Council (HRC): Resolution 47/23 on "New and Emerging Digital Technologies and Human Rights",13 July 2021, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/192/18/PDF/G2119218.pdf?OpenElement

36 OHCHR (2023). Call for inputs: The relationship between human rights and technical standard-setting processes for new and emerging digital technologies - Report of the High Commissioner for Human Rights, 30 June 2023; https://www.ohchr.org/en/calls-for-input/2023/call-inputs-relationship-between-human-rights-and-technical-standard-setting

37 European Commission (2018a). *"Artificial Intelligence for Europe"*, Communication from the Commission COM(2018) 237, Brussels, 25.4.2018; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

38 European Commission (2018b). *"Coordinated Plan on Artificial Intelligence",* Communication from the Commission to the E.Parliament, the European Council, the Council, the European

Artificial Intelligence (AI) refers to systems that exhibit intelligent behaviours by analyzing their environment and take action, with some degree of autonomy, to achieve specific goals (EC, 2019: 46).[39] AI systems can be based solely on software, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, voice and facial recognition systems), or AI can be embedded in hardware devices (e.g. advanced robots, autonomous vehicles, drones or applications for the Internet of Things) (EC, 2018a:1). *Deep learning* is today the dominant approach to facial detection and analysis, and algorithms are routinely trained to learn and extract facial features and properties from large datasets (EP, 2021a: 2).[40]

Video surveillance using AI is capable of ***remote identification through facial recognition.***[41]. Biometric data capture, matching and identification all happen without significant delays. These include not only instant identification but also limited short delays to avoid circumvention (Art. 3 (37) of the Proposal for the *Artificial Intelligence Act,* 2021). Facial recognition technology can compare digital facial images to determine if they are of the same person. *Live facial recognition technology* implies comparing images obtained from video cameras (CCTV) with images from databases. Peoples' facial images are recognizes as a

Economic and Social Committee and the Committee of the Regions COM(2018) 795, Brussels, 7.12.2018; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0795

39 "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions" (European Commission/EC (2019). High-Level Expert Group on Artificial Intelligence: "*Ethics guidelines for trustworthy AI*", 8 April 2019, 46. Retrieved 20 March 2023 from https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai).

40 European Parliament (2021a). *Regulating facial recognition in the EU*, by T.Madiega and H.Mildebrath, European Parliamentary Research Service/EPRS, PE 698.021, September 2021, Retrieved 20 March 2023 from https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf
As stated in the EP/EC Communication *A European strategy for data* (2020), "the volume of data produced in the world is growing rapidly, from 33 zettabytes in 2018 to an expected 175 zettabytes in 2025" (EC, 2020a: 2).

41 *Remote biometric identification* can be defined as "AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used" (Recital 8 of Proposal for the *Artificial Intelligence Act*, COM/2021/206, 2021).

form of sensitive data (FRA, 2019:1).[42] Yet, facial images do not refer to simple photographs, as provided for in Recital 51 of the GDPR.[43] Images will constitute biometric data when they are processed through specific technical tools that allow the unique identification or authentication of a person (CoE, 2021:3).[44] *Emotion recognition systems* are defined as "AI systems whose purpose is to identify or infer the emotions or intentions of individuals based on their biometric data" (Art.3(34) *Proposal for the Artificial Intelligence Act,* 2021).

Biometric data[45], which are considered sensitive data[46], can thus be collected and used. The GDPR prohibits the processing of biometric data for the unique

42 FRA/EU Agency for Fundamental Rights (2019). *"Facial recognition technology: fundamental rights considerations in the context of law enforcement"*, Retrieved 20 March 2023 from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

43 Preamble §51 of the GDPR: "The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person".

44 Council of Europe/CoE (2021). *Convention 108: Guidelines on Facial Recognition*", T-PD(2020)03rev4, Directorate General of Human Rights and Rule of Law, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 2021, 3; https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

45 Article 4 (§14) of the GDPR stipulates: "*biometric data* means personal data 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 or dactyloscopic data." Directive EU/2016/680 or Regulation EU/2018/1725 contain a similar definition (Art. 3(18) Regulation EU/2018/1725 of the E.Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation EC/No 45/2001 and Decision No.1247/2002/EC, **OJ L** 295, 21.11.2018, 39-98).

46 Facial images fall into the special category of personal data, designated as sensitive data. Thus, EU data protection law provides for enhanced protection and additional safeguards compared to other personal data (FRA, 2019: 5).

identification of a natural person,[47] with some exceptions.[48] As noted by the Article 29 Data Protection Working Party experts, facial recognition technology may be used for identification, authentication/verification and categorisation purposes, by relying on: 1) biological/physical properties, physiological or behavioural characteristics, unique traits or repeatable action (WP 2012a:4)[49], such as: fingerprint verification, fingerprint image analysis, iris recognition, retina analysis, face recognition, hand pattern contour, ear shape recognition, body odour detection, voice recognition, DNA pattern analysis and sweat pore analysis, etc), and 2) behaviour-based techniques measuring one's conduct (e.g. analysing handwritten signatures, keystroke analysis, patterns indicating subconscious thoughts, movements, walk, talk, etc. (WP 2012b: 4).[50]

AI and real-time surveillance are important for prevention and security purposes. The rule-based video surveillance, and especially facial recognition technology, can help law enforcement bodies classify data and find missing people; they can also be used in identity theft investigations, etc. "AI-powered cameras are not limited to public surveillance, but also engage in intelligent analytics" (*Security Boulevard:* Zola, 2020).[51]

47 Art. 9 para. (1) of GDPR prescribes: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited." According to Article 22(2) and (4) of the GDPR, automated decision-making, including profiling, must not be based on sensitive data, and the operator is obliged to ensure measures to safeguard the data subject's rights, freedoms and legitimate interests.

48 The European Parliament Resolution of 25 March 2021 on *a European strategy for data* (2021/C 494/04) recalls that the processing of special categories of personal data under Article 9 of the GDPR is in principle prohibited, with certain strict exceptions, which include specific processing rules and the obligation to conduct a data protection impact assessment; it also highlights the potentially disastrous and irreversible consequences of wrongful or unsecure processing of sensitive data for the individuals concerned (§33). (EP Resolution of 25 March 2021 on *a European strategy for data* (2020/2217(INI)/(2021/C 494/04), O.J. EU C 494/37, 8.12.2021; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2021.494.01.0037.01.ENG

49 Article 29 Data Protection Working Party (2012a). *Opinion 02/2012 on facial recognition in online and mobile services*, WP 192, Brussels, 22 March 2012, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

50 Article 29 Data Protection Working Party/WP (2012b). *Opinion 3/2012 on developments in biometric technologies,* WP 193, Brussels, 27 April 2012, Retrieved 26 March 2023 from https://www.pdpjournals.com/docs/87998.pdf

51 *Security Boulevard:* Zola (2020). AI Surveillance in a Post-Pandemic World, by A. Zola, Security Bloggers Network, 10 June 2020, https://securityboulevard.com/2020/06/ai-surveillance-in-a-post-pandemic-world/

In spite of many advantages, the use of these advanced technologies can lead to abuses and the limitation of fundamental freedoms. The EC *White Paper on Artificial Intelligence* states that AI involves "a number of potential risks, such as opaque decision-making, gender-based or other kinds of discrimination[52], intrusion into our private lives or use for criminal purposes" (EC, 2020b:1). The EC *Proposal for the "Artificial Intelligence Act*" (2021) also points out that AI systems which are used for general purposes by or on behalf of public authorities for assessing social behaviour of natural persons may lead to discriminatory outcomes and exclusion of certain groups. They "may violate the right to dignity and non-discrimination, as well as the values of equality and justice" (Preamble § 17). The use of AI-powered technology may adversely affect fundamental rights and freedoms, including freedom of speech, assembly, religion, privacy, the rights of the child (due to their high vulnerability), human dignity, equality, democracy and the rule of law (Preamble § 15-18). Some "high-risk AI systems" may also have a negative impact on people's safety (EC, 2021:13-14).

It should be noted that, at this legislative stage, the GDPR only marginally addresses the implications of AI for data protection (Paal, 2022: 291). If we look at Article 5 GDPR, for example, in terms of *data transparency* in AI processes, it is hard to believe that data can be transparently collected or easily accessed (Paal, 2022: 292-293). Even in case of legitimate aims, which should be clearly communicated to data subjects, the aims may be incompatible with the actual purpose of AI technologies.[53] The data storage period must also be limited in time, "ensuring that the period for which personal data is stored is strictly limited to the minimum" (Preamble § 39 GDPR); it is in conjunction with Article 17 §1 of the GDPR: "the targeted subject has the right to obtain from the operator the deletion of personal data concerning him, without undue delay." Yet, we have to ask whether AI technology can still be developed if the storage period is limited in time?

The *Proposal for the "Artificial Intelligence Act"* (2021) states that "the use of AI systems for the ***"real-time" biometric identification*** of natural persons in publicly accessible spaces for the purpose of law enforcement is considered par-

52 It has been reported that facial recognition technology produced errors when it was used on people of color, which can lead to discrimination. Some AI facial analysis software shows biases based on gender and race, showing low errors in sex determination for lighter-skinned men but high errors in sex determination for darker-skinned women (Buolamwini, Gebru, 2018: 1-15). Browne asserts that "surveillance is both a discursive and material practice that reifies boundaries, borders, and bodies around racial lines, so much so that the surveillance of blackness has long been, and continues to be, a social and political norm" (Browne, 2015: 10).

53 Yet, imposing legitimate aim restrictions will inhibit the development and use of AI, preventing companies from experimenting with their algorithms or trying new uses for existing data. (Wallace, Castro, 2018:14).

ticularly intrusive in the rights and freedoms of the persons concerned, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly discourage the exercise of freedom of assembly and other fundamental rights. In addition, the immediacy of the impact and the limited opportunities to carry out further checks or corrections in relation to the use of such systems operating in real time entail increased risks for the rights and freedoms of persons targeted by law enforcement activities" (Preamble §18).These systems may only be used in case it is necessary to achieve a substantial public interest: in case of searching for missing children or potential victims of crime; in case of threats to the life or physical safety of natural persons or a terrorist attack; in case detection, location, identification or prosecution of the suspected persons or perpetrators of criminal offences envisaged in the Council Framework Decision 2002/584/JHA38[54], if those criminal offences are defined in the law of the Member State and punishable by a custodial sentence or a detention order for a maximum period of at least three years (Preamble §19).[55] Yet, the Member States are free to decide whether they wish to implement the exceptions in their national legislation and ban the use of real-time facial recognition systems in publicly accessible spaces for law enforcement purposes (Article 5 § 1d) of the Proposal *for the "Artificial Intelligence Act"* 2021).

Directive (EU) 2016/680[56] also establishes that "[...] the processing of biometric data for the unique identification of a natural person [...] is authorized only when it is strictly necessary and subject to adequate guarantees for the rights and freedoms of the data subject, and only when: a) it is authorized by Union law or internal law; b) it is necessary to protect the vital interests of the data subject or of another natural person, the respective processing refers to data that is made publicly available by the data subject" (Article 10 of Directive (EU) 2016/680).

Biometric facial recognition technologies are increasingly used to identify, classify, track individuals by both public and private entities. In recent years, they have become more widespread and more controversial, popping up everywhere

54 See: Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, the Council of the European Union, (OJ L 190, 18.7.2002, p. 1);

55 The custodial sentence threshold of at least 3 years indicates that the offence should be serious enough to justify the possible use of "real-time" remote biometric identification systems (Preamble §19 *of the Proposal for "the Artificial Intelligence Act",* 2021).

56 Directive (EU) 2016/680 of 27 April 2016 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, and repealing Council Framework Decision 2008/977/JHA, O.J. EU, L 119/89, 4.5.2016;https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680

(from airport check-in lines to police departments and pharmacies). However, while it may add a sense of security and convenience to businesses deploying it, the new technology has been widely criticized by privacy advocates for its built-in racial bias and potential for abuse. Machine learning, accompanied by the analysis of large amounts of data, makes these operations even more risky.

The AI Global Surveillance Index shows the results of empirical research on AI surveillance use in 176 countries worldwide. The data show that at least 75 out of 176 countries globally (43%) are actively using AI technologies for surveillance purposes (Feldstein, 2019:7). The common surveillance tools are: smart city/ safe city platforms (56 out of 75 states), facial recognition systems (64 out of 75 states), and smart policing (53 out of 75 states) (Feldstein, 2019:16). Liberal democracies are major users of AI surveillance. The index shows that 51% of advanced democracies are deploying AI surveillance systems to monitor borders, to catch potential criminals, to monitor citizens for inappropriate behaviour, to weed out terrorist suspects from crowds (Feldstein, 2019: 10). States with authoritarian systems and low levels of political rights are investing heavily in AI surveillance techniques (Feldstein, 2019:8). Governments in autocratic/semi-autocratic countries are more prone to abuse AI surveillance than governments in liberal democracies (Feldstein, 2019:2).

The overall mission of a smart city is to optimize the operational efficiency and quality of municipal and government services and drive the economic growth while improving the quality of life by using smart technology and data analytics (TechTarget, 2020).[57] By using AI, the images captured for surveillance purposes can be analyzed quickly and action can be taken in real time. Some studies note that AI technologies can help reduce crime by 30 to 40% and reduce response times for emergency services by 20 to 35% (*SmartCitiesDive*: Teale, 2018); others report on the use of AI technology in smart cities: facial recognition and biometrics (84%), in-car and body cameras for police (55%), drones and aerial surveillance (46%), crime reporting and emergency apps (39%), etc. (Deloitee, 2021: 131).[58] The global video surveillance market is currently worth approximately $45.5 billion, growing at a compound annual growth rate of 10.4% to reach $74.6 billion by 2025 (*Security Boulevard:* Zola, 2020). As city surveillance is the dominant application of surveillance infrastructure, the global video

57 TechTarget (2020). Smart City; July 2020; https://www.techtarget.com/iotagenda/definition/smart-city (accessed 30 March 2023).

58 Deloitte (2021). Urban Future with a Purpose; https://www.deloitte.com/content/dam/assets-shared/legacy/docs/perspectives/2022/deloitte-urban-future-with-a-purpose-study-set2021.pdf

surveillance market is expected to grow from USD 53.7 billion in 2023 to the projected USD 83.3 billion by 2028 (MarketsandMarkets, 2023).[59]

Facial recognition technologies are already used for different purposes, including detecting emotions. Wales used this technology during the UEFA Champions League in 2017. The German police used facial recognition technology during the G20 summit in Hamburg (2017). The French police tested this technology by using volunteers during the 2018 carnival in Nice (FRA, 2019:11-12). Elaborate AI-powered technologies were also used in EU project *iBorderCtrl* (2016-2019), aimed at testing an automated border-control system at the EU external borders (in Hungary, Greece, Latvia, Poland, Spain, UK) by integrating facial recognition, lie-detection and other technologies (FRA, 2019: 8; EC, 2018).[60] At the outset of the Covid-19 pandemic, France used AI to monitor the subway/metro system to ensure passengers are wearing protective masks, not in order to identify and punish the non-abiding citizens but to generate anonymous data to help the authorities anticipate the likelihood of future infection outbreaks (*The Verve:*Vincent, 2020).[61] In France, facial recognition technology was also tested in two high schools to help security guards prevent intrusion by strangers or identity theft (EP, 2021a:37). Spain uses facial recognition for surveillance at airports (to improve border control and security) and bus stations (to prevent petty crime and vandalism); recently, a supermarket chain *Mercadona* has stated using it to detect people who have been given a restraining order or banned by the court from entering the supermarket premises (EP, 2021a:38). Great Britain, Hungary and the Czech Republic also use facial recognition systems at their airports and in the streets to preserve the public order, road safety, identify criminals, etc. (FRA, 2019:3). During the Covid-19 lockdown, Russia used tens of thousands of facial recognition cameras and digital passes on cell phones to track citizens and keep them in quarantine (*BBC*, 2020).[62] The UK Gambling Commission allowed the use of facial recognition systems to keep track of players, monitor those moving around gambling sites and control addiction (Onufreiciuc,

59 MarketsandMarkets (2023). Video Surveillance Industry worth $83.3 billion by 2028, Press release, https://www.marketsandmarkets.com/PressReleases/global-video-surveillance-market.asp

60 EC (2018). *Smart lie-detection system to tighten EU's busy borders* (press release), 24 October 2018, accessed 30 March 2023
https://ec.europa.eu/research-and-innovation/en/projects/success-stories/all/smart-lie-detection-system-tighten-eus-busy-borders

61 *The Verge* (2020). France is using AI to check whether people are wearing masks on public transport, by J. Vincent, 7 May 2020, https://www.theverge.com/2020/5/7/21250357/france-masks-public-transport-mandatory-ai-surveillance-camera-software

62 *BBC* (2020). Coronavirus: Russia uses facial recognition to tackle Covid-19, 4 April 2020; https://www.bbc.com/news/av/world-europe-52157131

2020: 95-103). Kyrgyzstan, India, Israel, the USA or Australia are also among the countries that have implemented facial recognition and AI-assisted surveillance systems in public spaces (EP, 2021a:32).

In Romania, the Police implemented the project "Development of the facial identification and recognition system (NBIS) and its interconnection with EU law enforcement authorities through sTESTA", financed by the European Commission (2018-2021).[63] On the occasion of the Pope's visit, Kenya used a video surveillance system from the *Kenya Safe City* project, initiated by Huawei, including 1800 HD cameras and 200 HD traffic surveillance cameras in the country's capital Nairobi. The national police command centre, with more than 9,000 police officers and 195 police stations, was established to carry out monitoring and case resolution (Feldstein, 2019: 18).

Facial recognition systems are also widely used by public authorities or police for video surveillance during social protests. According to a report by Amnesty International, at least 64 countries are actively using facial recognition systems in the world today (Feldstein, 2019: 32). A study conducted in Montreal showed that real-time CCTV monitoring can provide behavioural cues related to suicide risk, identify individuals and save lives (Mishara, Bardon, Dupont, 2016: 1245).

In 2018, Middle School no. 11 in Hangzhou (China) held a *smart campus* seminar which unveiled the project *Smart Classroom Behaviour Management System*. In addition to using facial recognition to monitor library loans or mobile payments in the coffee shop, "smart eyes" were also installed in the classroom so that students no longer dared to be inattentive in classes (Article 19, 2021: 29-30).[64] There are countries like India, Kenya, South Africa, Argentina, Bangladesh, Chile, USA, where biometric data collection systems are used in social welfare systems (EP, 2021b:17).[65]

63 Poliția Româna (2021). Proiectul ,,Dezvoltarea sistemului de identificare și recunoaștere facială (nbis) și interconectarea acestuia cu autoritățile de aplicare a legii din ue prin intermediul stesta" (Project: Development of facial identification and recognition system (NBIS) and its interconnection with EU law enforcement authorities through sTESTA, 25 Noiembrie 2021; https://www.politiaromana.ro/ro/comunicate/proiectul-dezvoltarea-sistemului-de-identificare-si-recunoastere-faciala-nbis-si-interconectarea-acestuia-cu-autoritatile-de-aplicare-a-legii-din-ue-prin-intermediul-stesta

64 Article 19/Free Word Center (2021). *Emotional Entanglement: China's emotion recognition market and its implications for human rights*, Jan.2021, 29, Retrieved 31 March 2023 https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf

65 European Parliament (2021b). *Digital technologies as a means of repression and social control,* by D.Głowacka, R.Youngs, A. Pintea, E.Wołosik, Directorate-General for External Policies of the EU, 2021, 17, Retrieved 31 March 2023 from https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653636/EXPO_STU(2021)653636_EN.pdf

Due to the controversies concerning the use of these technologies, some states in the USA (e.g. Oregon) have banned the use of facial recognition technology by the city departments, including the local police, and businesses catering for the general public (stores, restaurants, hotels) (Portland.gov, 2020[66]; *CNN Business:* Metz, 2020)[67]. San Francisco, Oakland or Boston banned the use of this surveillance technology in the city (*The New York Times*: Conger, Fausset, Kovaleski, 2019).[68] In 2016, Baltimore police secretly launched aerial drones to conduct daily surveillance of the city's residents; the project was abruptly ended when the media revealed this fact (*Axios:* Hart, 2019). In the U.S., the *Commercial Facial Recognition Privacy Act* (bill) of 2019 prohibited entities from collecting, processing, storing, or controlling facial recognition data unless those entities provide documentation explaining the capabilities and limitations of facial recognition technology and obtain the end users' explicit and affirmative consent to use such technology after they have been informed of the reasonably foreseeable uses of the data collected through facial recognition (US Congress, 2019).[69]

4. Instead of conclusion: *How do these technologies affect our daily lives? Do the benefits outweigh the risks?*

Facial recognition technologies are no longer a novelty, and the fact that they are increasingly used in various fields raises contradictory opinions. The personal safety and general security is seen as opposed to the human rights and fundamental freedoms that can be affected by the use of these technologies. The standards and related guarantees for the use of AI must be strictly regulated in order not to amplify the justified fears related to these facial recognition systems. It is a real challenge to reconcile the use of new technologies with the protection of human rights, but the instruments adopted by the EU and those at the international level show concern for addressing the specific issues raised by AI. It is imperative to adopt a legislative framework that regulates the use

66 Portland.gov (2020). *City Council approves ordinances banning use of face recognition technologies by City of Portland bureaus and by private entities in public spaces*, 9 September 2020, Retrieved 31 March 2023 from https://www.portland.gov/smart-city-pdx/news/2020/9/9/city-council-approves-ordinances-banning-use-face-recognition

67 CNN Business (2020): Portland passes broadest facial recognition ban in the US, by R. Metz, 9 September 2020, https://edition.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html

68 *The New York Times* (2019): San Francisco Bans Facial Recognition Technology, by Conger, K.,Fausset, R. Kovaleski, S.F.; 14 May 2019; https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

69 US Congress (2019): Commercial Facial Recognition Privacy Act of 2019, S.847 - 116th Congress (2019-2020), March 2019; https://www.congress.gov/bill/116th-congress/senate-bill/847

of these technologies, according to the principle of proportionality, but also to provide sufficient guarantees for the protection of fundamental human rights. The GDPR limited the use of data, especially in AI processes, but this Regulation should be further amended in the future.

The EU legislation recognizes that facial images constitute biometric data, as they can be used to monitor, track, identify, classify and assess people (surveillance, identity verification, classification by specific characteristics, etc.). AI technologies have multiple uses: at police headquarters, at work, in schools, means of transport, banks, shops, stadiums, homes, various events. The need to control migrations, track terrorist threats, repress antisocial conduct (etc.) urges both developed and poor economies to allocate budgets for the development of AI technologies. There are good reasons for using these technologies but the huge amount of data, the way they are stored and used seems to be getting out of control, and surveillance does not seem so legitimate anymore. The legitimate interest of the operator cannot be superior to the fundamental rights, freedoms and interests of subjects requesting the protection of their data. Balancing these interests calls for legislative harmonization and guarantees of equal data processing conditions for all EU market participants.[70]

Whoever holds information holds power, and whoever holds vast amounts of information has even greater power. The competition between law and technology is unequal (Lascateu, 2020: 66), but the human being must be the focal point of concerns in both. As aptly stated by Bălan (2015), "it is necessary to abandon the protection of private life in line with all-or-nothing paradigm [...]; surveillance has to be treated distinctly in line with the targeted space and time" (Bălan, 2015: 65).

70 Recital 9 of the GDP: "Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law".

Recital 10 of the GDP: "In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States."

References

Bălan, I. (2015). Dreptul la respectarea vieţii private şi supravegherea video, audio sau prin fotografiere Partea a II-a. *Pandectele Române* 8: 63-93.
Brkan, M. (2019). The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal*, 20(6). 864-883.

Browne, S. (2015). Dark Matters: on the Surveillance of Blackness, Duke University Press, Durham, 10.

Buolamwini, J., Ordóñez V., Morgenstern J., Learned-Mill E. (2020). Facial Recognition Technologies: A Primer, Algorithmic Justice League/Mc Arthur Foundation, *29 May 2020,* 2-6; https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf

Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, *Proceedings of Machine Learning Research* 81, 1-15. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

De Gregorio, G. (2022). Digital Constitutionalism, Privacy and Data Protection, in Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society (2022). *Cambridge Studies in European Law and Policy*, 216, 217. Cambridge University Press; doi:10.1017/9781009071215.007

Feldstein, S. (2019). The Global Expansion of AI Surveillance, Carnegie Endowment for International Peace, Sept. 1019, 16, https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf

Lascateu, C. (2020). Culegerea de informaţii de securitate naţională în era digitală – dimensiunea etică, *Revista Universul Juridic* (3), March, 66.

Manescu, D. (2020). Viaţa privată, datele personale şi dreptul la informare, provocări ale zilelor noastre, in *Pandectele Române* (3), 102-114.

Mishara, B.L., Bardon, C., Dupont, S. (2016). Can CCTV identify people in public transit stations who are at risk of attempting suicide? An analysis of CCTV video recordings of attempters and a comparative investigation, *BMC Public Health*, 16(1):1245, 15 Dec. 2016 Dec; DOI 10.1186/s12889-016-3888-x.

Onufreiciuc, R. (2020). Protecţia datelor şi recunoaşterea facială automată: avem dreptul de a rămâne fără (un) chip?, *Studii si cercetari juridice europene*, 95-103.

Paal, B.P. (2022). Artificial Intelligence as a Challenge for Data Protection Law And Vice Versa, In: Voeneky S., Kellmeyer P., Mueller O., Burgard W. (Eds.), *The Cambridge Handbook of Responsible Artificial Intelligence*: Interdisciplinary Per-

spectives, Cambridge Law Handbooks., Cambridge: Cambridge University Press. 290, 297, doi:10.1017/9781009207898.023.

Şandru, D.M. (2019). Unele consideraţii cu privire la relaţia dintre protecţia datelor (în special Regulamentul general privind protecţia datelor) şi proprietatea intelectuală. *Revista Română de Drept European (Comunitar)* 3: 21-31.

Thome, B., Shamma D.A,, Friedland G., Elizalde B., Ni K., Poland D., Borth D., Li L-J. (2016). YFCC100M: The New Data in Multimedia Research, *Communications of the ACM*, vol.59, no.2, 2016; https://arxiv.org/pdf/1503.01817v2.pdf; https://dl.acm.org/doi/pdf/10.1145/2812802; (accessed 22 March 2023)

Wallace N., Castro D. (2018). *The Impact of the EU's New Data Protection Regulation on AI*, Centre for Data Innovation Policy Brief, 27 March 2018, 14, Retrieved 30 March 2023 from https://www2.datainnovation.org/2018-impact-gdpr-ai.pdf

Legal documents

Article 29 Data Protection Working Party/WP (2005). *Working document on data protection issues related to intellectual property rights,* 18 January 2005, WP 104 (Working Party set up under Article 29 of Directive 95/46/EC), Directorate E (Services, Copyright, Industrial Property and Data Protection) of the European Commission, Internal Market Directorate-General, Brussels, 2005; Retrieved 26 March 2023 from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp104_en.pdf

Article 29 Data Protection Working Party/WP (2012a), *Opinion 02/2012 on facial recognition in online and mobile services*, 00727/12/EN, WP 192, Brussels, 22 March 2012, p.2, https://www.pdpjournals.com/docs/87998.pdf; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

Article 29 Data Protection Working Party/WP (2012b). *Opinion 3/2012 on developments in biometric technologies,* 00720/12/EN, WP 193, Brussels, 27 April 2012, https://www.pdpjournals.com/docs/87998.pdf

Article 29 Data Protection Working Party/WP (2014): *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP 217, 9 April 2014; Retrieved 27 March 2023 from https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp217_en.pdf

Council of Europe/CoE (2018). Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (108/1981), No. 223, Strasbourg, 10.10.2018; https://rm.coe.int/16808ac918

Council of Europe/CoE (2021). *Convention 108: Guidelines on Facial Recognition*", T-PD(2020)03rev4, Directorate General of Human Rights and Rule of Law, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 Jan.2021, https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066

Council of Europe/European Court of Human Rights (2022).*Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence*, 31 August 2022, Retrieved 7 March 2023 from https://www.echr.coe.int/documents/guide_art_8_eng.pdf

The Charter of Fundamental Rights of the European Union (CFREU), *Official Journal of the European Communities* C 2000/C 364/01); https://www.europarl.europa.eu/charter/pdf/text_en.pdf

The Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, the Council of the European Union, (OJ L 190, 18.7.2002, p. 1); https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002F0584

Directive (EU) 2016/680 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 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, and repealing Council Framework Decision 2008/977/JHA, *Official Journal of the EU*, L.119/89, 4.5.2016; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC; PE/51/2019/REV/1; OJ L 130, 17.5.2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790

European Commission (2018a). *Artificial Intelligence for Europe*, Communication from the Commission COM(2018) 237, Brussels, 25.4.2018; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

European Commission (2018b). *Coordinated Plan on Artificial Intelligence,* Communication from the Commission to the E.Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2018)795, Brussels, 7.12.2018; Retrieved 20 March 2023 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0795

European Commission (2019). High-Level Expert Group on Artificial Intelligence: "*Ethics guidelines for trustworthy AI*", 8 April 2019, 46; https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

European Commission (2020a). *A European strategy for data*, Communication from the Commission to the EP, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2020)66, Brussels, 19.02.2020; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066

European Commission (2020b). *White Paper on Artificial Intelligence - A European approach to excellence and trust*, COM(2020)65, Brussels, 19.2.2020; Retrieved 20 March 2023 https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf

European Court of Human Rights/ECtHR (2020). *Guide to the Case-Law of the of the European Court of Human Rights, Data protection*, 31 August 2022, (p.86), https://www.echr.coe.int/documents/d/echr/Guide_Data_protection_ENG

European Data Protection Board/EDPB (2020): Guidelines 3/2019 on processing of personal data through video devices, 29 Jan. 2020.https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices.pdf

European Parliament/European Council (2021): Proposal for Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (*Artificial Intelligence Act*) and amending certain Union legislative acts, Brussels, 21.4.2021, COM(2021)/0106(COD)/206; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

European Parliament Resolution of the European Parlaiment of 25 March 2021 on *a European strategy for data* (2020/2217(INI)/(2021/C 494/04), *Official Journal EU,* C 494/37, 8.12.2021; Retrieved 20 March 2023 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2021.494.01.0037.01.ENG

European Parliament (2021). *Regulating facial recognition in the EU*, by T.Madiega and H.Mildebrath, European Parliamentary Research Service/EPRS, September 2021, Retrieved 20 March 2023 from https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

FRA/EU Agency for Fundamental Rights (2019). *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, Retrieved 20 March 2023 from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

General Data Protection Regulation (GDPR): 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 (GDPR), *JO L 119*, 4.5.2016; https://gdpr-info.eu

OHCHR/Office of the United Nations High Commissioner for Human Rights (2023). Call for inputs: The relationship between human rights and technical standard-setting processes for new and emerging digital technologies - Report of the High Commissioner for Human Rights, 30 June 2023; https://www.ohchr.org/en/calls-for-input/2023/call-inputs-relationship-between-human-rights-and-technical-standard-setting

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No.45/2001 and Decision No.1247/2002/EC, OJ L 295, 21.11.2018, (39-98); https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1725

UN Human Rights Council (HRC): Resolution A/HRC/44/L.11 on "The Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, including the Right to Development", 13 July 2020; https://documents-dds-ny.un.org/doc/UNDOC/LTD/G20/178/26/PDF/G2017826.pdf?OpenElement

UN Human Rights Council (HRC): Resolution 47/23 on "New and Emerging Digital Technologies and Human Rights",13 July 2021, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/192/18/PDF/G2119218.pdf?OpenElement

Romanian Law 333/2003 on the protection of objectives, goods, values and persons, with subsequent additions and amendments, *Official Gazette of Romania*, no.189/18 March 2014; https://legislatie.just.ro/Public/DetaliiDocument/156432

Romanian Law no.190/2018 on measures to implement 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 repeal of Directive 95/46/CE(GDPR), *Official Gazette* no.651/2018; https://legislatie.just.ro/Public/DetaliiDocument/203151

Romanian Law no. 363/2018 on the protection of natural persons regarding the processing of personal data by the competent authorities for the purpose of prevention, discovery, investigation, prosecution and combating of crimes or the execution of punishments, educational and safety measures, as well as regarding the free circulation of these data, *Official Gazette* no. 13/7 January 2019, https://legislatie.just.ro/Public/DetaliiDocument/209627

Government Decision no. 301 of 11 April 2012 on the approval of the Methodological Norms for the application of Law no. 333/2003, *Official Gazette* no. 335/17 May 2012, https://legislatie.just.ro/Public/DetaliiDocument/138059

Decision no. 174 of 18 October 2018 on the list of operations for which a personal data protection impact assessment is obligatory, National Supervisory Authority for the Processing of Personal Data, *Official Gazette* no. 918/ 2018, https://legislatie.just.ro/Public/DetaliiDocument/206331

Case law

Court of Justice of the European Union/CJEU case: Volker und Markus Schecke GbR and Hartmut Eifert Joined cases C-92/09 and C-93/09, Judgment of the Court (Grand Chamber) of 9 November 2010, par. 48.

CJEU case: *Volker und Markus Schecke and Eifert GbR and Hartmut Eifert*, joined cases C-92/09 and C-93/09, Opinion of Advocate General Sharpston, 17 June 2010, para. 71).

CJEU case: *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, joined Cases C-293/12 and C-594/12, Judgment (Grand Chamber), 8 April 2014).

CJEU case: *Maximillian Schrems v Data Protection Commissioner*, Request for a preliminary ruling from the High Court (Ireland). C-362/14, Judgment of the Court (Grand Chamber) of 6 October 2015, para. 94).

ECtHR case: *S. and Marper v. the United Kingdom*, Appl. no 30562/04, Strasbourg, December 2008, para.103).

ECtHR case: *Gaughran v. the United Kingdom, Appl.no 45245/15, Judgment 13.02.2020, Strasbourg,* https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-12731%22]}; accessed on 5 March 2023

ECtHR case: *Antović and Mirković v. Montenegro*, Application no 70838/13 Judgment 28 November 2017.

ECtHR case: *Bărbulescu v. Romania* Application no 61496/08, Judgment 5 September 2017.

ECtHR, *Peck v. the United Kingdom,* Application no 44647/98, Judgment 28 January 2003;

ECtHR Factsheet (2022). *Personal data protection*, December 2022, https://www.echr.coe.int/documents/d/echr/fs_data_eng

Online sources

Article 19/Free Word Center (2021). *Emotional Entanglement: China's emotion recognition market and its implications for human rights*, Jan.2021, Retrieved 31 March 2023; https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf

Axios: Hart, K. (2019). Baltimore Wrestles With Aerial Surveillance, *Axios,* 31 July 2019; (accessed 30 March 2023) https://www.axios.com/2019/07/31/baltimore-wrestles-with-aerial-surveillance-to-reduce-crime

BBC (2020). Coronavirus: Russia uses facial recognition to tackle Covid-19, 4 April 2020; https://www.bbc.com/news/av/world-europe-52157131

CNN Business: Metz, R. (2020): Portland passes broadest facial recognition ban in the US, by R. Metz, 9 September 2020, https://edition.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html

Deloitte (2021). *Urban Future With a Purpose*; https://www.deloitte.com/content/dam/assets-shared/legacy/docs/perspectives/2022/deloitte-urban-future-with-a-purpose-study-set2021.pdf (accessed 30 March 2023)

European Commission (2018). *Smart lie-detection system to tighten EU's busy borders* (press release), 24 October 2018;

https://ec.europa.eu/research-and-innovation/en/projects/success-stories/all/smart-lie-detection-system-tighten-eus-busy-borders

European Parliament (2021). *Digital technologies as a means of repression and social control,* by D.Głowacka, R.Youngs, A. Pintea, E.Wołosik, Directorate-General for External Policies of the EU, 2021, 17, Retrieved 31 March 2023 from https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653636/EXPO_STU(2021)653636_EN.pdf

MarketsandMarkets (2023). Video Surveillance Industry worth $83.3 billion by 2028, Press release, https://www.marketsandmarkets.com/PressReleases/global-video-surveillance-market.asp

The New York Times: Conger, K.,Fausset, R. Kovaleski, S.F. (2019). San Francisco Bans Facial Recognition Technology*,* 14 May 2019; https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

The New York Times: Hill, K., Krolik, A. (2019). How Photos of Your Kids Are Powering Surveillance Technology*, The New York Times*, https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html

Poliția Româna (2021). Proiectul "Dezvoltarea sistemului de identificare și recunoaștere facială (nbis) și interconectarea acestuia cu autoritățile de aplicare a legii din ue prin intermediul stesta" (Project: Development of facial identification and recognition system (NBIS) and its interconnection with EU law enforcement authorities through sTESTA), 25 Nov. 2021; https://www.politiaromana.ro/ro/comunicate/proiectul-dezvoltarea-sistemului-de-identificare-si-recunoastere-faciala-nbis-si-interconectarea-acestuia-cu-autoritatile-de-aplicare-a-legii-din-ue-prin-intermediul-stesta

Portland.gov (2020). City Council approves ordinances banning use of face recognition technologies by City of Portland bureaus and by private entities in public spaces, 9 September 2020, Retrieved 31 March 2023 from https://www.portland.gov/smart-city-pdx/news/2020/9/9/city-council-approves-ordinances-banning-use-face-recognition

SmartCitiesDive: Teale, C. (2018). Report: Smart city technology could dramatically improve quality-of-life indicators, by C.Teale, 12 June 2018, https://www.smartcitiesdive.com/news/smart-city-technology-quality-of-life/525495/

Security Boulevard: Zola, A. (2020). AI Surveillance in a Post-Pandemic World, by A. Zola, Security Bloggers Network, 10 June 2020, https://securityboulevard.com/2020/06/ai-surveillance-in-a-post-pandemic-world/

TechTarget (2020). Smart City; July 2020; https://www.techtarget.com/iotagenda/definition/smart-city (access 30 March 2023).

US Congress (2019):Commercial Facial Recognition Privacy Act of 2019, S.847 - 116th Congress (2019-2020), March 2019; https://www.congress.gov/bill/116th-congress/senate-bill/847

The Verge: Vincent, J. (2020). France is using AI to check whether people are wearing masks on public transport, by J. Vincent, 7 May 2020, https://www.theverge.com/2020/5/7/21250357/france-masks-public-transport-mandatory-ai-surveillance-camera-software

Carmen Oana Mihăilă, LL.D.
Ванредни професор,
Правни факултет, Универзитет у Орадеи,
Орадеа, Бихор, Република Румунија

Mircea Mihăilă, PhD (компјутерске науке),
Предавач,
Факултет електротехнике и информационих технологија Универзитета у Орадеи,
Орадеа, Бихор, Република Румунија

ВИДЕО НАДЗОР И ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА: УТИЦАЈ НА ПРАВО НА ПРИВАТНОСТ И ПРАВА ИНТЕЛЕКТУАЛНЕ СВОЈИНЕ

Резиме

Заштита права на приватност је све више представља кључно питање у контексту у видео надзора који се данас ефикасно обавља употребом врхунских савремених технологија. Технологија се непрестано развија и доприноси унапређењу у разним областима живота, међутим, брзи развој нових технологија доноси и велике ризике и потенцијалне претње, нарочито када су у те процесе укључене технологије попут вештачке интелигенције (паметне камере и системи видео надзора, биометрија и препознавање лица) које су у стању да анализирају огромну количину података, идентификују везе између података, и открију тачан идентитет појединца.

Употреба видео камера за надзор покреће важна питања приватности. Даљинска барометријска идентификација се може извршити само уз поштовање одређених гаранција људских права, у контексту оправданог интереса и у складу са принципом пропорционалности. Технологија препознавања лица је свеприсутна (у редовима за чекирање на аеродрому, полицијским управана, апотекама) мада последњих година постаје све конторверзнија тема, нарочито у погледу заштите људских оправа и слобода. Иако употреба савремених технологија може допринети осећају сигурности и удобности ентитета који је примењују, заговорници приватности увелико критикују употребу ове технологије, посебно због расне пристрасности и могућности злоупотребе. Сматра се да употреба биометријске идентификације појединаца у „реалном времену" и у јавним просторима, у сврху спровођења полицијских овлашћења, представља повреду људских права и слобода, али такође даје осећај сталног надзора и индиректно обесхрабрује остваривање слободе окупљања и других основних људских права.

Још један важан проблем је употреба видео надзора у контексту повреде права интелектуалне својине. Неовлашћена употреба видео/аудио снимака може утицати пословање привредног субјекта или појединца. Пословне тајне и поверљиве информације су често суштински део пословног порфолија интелектуалне својине неке компаније. Због тога компаније предузимају додатне заштитне мере како би осигурале да слике и видео записи буду безбедно ускладиштене и доступне само овлашћеном особљу. Камерама се снимају слике уметничких дела, приредбе, представе, изложбе, итд., тако да неконтролисани приступ може довести до кршења ауторских и сродних права. Снимљени видео записи се затим могу поставити на интернет платформе, па таква употреба интелектуалне својине може довести до кршења ауторских права, посебно када се видео материјал заштићен ауторским правима користи без дозволе власника или аутора, што представља кршење права интелектуалне својине.

Кључне речи: *видео надзор, технологија за препознавања лица, вештачка интелигенција, интелектуална својина, Општа уредба о заштити података (ГДПР).*