UDK [34:004.932'1]:341.231.14

*Mirjana DOKMANOVIĆ, Neven CVETIĆANIN**

REGULATION OF THE USE OF FACIAL RECOGNITION TECHNOLOGY –LIMITATIONS AND CHALLENGES FROM A HUMAN RIGHTS PERSPECTIVE**

Abstract. *The aim of this article to identify and highlight limitations and challenges of the legal regulation of the use of facial recognition technology for surveillance purposes. The UN and the EU are seeking to develop robust human rights safeguards to regulate such practices, whereas civil society calls for a complete ban on it use for mass surveillance. The type of this technology makes it difficult to impose legal and democratic control over its lawful use and to prevent abuse. We conclude that the regulation of this area, no matter how restrictive, amounts to tacit approval of the mass use of this type of technology that opens the door to various ways of abusing human rights and freedoms, and whose justification from the perspective of the public interest is questionable.*

Keywords: *video surveillance; facial recognition technology; right to privacy; protection of personal data; Clearview AI*

Introduction

> *The explosion of AI technologies,*
> *without sufficient guardrails,*
> *has already led to chilling setbacks for human rights.*
> (Volker Türk, UN High Commissioner for Human Rights)[1]

Video surveillance cameras on streets, roads, banks and shops, even in workplaces, have become commonplace. Ever more of these cameras (e.g.,

* *Mirjana Dokmanović, PhD, Research Associate, Centre for Legal Research, Institute of Social Sciences, Belgrade, Serbia; Neven Cvetićanin, PhD, Senior Research Associate, Centre for Sociological Research and Anthropological Research, Institute of Social Sciences, Belgrade, Serbia.*

** *This article was written as part of the 2023 Research Programme of the Institute of Social Sciences with support from the Ministry of Science, Technological Development and Innovation of the Republic of Serbia.*

DOI: 10.51936/tip.60.3.548

[1] *United Nations Office of the High Commissioner for Human Rights. Türk addresses World Standards Cooperation meeting on human rights and digital technology, 24. 2. 2023.*

closed-circuit television (CCTV)) rely on advanced technologies containing software to recognise faces and emotions. This facial recognition technology (FRT) is defined as "a specific type of biometric technology that refer to a multitude of technologies used for different purposes, ranging from the simple detection of the presence of a face in an image, to more complex verification, identification, and categorisation or classification of individuals" (Madiega and Mildebrath, 2021: 1).

The use of FRT is increasing globally. It was estimated that by January 2022 approximately 110 countries were either using or had approved the use of FRT for surveillance purposes (Bischoff, 2022). Common uses of CCTV with FRT for general surveillance include: as part of border control; in policing, to detect criminals and accelerate investigations, and find missing children and persons; in airports, to improve security and speed up boarding; in institutions like companies, banks and government buildings, to monitor visitation. One may expect an increase in the areas where this technology will be used, for example, in mobile banking systems eliminating the need for passwords, to unlock a car, in 'smart buildings' or to monitor employee productivity (Forbes, 2022). Companies have started using facial recognition to target advertising toward a specific audience group (Altaf, 2022). The recent COVID-19 pandemic saw novel uses of FRT such as for monitoring whether potential carriers of the coronavirus were obeying the rules of quarantine, to check whether an individual was wearing a mask and whether people were respecting the social distance rules (Becuywe et al., 2022: 27–31).

Accordingly, notable proportions of people's lives all around the world are today being tracked and monitored by police, government agencies, advertisers, security agencies, banks and companies (Rainie et al., 2022). At the same time, the regulation of this area in many countries is still poor or does not exist at all. Clear boundaries on the use of this type of 'smart' surveillance of people have yet to be established, even though the risks of the uncontrolled use of surveillance of privacy and protection of personal data are high and indisputable. The aim of this article to identify and highlight limitations and challenges of the legal regulation of FRT use for surveillance purposes. The first section of the article presents an overview of the main concerns related to the use of this technology from a human rights perspective. The second part elaborates the position of countries and civil society in Europe with respect to attempts to regulate the use of FRT. The third section discusses the limitations of legal regulation on the use of FRT surveillance to safeguard individuals' human rights and freedoms. In the conclusion, we argue that the regulation of this area, no matter how restrictive, amounts to tacit approval of the mass use of a type of technology that is opening the door to various types of abuses and restrictions on human rights and freedoms, and whose justification from the perspective of the public interest is questionable.

Overview of the problem

The use of FRT is accompanied by many concerns regarding, among others, privacy, accuracy and control of the usage and storage of the data gathered. Over a decade ago, Karlovšek et al. (2008) warned about the need to set up boundaries for the use of a video surveillance to monitor employees. Worries have been particularly raised by the development of web-based intelligence platforms powered by FRT that are used not only by law enforcement and other state actors, but private companies such as Clearview AI as well. The practice of the mentioned company raises so many issues that some national authorities have banned Clearview AI from the further collection of data, as described in the second section of this article. Namely, this US-based private company's platform has gathered the largest known database of 30+ billion facial images sourced from public-only web sources, including news media, mugshot websites, public social media, and other open sources (Clearview AI). Clearview AI uses a process called data scraping to scour the Internet for what it states are "public" photos to stockpile its database. This includes gathering images from Facebook, Instagram, Twitter, YouTube, LinkedIn, Venmo and other social media applications without the tacit approval of their users. The company has declared that it "serves federal, state, tribal and local law enforcement agencies", supporting them "to identify victims and perpetrators in order to safeguard their communities and secure industry and commerce" (Clearview AI). Clearview AI states that it uses the photos gathered only to assist law enforcement. Yet, many argue the software represents "an invasion of privacy because there was no consent for Clearview AI to use their photos. Because of its algorithm, which recognizes faces even in the background of images, people can be identified even if they are unaware their photo was being taken" (University of Miami News, 2020). The possibilities for the abuse of photos gathered from social media without the knowledge and consent of the persons in those photos are immense, and the consequences may be chilling.

In many countries, citizens have pointed to the substantial and potential misuse of this technology and threats to privacy and the enjoyment of human rights. A survey by Kostka, Steinacker and Meckel (2023) indicates that trust in respective governments and their administrations plays a key role in the development of these acceptance levels. Acceptance of the public use of FRT correlates with cross-country differences in political contexts "with 51% of Chinese respondents showing the highest level of acceptance", while "only 37% of their American and 38% of their German counterparts strongly or somewhat accept FRT for public use" (Kostka, Steinacker and Meckel, 2023: 12). This study also shows that citizens are especially critical of FRT uses in public when they perceive FRT uses as a threat to their individual privacy. A survey taken in the United States reveals that "only 36% of Americans trust technology companies will use facial recognition responsibly, and 95% of citizens feel they should have the right to opt-out of facial recognition; just 32% of consumers feel comfortable having their faces scanned by businesses, and 81% of them are concerned about biometric data misuse" (Wolf, 2023). In 2020, civil society across Europe launched the "Reclaim Your Face" campaign, demanding that "local and national authorities listen to their communities about the serious risks of using facial recognition and other biometric technologies in public spaces" (EDRI, 12 November 2020), while a global campaign to ban the use of FRT was started in January 2021 by Amnesty International (Amnesty International, 2021a).

Citizens' concerns about the threat to the right to privacy and other human rights are particularly in response to the lack of liability of and control over authorities, companies and other users of FRT. Addressing this issue, in June 2021 Andrea Jelinek, Chair of the European Data Protection Board (EDPB), and Wojciech Wiewiórowski, European Data Protection Supervisor (EDPS), issued a joint statement:

> *Deploying remote biometric identification in publicly accessible spaces means the end of anonymity in those places. Applications such as live facial recognition interfere with fundamental rights and freedoms to such an extent that they may call into question the essence of these rights and freedoms. This calls for an immediate application of the precautionary approach. A general ban on the use of facial recognition in publicly accessible areas is the necessary starting point if we want to preserve our freedoms and create a human-centric legal framework for AI. The proposed regulation should also prohibit any type of use of AI for social scoring, as it is against the EU fundamental values and can lead to discrimination.* (EDPB, 21 June 2021)

The EDPB and the EDPS have jointly called for a ban on the use of facial recognition in public spaces. The call for a global ban has also been echoed by numerous civil society organisations around the world (Privacy International, 2021; European Centre for Non-for-Profit Law, 2021; Amnesty International, 2021).

In addition, this issue was the subject of various policy briefings whose goal was to warn European Union institutions about the consequences of using FRT for fundamental human rights. In 2021, the European Parliamentary Research Service produced a study containing analysis of all aspects of the regulation of FRT in the EU, considering that hitherto there have been "limited legally binding rules applicable to FRT" (Madiega and Mildebrath, 2021).

Position of the EU member states

In the EU member states a debate is still underway among legislators about the benefits and risks of using facial recognition systems. In October 2021, the European Parliament (EP) adopted a resolution on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters. [2] The EP expressed its great concern over the use of private facial recognition databases by law enforcement actors and intelligence services, such as Clearview AI, which has without a lawful basis collected a database of over 30 billion pictures from social networks and other parts of the Internet, including from EU citizens. The EP resolution calls on member states to oblige law enforcement actors to disclose whether they are using the Clearview AI technology or equivalent technologies from other providers; recalls the European Data Protection Board (EDPB) opinion that the use of a service such as Clearview AI by law enforcement authorities in the European Union would "likely not be consistent with the EU data protection regime"; and calls for a ban on the use of private facial recognition databases in law enforcement. Moreover, this resolution

> *calls for a moratorium on the deployment of facial recognition systems for law enforcement purposes that have the function of identification, unless strictly used for the purpose of identification of victims of crime, until the technical standards can be considered fully fundamental rights compliant, results derived are non-biased and non-discriminatory, the legal framework provides strict safeguards against misuse and strict democratic control and oversight, and there is empirical evidence of the necessity and proportionality for the deployment of such technologies.* (para. 27)

The resolution seeks a ban on facial recognition and automated analysis and/or recognition of other human features, such as gait, fingerprints, DNA, voice, and other biometric and behavioural signals, in publicly accessible spaces; private facial recognition databases in law enforcement; predictive policing, i.e., algorithmic-driven behavioural predictions to identify people likely to commit a crime on the basis of historical data and past behaviour,

[2] *European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)).*

group membership, location or any other such characteristic; on any processing of biometric data, including facial images, for law enforcement purposes that leads to mass surveillance in publicly accessible spaces; on AI-enabled mass-scale scoring of individuals.

In its Guidelines on Facial Recognition (2021), the Council of Europe has also called for a moratorium on the use of live FRT in uncontrolled environments, places freely accessible to individuals where they can also pass through, including public and quasi-public spaces like shopping malls, hospitals or schools. In June 2021, the EDPB and European Data Protection Supervisor (EDPS) issued a joint statement calling for a ban on the use of AI for the automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination. Further, the EDPB and the EDPS consider that the use of AI to infer the emotions of a natural person is highly undesirable and should be prohibited, except in very specified cases such as some health purposes, and that the use of AI for any type of social scoring should be prohibited.

In line with these demands, in November 2022 the Council of the EU approved the proposal for the Artificial Intelligence Act, which is expected to be adopted close to the end of 2023. The text of the proposed Act clarifies that the use of "real-time" remote biometric identification system in public spaces is strictly necessary for law enforcement purposes and where law enforcement authorities should be allowed to use the system as an exception. However, several members of the European Parliament are demanding a complete ban on these practices (Reclaim Your Face, 15 September 2022). They consider that the proposed AI Act is weak because it does not prohibit 'post' uses of remote biometric identification, the ban would only be applied to law enforcement actors, and since it contains wide and dangerous exceptions that could undermine the purpose of the ban.

In the majority of EU countries, facial recognition in offence proceedings is not directly or clearly regulated but is generally a topic of legislation related to a criminal procedure code, data protection, personal data proceeding, national security service, police etc. (TELEFI Project, 2020: 40–190). The legal basis for having such a database for facial images is missing in many countries (TELEFI Project, 2020: 40–190).

In March 2023, France became the first European country to legalise the use of FRT surveillance. By adopting the Law on Olympic Games that envisages the use of FRT surveillance during the 2024 Paris Olympics, the French parliament formalised the introduction of the algorithmic processing of private data in public spaces (La Quadrature du Net, 2023). This step has triggered protests of civil society, branding the legislation "dystopian", unconstitutional, and one of the greatest-ever violations of the right to privacy (Barker, 2023; European Centre for Non-for-Profit Law, 1 March 2023;

European Centre for Non-for-Profit Law, 25 April 2023). Many believe that the French government used the Law on Olympics as a pretext to authorise algorithmic video surveillance (AVS), thereby creating a worrisome precedent and normalising biometric mass surveillance (Duroy, 2023).

Belgium and Luxembourg are known as the only two countries, not just in Europe, but in the world, to have banned facial recognition. Even though there is no law in Belgium regulating the use of FRT by the government, civil society organisations have observed that the police and the government still (want) to use it, hindering the right to privacy, the right to anonymity, the freedom of movement, association, assembly and demonstration, and the right not to be discriminated against (Democratie Brussels, 2023). FRT has been used several times by the Belgian police, provoking a coalition of organisations to launch the petition "Protect my space" in public spaces (The Brussels Times, 15 March 2023). In November 2022, Italy prohibited the use of FRT until a specific law has been adopted; except where such technologies are used in judicial investigations or the fight against crime (Reuters, 14 November 2022). Many European countries are currently considering enacting legislation that would ban the use of FRT (CaseGuard, 2022).

In response to the concerns of European Parliament members regarding certain developments in facial recognition technologies, the EDPB recalled that under Law Enforcement Directive (EU) 2016/680 law enforcement authorities may process biometric data for the purpose of uniquely identifying a natural person only pursuant to the strict conditions of Articles 8 and 10 of the Directive (EDPB, 10 June 2020). The EDPB issued the opinion that the use of a service like Clearview AI by law enforcement authorities in the European Union would, as it stands, likely not be consistent with the EU data protection regime (EDPB, 10 June 2020).

In line with this EDPB opinion, in 2022 the Italian authorities imposed a fine of EUR 20 million on Clearview AI company for having unlawfully collected and processed biometric and other personal information of persons in the territory of Italy without an appropriate legal basis (EDPB, 10 March 2022). The US-based company was also banned from any further collection and processing and was ordered to erase the data. Based on the same grounds, Clearview AI was fined EUR 20 million in France (EDPB, 20 October 2022) and Greece (EDPB, 20 July 2022).

The Swedish Authority for Privacy Protection also determined that the Swedish Police Authority had processed personal data in breach of the Swedish Criminal Data Act while using Clearview AI to identify individuals (EDPB, 12 February 2021). It was found that when using Clearview AI the Police unlawfully processed biometric data for facial recognition and failed to conduct a data protection impact assessment. The Police was ordered to inform the data subjects whose data had been disclosed to Clearview AI, when the confidentiality rules so allow, and to ensure that any personal data transferred to Clearview AI was deleted. Similarly, the Finish Deputy Data Protection Ombudsman has issued a statutory reprimand to the National Police Board for the illegal processing of special categories of personal data when using facial recognition software (EDPB, 7 October 2021). The Finish National Police Board was ordered to notify the data subjects of the personal data breach and to demand that Clearview AI erase the data transmitted by the police from its storage platforms.

In the Netherlands, the Data Protection Authority has issued a formal warning to a supermarket for its use of facial recognition technology, even though facial recognition technology has been banned for uses outside the home since December 2019 (EDPB, 26 January 2021). Facial recognition used to monitor the attendance of students at a school was a basis for the Swedish Data Protection Authority to impose a fine on the local municipality responsible for the school (EDPB, 22 August 2019). The Data Protection Authority concluded that the school had processed sensitive biometric data unlawfully and failed to prepare an adequate impact assessment. In 2016, the European Commission for Justice warned the Maltese government that the planned deployment of a Safe City CCTV network with FRT would need to undergo a data protection impact assessment and comply with EU law (Biometric Update, 8 April 2019).

Many European human rights organisations have also pointed to the numerous severe harms that biometric mass surveillance entails, demanding a ban on the use of this technology in public spaces (EDRI). A coalition of parliamentarians and human rights organisations in the United Kingdom has called on the Frasers Group to end its use of facial recognition surveillance in its stores (Big Brother Watch, 24 April 2023). British human rights organisations have also expressed the concern that "live FRT would turn citizens into walking ID cards" (Big Brother Watch, 6 April 2023). Similarly, people across Switzerland (Reclaim Your Face, 30 November 2021) and Italy (Reclaim Your Face, 14 July 2022) have taken a stand in support of human rights and are opposed to any expansion of FRT mass surveillance.

This brief overview of the position of the EU member states and their data protection authorities regarding the use of facial recognition software in surveillance systems indicates that they are seeking to develop robust human rights safeguards to regulate such practices, whereas civil society demands a ban on FRT mass surveillance.

Discussion

The UN and the EU data protection authorities agree that the use of FRT surveillance brings clear risks for the enjoyment of some basic human rights and freedoms, including the rights to privacy, protection of personal data and freedom of peaceful assembly. Thus, they stress the importance of establishing a strong national legislative framework in this area. In 2022, the UN High Commissioner for Human Rights noted that "biometric recognition systems should only be used in public spaces to prevent or investigate serious crimes or serious public safety threats and if all requirements under international human rights law are implemented".[3]

While states are tending to develop relevant regulation, there are growing demands from civil society and human rights organisations worldwide to ban FRT use. Scholars also hold different positions on this aspect. Only a few authors argue that the use of FRT should be prohibited. For example, Barrett (2020) insists that the use of this technology for children should be banned, but also for everyone else. The majority of authors, such as Nakar and Greenbaum (2017), Sarabdeen (2022) and Dushi (2020), are in favour of adopting adequate regulation. Sarabdeen (2022: 6) underlines that the current telecommunication and criminal law has "failed to address the technology induced crimes and breaches", and hence "it is necessary to criminalise the unauthorised use, storage and communication of images through FRT". He concludes that the passing of appropriate laws is inevitable given that the existing laws are inadequate for regulating the use of FRT by government and commercial organisations (Sarabdeen, 2022).

In its report published in 2020, the Fundamental Rights Agency (FRA) highlights that it is essential to consider procedural rights when FRT is used by public administrations, including the rights to good administration, to an effective remedy, and to a fair trial (FRA, 2020: 33). The FRA considers that FRT may be used in public spaces if the deployment of such technology is assessed to be necessary and proportionate (FRA, 2020: 34). A study by Nakar and Greenbaum (2017) is a classic study that researches almost every aspect of FRT and the growing lack of privacy, researching in the same time legal framework for the use of FRT, especially in the USA and Europe, and universal concerns with FRT in their ethical and legal aspects. Nakar and Greenbaum observe that there is no definite consensus even in the industry and among stakeholders over different recommendations and instructions for how to use FRT, and that it is essential that the government step up and provide the regulation (Nakar and Greenbaum, 2017: 123).

Many other authors warn of the risks that FRT use imposes on individuals and their basic rights and freedoms (Lai and Rau, 2021; Lynch, 2020; Barrett, 2020; Hamman and Smith, 2019; Hirose, 2016; Introna and Nissenbaum,

[3] *United Nations Office of the High Commissioner for Human Rights. Interactive dialogue with the High Commissioner on the report identifying recent trends and challenges with regard to the human right to privacy. 16 September 2022. Accesible at https://www.ohchr.org/en/speeches/2022/09/interactive-dialogue-high-commissioner-report-identifying-recent-trends-and, 5. 5. 2023.*

2010; Dushi, 2020; Brey, 2004). In her article that includes a "Non-Orwellian draft legal proposal", Raposo (2020) advocates

> *the creation of a specific law on the use of facial recognition technology for identification in law enforcement, based on existing regulations, to specifically address the pressing issues arising in this domain, with the ultimate aim to allow its use under certain conditions and to protect the rights of the people involved, but also to provide law enforcement authorities with the necessary tools to combat serious crimes.*

In their comparative analysis of video surveillance regulation in data protection laws in the former states of Yugoslavia, Krivokapić et al. (2020) conclude that it will be difficult to implement novel regulations on video surveillance based on the new technology due to its considerable potential to violate fundamental human rights. Crawford (2019) argues that there is a need for a moratorium on this technology until appropriate safeguards are put in place. Madiega and Mildebrath (2021: 1) warns that "even if courts attempted to close gaps in protection through an extensive interpretation of the pre-existing legal framework, legal uncertainties and complexities would remain".

The overview of the standpoints of authors with respect to this problem indicates that, despite their different views, they agree on the great potential of FRT surveillance to violate basic human rights and freedoms. They also agree that it is difficult to monitor the implementation of regulation, prevent abuses and sanction violators.

We contend that no regulation, no matter how strict, can prevent the misuse and abuse of this sophisticated AI technology. In support of this claim, we argue as follows:

- There is no efficient mechanism thus far to ensure democratic control of the controllers and the FRT operators in charge of the processing, storing and use of collected photos and other data, especially regarding live surveillance in public spaces. While a legal framework may foresee organisational, technical and personnel protection measures aimed at preventing the violation of human rights and freedoms, there is no efficient way to monitor whether are they being implemented properly, lawfully and ethically.
- The performance of AI algorithms has been developing at a fast pace, while the use of this technology has also been widening rapidly. Face recognition accuracy was increased with mask-aware face recognition system, developed during COVID-19 pandemic, that can identify persons with or without facial mask presence. Face Emotion Recognition software, the process of mapping facial expressions to identify emotions, is

also in growing use, as are other technologies related to speech recognition, sound identification etc. The quick development of this technology means that gaps in legislation may be expected, along with an increase in risks of the violation of human rights and freedoms.

- Putting the face of an individual into a search engine creates the possibility that their face could be linked to their name and other personal data by cross-checking the face with their social media profile. This and similar types of cross-checking of data using AI algorithms cannot be prevented, thus there is a high risk of the collected data being abused.
- As a rule, scanning the faces of individuals is done without their consent. Even if they had been warned that they were being watched, mass general surveillance causes 'chilling effects' and the substantial erosion of privacy and other rights and freedoms.
- There is no reasonable justification to use FRT surveillance in stores, parks and other public spaces, except when everyone is considered to be a potential criminal. This is unacceptable and in fact contrary to international human rights law.
- Even if law enforcement officials and controllers of surveillance fully obey the legal and ethical norms, the danger of cyberattacks and hacking is high. It is very difficult, if not impossible, to protect software and database from a cyberattack outside of the system. This fact adds to the high risk of recorded and stored data being misused.
- Finally, it should be considered that the development of facial recognition software and video surveillance cameras has become a profitable business. The facial recognition market is soaring and dominated by key players like 3M, Microsoft Corporation, IBM Corporation, Panasonic Corporation, Cognitec System GmbH, FaceFirst Inc., and Fijutsu Limited (Expert Market Research, 2022). Many of these corporations are more powerful than states, contributing to concerns with the rational use of this technology: is it about the security of citizens and preventing crimes, creating room for corporations to make big profits, or about establishing authoritarian control over citizens? In any case, the benefits for 'ordinary' citizens may be questioned.

Conclusion

The rapid development and use of FRT surveillance systems raises unprecedented issues from the perspective of the protection of personal data and other human rights and freedoms. On the other hand, no evidence could be found that laws may provide safeguards against the misuse of FRT surveillance in public spaces and ensure democratic control over it. The UN and EU are seeking to develop robust human rights safeguards to regulate these practices, while civil society is demanding a complete ban on this practice.

The overview of the state of play in this area permits the conclusion that the right to privacy, protection of personal data, freedom of expression and freedom of assembly face greater risks than ever before. It is particularly disturbing and 'chilling' that sophisticated modern data-driven technologies create possibilities for state and private actors "to operate at a scale never before possible, obtaining and storing massive amounts of private data, and targeting communities, neighbourhoods and groups".[4] These new technologies have shifted the balance of power between of those doing the monitoring and those being monitored. Besides, the mass use of this type of technology facilitates various types of violations and restrictions of human rights and freedoms that are difficult, if not impossible, to prevent by legal means. Those being monitored may be unaware of it, meaning that they may not be aware that their privacy, private data or other human rights are being violated or abused. It is also difficult to impose a democratic control mechanism on multinational corporations and private entities to ensure their proper and lawful use of FRT. If state actors rely on this type of 'smart' surveillance, it is also difficult to prevent abuse and to pinpoint 'a legitimate aim' and 'the public interest' of using FRT in each case.

We therefore argue that regulation can only limit the risks of FRT use, but not prevent them. Further, developing regulation in this area, no matter how restrictive, amounts to tacit approval of the mass use of a type of technology that opens the door to various types of abuses and restrictions on human rights and freedoms, and whose justification from the perspective of the public interest may be questioned.

BIBLIOGRAPHY

Auxer, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner (2019): Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research Center. Accessible at https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/, 20. 4. 2023.

Barrett, Lindsey (2020): Ban Facial Recognition Technologies for Children – And for Everyone Else. Boston University Journal of Science and Technology Law 26 (2): 223–285.

[4] *United Nations office of the High Commissioner for Human Rights. Interactive dialogue with the High Commissioner on the report identifying recent trends and challenges with regard to the human right to privacy. 16 September 2022. Accessible at: https://www.ohchr.org/en/speeches/2022/09/interactive-dialogue-high-commissioner-report-identifying-recent-trends-and, 5. 5. 2023.*

Becuywe, Mathias, Tatiana Beliaeva, Stephanie Beltran Gautron, Theodore Christakis, Maeva El Bouchikhi and Agnes Guerraz (2022): Landscape of Start-ups Developing Facial Recognition. Analysis and Legal Considerations. AI-Regulation.com, 27–31.

Brey, Philip (2004): Ethical Aspects of Facial Recognition Systems in Public Places. Journal of Information, Communication and Ethics in Society 2 (2): 97–109.

Crawford, Kate (2019): Halt the Use of Facial-recognition Technology Until It Is Regulated. Nature 572 (7771): 565–566.

Duroy, Sophie (2023): Big Brother is Watching the Olympic Games – and Everything Else in Public Spaces. VerfBlog, 3–22.

Dushi, Desara (2020): The use of facial recognition technology in EU law enforcement: Fundamental rights implications.

European Union Agency for Fundamental Rights (FRA) (2020): Facial recognition technology: fundamental rights considerations in the context of law enforcement. Vienna: FRA.

Hirose, Mariko (2016): Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology. Connecticut Law Review 49: 1591.

Introna, Lucas and Helen Nissenbaum (2010): Facial recognition technology a survey of policy and implementation issues. Working Paper. The Department of Organisation, Work and Technology, Lancaster University.

Karlovšek, Bien, Sonja, Alenka Jerše, Klemen Mišić, Nataša Pirc Musar, Jasna Rupnik and Andrej Tomšić (2008): Zasebnost delavcev in interesi delodajalcev – kje so meje? Ljubljana: Uradni list Republike Slovenije.

Kostka, Genia, Lea Steinacker and Miriam Meckel (2023): Under Big Brother's Watchful Eye: Cross-Country Attitudes Toward Facial Recognition Technology. Government Information Quarterly 40: 1–20.

Krivokapić, Đorđe, Danilo Krivokapić, Jelena Adamović and Aleksandra Stefanović (2021): Comparative Analysis of Video Surveillance Regulation in Data Protection Laws in the Former Yugoslav States. Journal of Regional Security 16 (1): 5–26.

Lai, Xiaojun and Pei-Luen Patrick Rau (2021): Has Facial Recognition Technology Been Misused? A Public Perception Model of Facial Recognition Scenarios. Computers in Human Behavior 124.

Lynch, Jennifer (2020): Face off: Law enforcement use of face recognition technology.

Madiega, Tambiama and Hendrik Mildebrath (2021): Regulating facial recognition in the EU: In-depth analysis. Brussels: European Parliamentary Research Service.

Nakar, Sharon and Dov Greenbaum (2017): Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy. Boston University Journal of Science and Technology Law 23: 88–123.

Rainie, Lee, Cary Funk, Monica Anderson and Alec Tyson (2022): Public more likely to see facial recognition use by police as good, rather than bad for society, 17 March. Pew Research Center. Accessible at https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/, 20. 4. 2023.

Raposo, Vera Lucia (2022): The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal. European Journal on Criminal Policy and Research.

Sarabdeen, Jawahitha (2022): Protection of the Rights of the Individual When Using Facial Recognition Technology. Heliyon 8 (3).

TELEFI Project (2020): Towards the European Level Exchange of Facial Images – Legal Analysis for TELEFI project. 7 February, 40–190. Accessible at https://www.telefi-project.eu/sites/default/files/TELEFI_LegalAnalysis.pdf, 10. 3. 2023.

TELEFI Project (2021): Summary Report of the project "Towards the European Level Exchange of Facial Images". Accessible at https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf, 10. 3. 2023.

United Nations Office of the High Commissioner for Human Rights. Artificial intelligence risks to privacy demand urgent action – Bachelet, 15 September 2021. Accessible at https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet, 28. 4. 2023.

SOURCES

Altaf, Yasin (2022): Your Face is the Future of Targeted Marketing. Here's Why Businesses Should Use Facial Recognition, 14 October. Accessible at https://www.entrepreneur.com/science-technology/facial-recognition-the-future-of-targeted-marketing/437103, 16. 4. 2023.

Amnesty International (2021): Amnesty International and more than 170 organisations call for a ban on biometric surveillance, 7 June. Accessible at https://www.amnesty.org/en/latest/press-release/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/, 24. 4. 2023.

Amnesty International (2021a): Ban dangerous facial recognition technology that amplifies racist policing. Amnesty International, 26 January. Accessible at https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/, 10. 3. 2023.

Barker, Phillip (2023): French Greens and France Unbowed launch challenge to Olympic surveillance. Inside the Games, 18 April. Accessible at https://www.insidethegames.biz/articles/1136044/french-surveillance-law-paris-2024, 3. 5. 2023.

Big Brother Watch (2023): ITV News – live facial recognition tech will turn us into walking ID cards, 6 April 2023. Accessible at https://bigbrotherwatch.org.uk/2023/04/itv-news-live-facial-recognition-tech-will-turn-us-into-walking-id-cards/, 5. 5. 2023.

Big Brother Watch (2023): Parliamentarians and rights groups call on Frasers Group to drop facial recognition cameras, 24 April. Accessible at https://bigbrotherwatch.org.uk/2023/04/parliamentarians-and-rights-groups-call-on-frasers-group-to-drop-facial-recognition-cameras/, 5. 5. 2023.

Biometric Update (2019): EU Commissioner warns Malta public facial recognition plan may not meet legal requirements, 8 April. Accessible at https://www.biometricupdate.com/201904/eu-commissioner-warns-malta-public-facial-recognition-plan-may-not-meet-legal-requirements, 14. 3. 2023.

Bischoff, Paul (2022): Facial recognition around the world, 24 January. Accessible at https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/, 18. 9. 2023.

CaseGuard (2022): Efforts to Ban Facial Recognition in Europe Gain New Steam. 22 September. Accessible at https://caseguard.com/articles/efforts-to-ban-facial-recognition-in-europe-gain-new-steam/, 27. 4. 2023.

Clearview AI. Accessible at https://www.clearview.ai, 10. 2. 2023.

Council of Europe. 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. Convention 108. Guidelines on Facial Recognition of 28 January 2021. T-PD(2020)03rev4.

Democratie Brussels. Pour l'interdiction de la reconnaissance faciale à Bruxelles. Pétition. Accessible at https://democratie.brussels/initiatives/i-155, 28. 4. 2023.

European Center for Non-for-Profit Law (2021): Civic voices heard: european parliament calls for facial recognition ban, 15 October. Accessible at https://ecnl.org/news/civic-voices-heard-european-parliament-calls-facial-recognition-ban, 24. 4. 2023.

European Center for Non-for-Profit Law (2023): Civil society open letter on the proposed French law on the 2024 Olympic and Paralympic Games. 1 March. Accessible at https://ecnl.org/news/civil-society-open-letter-proposed-french-law-2024-olympic-and-paralympic-games#:˜:text=Article%207%20of%20the%20proposed,to%20explicitly%20legalise%20such%20practices, 3. 3. 2023.

European Center for Non-for-Profit Law (2023): Civil society shares external contribution with the French constitutional council as it reviews the Olympics Law. 25 April. Accessible at https://ecnl.org/news/civil-society-shares-external-contribution-french-constitutional-council-it-reviews-olympics, 3. 5. 2023.

European Data Protection Board (EDPB) (2019): Facial recognition in school renders Sweden's first GDPR fine, 22 August. Accessible at https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en, 10. 4. 2023.

European Data Protection Board (EDPB) (2020): EDPB response to MEPs Sophie in 't Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI, 10 June. Accessible at https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf, 20. 4. 2023.

European Data Protection Board (EDPB) (2020): Thirty-first Plenary session: Establishment of a taskforce on TikTok, Response to MEPs on use of Clearview AI by law enforcement authorities, Response to ENISA Advisory Group, Response to Open Letter NYOB. 10 June. Accessible at https://edpb.europa.eu/news/news/2020/thirty-first-plenary-session-establishment-taskforce-tiktok-response-meps-use_en, 27. 4. 2023.

European Data Protection Board (EDPB) (2021): Dutch DPA issues Formal Warning to a Supermarket for its use of Facial Recognition Technology. 26 January.

Accessible at https://edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_en, 10. 4. 2023.

European Data Protection Board (EDPB) (2021): EDPB and EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination, 21 June. Accessible at https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en, 21. 4. 2023.

European Data Protection Board (EDPB) (2021): Finnish SA: Police reprimanded for illegal processing of personal data with facial recognition software, 7 October. Accessible at https://edpb.europa.eu/news/national-news/2021/finnish-sa-police-reprimanded-illegal-processing-personal-data-facial_en, 28. 4. 2023.

European Data Protection Board (EDPB) (2021): Swedish DPA: Police unlawfully used facial recognition app, 12 February. Accessible at https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en, 20. 4. 2023.

European Data Protection Board (EDPB) (2022): Facial recognition: Italian SA fines Clearview AI EUR 20 million, 10 March. Accessible at https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en, 27. 4. 2023.

European Data Protection Board (EDPB) (2022): Hellenic DPA fines Clearview AI 20 million euros, 20 July. Accessible at https://edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en, 27. 4. 2023.

European Data Protection Board (EDPB) (2022): The French SA fines Clearview AI EUR 20 million, 20 October. Accessible at https://edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en, 27. 4. 2023.

European Digital Rights (EDRI) (2020): Campaign “Reclaim Your Face” calls for a Ban on Biometric Mass Surveillance, 12 November. Accessible at https://edri.org/our-work/campaign-reclaim-your-face-calls-for-a-ban-on-biometric-mass-surveillance/, 5. 4. 2023.

European Digital Rights (EDRI): Ban Biometric Mass Surveillance – A set of fundamental rights demands for the European Commission and EU Member States. Brussels: EDRI. Accessible at https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf, 3. 11. 2022.

Expert Market Research (2022): Top 10 Companies in the Global Facial Recognition Market, Driven by Increasing Data Security Initiatives, 27 November. Accessible at https://www.expertmarketresearch.com/articles/top-facial-recognition-companies, 6. 5. 2023.

Forbes (2022): 11 Areas in Which Facial Recognition Technology Is (Or Will Be) Being Used, 15 September. Accessible at https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/where-facial-recognition-used, 20. 4. 2023.

La Quadrature du Net (2023): France becomes the first European country to legalize biometric surveillance, 29 March. Accessible at https://www.laquadrature.

net/en/2023/03/29/france-becomes-the-first-european-country-to-legalize-biometric-surveillance/, 30. 4. 2023.

New York Times (2020): The Secretive Company that Might End Privacy as we Know It, 18 January. Accessible at https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html, 20. 4. 2023.

Reclaim Your Face (2021): People across Switzerland reclaim their faces and public spaces! 30 November. Accessible at https://reclaimyourface.eu/switzerland-action/, 5. 5. 2023.

Reclaim Your Face (2022): Week of actions: Reclaim Your Face Italy and the need for a real EU ban on biometric mass surveillance, 14 July. Accessible at https://reclaimyourface.eu/week-of-actions-reclaim-your-face-italy-and-the-need-for-a-real-eu-ban-on-biometric-mass-surveillance/, 5. 5. 2023.

Reuters (2023): Italy outlaws facial recognition tech, except to fight crime, 14 November. Accessible at https://www.reuters.com/technology/italy-outlaws-facial-recognition-tech-except-fight-crime-2022-11-14/, 27. 4. 2023.

The Brussels Times (2023): 'Protect my face': Facial recognition petition demands ban in Brussels public spaces, 15 March. Accessible at https://www.brusselstimes.com/407531/protect-my-face-anti-facial-recognition-petition-demands-ban-in-brussels-public-spaces, 28. 4. 2023.

The EU Artificial Intelligence Act. Accessible at https://www.artificial-intelligence-act.com, 1. 03. 2023.

United Nations Office of the High Commissioner for Human Rights. Türk addresses World Standards Cooperation meeting on human rights and digital technology, 24 February 2023. Accessible at https://www.ohchr.org/en/statements/2023/02/turk-addresses-world-standards-cooperation-meeting-human-rights-and-digital, 28. 4. 2023.

United Nations office of the High Commissioner for Human Rights. Interactive dialogue with the High Commissioner on the report identifying recent trends and challenges with regard to the human right to privacy, 16 September 2022. Accessible at https://www.ohchr.org/en/speeches/2022/09/interactive-dialogue-high-commissioner-report-identifying-recent-trends-and, 5. 5. 2023.

University of Miami News (2020): New facial recognition software 'scrapes' inventory from social media. Accessible at https://news.miami.edu/stories/2020/02/new-facial-recognition-software-scrapes-inventory-from-social-media.html, 20. 4. 2023.

Wolf, Max (2023): 54+ Facial Recognition Statistics, Facts, and Trends. 31 January. Accessible at https://passport-photo.online/blog/facial-recognition-statistics/, 19. 4. 2023.