Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world

Irena Nesterova[1,*]

[1]University of Latvia, Faculty of Law, 19 Raina Blvd., Riga, Latvia

Abstract. The growing use of facial recognition technologies has put them under the regulatory spotlight all around the world. The EU considers to regulate facial regulation technologies as a part of initiative of creating ethical and legal framework for trustworthy artificial intelligence. These technologies are attracting attention of the EU data protection authorities, e.g. in Sweden and the UK. In May, San Francisco was the first city in the US to ban police and other government agencies from using facial recognition technology, soon followed by other US cities. The paper aims to analyze the impact of facial recognition technology on the fundamental rights and values as well as the development of its regulation in Europe and the US. The paper will reveal how these technologies may significantly undermine fundamental rights, in particular the right to privacy, and may lead to prejudice and discrimination. Moreover, alongside the risks to fundamental rights a wider impact of these surveillance technologies on democracy and the rule of law needs to be assessed. Although the existing laws, in particular the EU General Data Protection Regulation already imposes significant requirements, there is a need for further guidance and clear regulatory framework to ensure trustworthy use of facial recognition technology.

1 Introduction

Artificial intelligence has the potential to transform society, solve global problems and bring great benefits in many areas, however it also raises serious challenges. One of the serious concerns is about the growing use of surveillance technologies both by public authorities and private entities that may significantly undermine fundamental rights. European countries, for example, the United Kingdom (the UK), Germany and France are testing these technologies that have sparked a great concern about the over-abusive use of such privacy intrusive measures [1]. There is expected to be a rapid advancement of facial recognition technologies that will make it possible to match faces recorded on video taken from surveillance cameras installed in public places against biometric pictures stored in IT systems [2]. These technologies are under the regulatory spotlight all around the world.

The EU intends to regulate facial regulation technologies as a part of initiative of creating ethical and legal framework for trustworthy artificial intelligence [3]. These

[*] Corresponding author: Irena.nesterova@lu.lv

technologies are also attracting attention of the EU data supervision authorities. On August 20 this year, the Swedish data protection authority issued the decision [4] finding that a school that used facial recognition technology to monitor the attendance of students has violated the General Data Protection Regulation (the GDPR) [5]. On August 15, the Information Commissioner's Office, the UK's data protection authority has launched an investigation regarding the use of live facial recognition in the King's Cross area of central London [6].

The restriction of facial recognition technologies is on the top of regulatory agenda not only in Europe, but also across the Atlantic. In May, San Francisco was the first United States (the US) city to ban police and state authorities from using facial recognition technology, soon followed by other US cities [7].

The paper aims to analyze the negative impact of facial recognition technologies on the fundamental rights and values that reveals the need for a clear regulation of the use of these technologies. Further, the paper discusses the development of facial recognition regulation in Europe and across the Atlantic. The development of artificial intelligence, including facial recognition technologies has to be based on the existing laws. The paper analyses the legal obligations and restrictions on the use of facial recognition technologies imposed by the GDPR. It argues that existing legal requirement are not sufficient and there is a need for further guidance and a clear regulatory framework to ensure trustworthy use of facial recognition.

2 The main concerns of facial recognition technologies

There is a growing use of facial recognition technologies both in public and private sector. Facial recognition as biometric authentication technology lets users of latest smartphones to unlock their devices and some banks use it to authorise transactions. Airports all around the world, including in Europe, are testing the use facial recognition for scanning passengers to speed up boarding.

Facial recognition is also increasingly used by police and other law enforcement agencies to ensure security and combat terrorism all around the world. Several European countries, such as France, Germany and, in particular, the UK are testing these technologies to identify criminals and terrorists in public places [1]. However, these mass surveillance measures are not regulated by national laws and raises concerns among civil liberties advocates, researchers and government officials [8].

The use of surveillance technologies significantly undermines fundamental rights, in particular the right to privacy and data protection. Privacy gives us a personal sphere in which we can exercise our autonomy, feel free in thoughts and actions, that would not be possible under the constant risk of observation [9, 10].

Alongside the loss of privacy, there is also the risk of artificial intelligence technology-induced bias that can lead to prejudice and discrimination against certain groups or individuals. The performance and results of artificial intelligence systems are strongly dependent on the quality of the data sets used, which can reflect biases, inaccuracies, errors and mistakes in the data gathering processes [11]. Studies have been conducted showing that artificial intelligence algorithms in facial recognition technologies work differently based on the age, gender and ethnicity of the person being identified [12, 8]. Moreover, as facial recognition technologies processes biometric data, they create significant security risks that is hard or currently even impossible to predict [13].

The use of facial recognition technologies presents not only risks to security and undermine fundamental rights, but they may also have negative impact which is difficult to anticipate and identify, including on democracy and the rule of law. Unavoidable surveillance by tech giants and governments brings serious threat to a society powered by free autonomous citizens making their own choices and actions based on their free will that is essential to democracy [14].

While surveillance technologies can be seen as powerful tool for law enforcement authorities to find suspects and fight terrorism, they can also be used to control people. Besides, security expert *Schneier* points out that data mining techniques used for surveillance are not proved to be an effective tool for fighting with terrorism, however they are much more suitable for other purposes such as social control, manipulation, discrimination and even creating a digital dictatorship [15]. The use of facial recognition technologies for mass surveillance by police authorities is compared to China's digital mass surveillance system powered by artificial intelligence and facial recognition, in combination with "social credit" system [16].

In April this year, the High-Level Expert Group on Artificial Intelligence (the AI HLEG) created by the European Commission published the Ethics Guidelines for Trustworthy artificial intelligence (the Guidelines) that draws attention to critical concerns raised by artificial intelligence. The AI HLEG states that automatic identification, including face recognition and other involuntary methods of identification using biometric data, i.e. lie detection, personality assessment through micro expressions, and automatic voice detection, "raises strong concerns of a both a legal and ethical nature as it may have an unexpected impact on many psychological and sociocultural level. The AI HLEG also emphasises that another critical concern raised by artificial intelligence is citizen scoring that can lead to the loss of this autonomy and endanger the principle of non-discrimination. [11]. European Parliament expresses great concern about the employment of artificial intelligence applications, including facial and voice recognition, in 'emotional surveillance' programmes, i.e. monitoring the mental conditions of workers and citizens in order to increase productivity and preserve social stability and stresses that such programmes are inherently at odds with European values and norms protecting the rights and freedoms of individuals [17].

In order to achieve trustworthy artificial intelligence and facial recognition, it is crucial to clearly define if, when and how artificial intelligence can be used for automated identification of individuals differentiating between the identification of an individual vs. the tracing and tracking of an individual, and between targeted surveillance and mass surveillance [11].

3 The development of facial recognition regulation

Artificial intelligence, including facial recognition technologies are already regulated by existing legal requirements at European, international and national level. The development, deployment and use of artificial intelligence systems must comply with the fundamental rights enshrined in the international and EU human rights instruments, e.g. the Charter of Fundamental Rights of the European Union (the Charter) [18]. Any interference with the fundamental rights requires a strict necessity and proportionality test [19]. According to Article 52 (1) of the Charter, limitations may be imposed on the exercise of fundamental rights and freedoms as long as they are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others. The use of facial recognition may entail unjustified interference with fundamental rights, in particular the right to privacy that goes beyond what is strictly necessary for the protection of such legitimate aims as security and public safety.

The development and use of facial recognition technologies must comply both with existing laws and ethical principles grounded in fundamental rights [20]. The AI HLEG

Guidelines state that trustworthy artificial intelligence has three components: 1) it should be lawful, complying with all applicable laws and regulations; 2) it should be ethical, ensuring adherence to ethical principles and values; and 3) it should be robust, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm. The Guidelines identify four ethical principles that should be adhered to in order to ensure ethical and robust AI: 1) respect for human autonomy; 2) prevention of harm; 3) fairness; and 4) explicability. Moreover, the Guidelines list seven key requirements that AI systems should implement and meet throughout their entire life cycle: (1) human agency and oversight; (2) technical robustness and safety; (3) privacy and data governance; (4) transparency; (5) diversity, non-discrimination and fairness; (6) environmental and societal well-being; and (7) accountability [11].

In addition to fundamental rights and ethical principles, the development and use of artificial intelligence technologies must comply with other legal requirements laid down in EU and national legislation, in particular in data protection laws. Facial recognition systems involve processing of biometric data that entails higher risks to individuals' fundamental rights and freedoms and therefore merits higher protection.

The GDPR provides additional requirements and restrictions to the use of special categories of personal data, including biometric data. The GDPR defines biometric data as "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" (Article 4 (14)). When processing biometric data, it is particularly important to respect all data protection principles forming the basis for all the other data protection requirements: - lawfulness, fairness and transparency; - purpose limitation; - data minimisation; - integrity and transparency, - accuracy; - storage restrictions; - integrity and confidentiality; - accountability (Article 5 of the GDPR). The EDPB also emphasises that it is crucial that the use of biometric technologies comply with the principles set forth in the GDPR [11].

One of the most significant principles that must be considered before deciding whether to use facial recognition is purpose limitation principle. It requires that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Article 5 (1) (b) of the GDPR). In June this year, the EDPB adopted the Guidelines on processing of personal data through video surveillance. They stress that "[w]hereas 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" [12]. In August, the Swedish data protection authority issued its first GDPR fine finding that monitoring the attendance of students cannot be considered a legitimate aim that justifies the use of facial recognition technologies in school [4].

The European Data Protection Board (the EDPB) draws attention that "[v]ideo surveillance is not by default a necessity when there are other means to achieve the underlying purpose. Otherwise we risk a change in cultural norms leading to the acceptance of lack of privacy as the general outset" [12]. These considerations even to a greater extend apply to surveillance systems that use facial recognition.

Article 9 (1) of the GDPR generally prohibits the processing of special categories of data, including biometrical data, unless one of the exceptions listed in Article 9 (2) of the GDPR applies. In most cases, private companies have to obtain the "explicit consent" for the use of facial recognition technologies. Consent must be obtained in a proper manner and meet all criteria laid down in the GDPR, i.e. it must be freely given, specific, informed and unambiguous (Article 4 (11), (7)). The EDPB emphasises that the data controller shall not condition the access to its services to the acceptance of the biometric processing and when such processing is used for authentication purpose, the data controller must offer an alternative solution that does not involve biometric processing - without restraints or additional cost for the data subject [12].

When processing biometric data, it is essential to respect all the other principles and requirements set by the GDPR, such as obligation to provide information to data subjects about the use of these technologies and the processing of data and to ensure the protection of other rights of data subject, to implement appropriate security measures etc.

Before implementing facial recognition technologies, the controller must carry out a data protection impact assessment (DPIA). The GDPR imposes an obligation to carry out DPIA where the type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of persons (Article 35 (1)). The set criteria for considering whether the DPIA needs to be carried out, in particular the use of new technologies, are to a great extend applicable to the use of facial recognition technologies. The GDPR states that DPIA is in particular required in the case of processing on a large scale of special categories of data (Article 35 (3) (b)) as well as a systematic monitoring of a publicly accessible area on a large scale (Article 35 (3) (c)). Facial recognition technologies involve processing of biometric data and their use may involve monitoring of public space. According to Article 36 of the GDPR, the controller shall consult the supervisory authority prior to processing where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures. It is predictable that national data protection authorities as well as the EDPB will be more and more frequently asked for opinion and will have to adopt decisions on the use of new technologies, including facial recognition technologies.

EU plays a leading role in the world in data protection, as it has set very high standards, in particular in the GDPR. Following the adoption of the GDPR, many countries around the world have introduced new privacy and data protection laws, e.g. Australia and Japan [21]. The restriction of the use of facial recognition technologies is on the top of regulatory agenda not only in Europe, but in other parts of the world.

In the US there is no comprehensive legislation regulating the use of personal data, including biometrical data and facial recognition. There are only some sector-specific laws and laws focusing on particular types of data. However, there are significant changes on the state-level [22]. In May, San Francisco was the first US city to ban police and other government agencies from using facial recognition technology, soon followed by other US cities, i.e. Oakland and Somerville [7].

Few US states, e.g. Illinois, Washington and Texas, have adopted biometric legislation. The Illinois Biometric Information Privacy Act sets the highest standarts. In contrast to the GDPR, the Act doesn’t prohibit the processing of biometric data at the outset. However, it sets many requirements to private entities, including obligation to obtain consent and provide information to persons before collecting or disclosing of biometric data, to implement security measures, to destroy data after the purpose of collection ends etc. The act is currently under revision of Senate and has been the subject of many court cases [23].

After the GDPR, several US states have introduced new privacy acts with California leading the way. In January 2020 the California Consumer Privacy Act (the CCPA) [24] becomes effective, that explicitly covers biometric data, including facial recognition, and sets significant legal requirements and grants data subjects a wide range of rights, such as the right to information. However, unlike the GDPR, the CCPA doesn’t create more protective regime for biometric data.

Data protection legislation, although very important, could not be enough to eliminate all the risks raised by the use of facial recognition technologies. For example, the DPIA only requires the assessment of the risks to the rights and freedoms of the data subjects, while a wider impact of facial recognition technologies on society and democracy have to be assessed [25]. The data protection requirements don't include obligation for testing for accuracy and unfair bias as well as don't regulate the scope of state surveillance.

Therefore, there is an urgent need for further guidelines and regulation on the use of facial recognition technologies by private and public actors both in Europe and the US. Like the US states, the EU member states are allowed to introduce further conditions and limitations with regard to the processing of biometric data (Article 9 (4)). However, taken the importance of the concerns raised by the use of these technologies as well as state mass surveillance a common position needs to be adopted both on EU and global level.

4 Conclusions

With the rapid advancement of artificial intelligence, facial recognition technologies are increasingly being used by public authorities for security purposes as well as private companies to promote efficiency. At the same time, the use of facial recognition technologies significantly undermines fundamental rights, in particular the right to privacy and data protection, may lead to discrimination and have an impact on democracy and the rule of law that is hard to predict or measure.

The development and use of facial recognition technologies must comply with fundamental rights and ethical principles grounded in these fundamental rights. The use of facial recognition may entail unjustified interference with fundamental rights, in particular the right to privacy, that goes beyond what is strictly necessary for the protection of such legitimate aims as security and public safety. The use of facial recognition technologies may also conflict with such ethical principles as respect for human autonomy, prevention of harm, fairness, explicability indicated in the AI HLEG Guidelines.

Artificial intelligence, including facial recognition technologies are already regulated by existing legal requirements provided in EU and national data protection legislation, in particular in data protection laws. The GDPR imposes strict requirements and restrictions on the use of facial recognition technologies, as they involve the processing of biometric data and thus present an increased risk to the rights of individuals. When processing biometric data, it is particularly important to respect all the basic principles for processing of personal data laid down in the GDPR. One of the most significant principles is the purpose limitation principle which underpinned the Swedish data protection authority's first GDPR fine for unlawful use of facial recognition technology. It imposes an obligation to assess whether the data processing is strictly necessary and proportionate and whether there are other less restrictive ways to achieve the particular purpose. The principle of lawfulness requires an appropriate legal basis for the use of these technologies, which will in most cases be "explicit consent". The use of facial recognition technologies must also comply with the other requirements set out in the GDPR, such as obligation to provide information about the use of these technologies and the processing of data and to ensure the protection of other rights of data subjects, to implement appropriate security measures and to carry out DPIA.

Data protection and the restriction of the use of facial recognition technologies is on the top of regulatory agenda not only in Europe, but also in the US. In May, San Francisco was the first US city to ban police and other government agencies from using facial recognition technology, soon followed by other US cities. Few US states have adopted biometric legislation as well as introduced new privacy acts with the CCPA leading the way. Although there are significant changes on the state-level, the US lacks comprehensive legislation regulating the use of personal data, including biometrical data and facial recognition.

Enforcing and completing existing data protection legislation, although is crucial, could not be enough to eliminate all the risks raised by the use of facial recognition technologies. Alongside risks to the fundamental rights and freedoms, the wider impact of the use of these technologies on society and democracy must be assessed. In order build trust in facial recognition technologies, there is an urgent need for further guidelines and regulation on the use of facial recognition technologies by both private and public actors. It is important to clearly define if, when and how they can be used, including the requirement for testing for accuracy and unfair bias and limiting state surveillance. Taken the importance of the concerns raised by the use of these technologies as well as state mass surveillance a common position needs to be adopted both on EU and global level.

This work is an output of the research project and has been financially supported by the specific support objective activity 1.1.1.2. "Post-doctoral Research Aid" of the Republic of Latvia (Project No.1.1.1.2/VIAA/1/16/196 "Striking the Right Balance between Privacy and Security in Cyberspace: Building Strong Data Protection Standards across Europe"), funded by the European Regional Development Fund.

References

1. M. Jacob. Facial recognition gains grounds in Europe, among big-brother fears. (20 October, 2017) Available: https://www.euractiv.com/section/data-protection/news/facial-recognition-gains-grounds-in-europe-among-big-brother-fears/
2. H. Hodson. Walking barcodes. *The Economist. The World in 2019*, **123** (2018)
3. M. Khan. EU plans sweeping regulation of facial recognition. (22 August, 2019) Available: https://www.ft.com/content/90ce2dce-c413-11e9-a8e9-296ca66511c9
4. EDPB. Facial recognition in school renders Sweden's first GDPR fine. (22 August, 2019) Available: https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en
5. European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119.
6. ICO. Statement: Live facial recognition technology in King's Cross. (15 August, 2019) Available: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/
7. S. Ravani. Oakland bans use of facial recognition technology, citing bias concerns. (17 July, 2019) Available: https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php
8. M. Madianou. The biometric assemblage: surveillance, experimentation, profit, and the measuring of refugee bodies. *Television & New Media* **20**, no. 6 (2019).
9. H. Nissenbaum, Privacy as Contextual Integrity. *Washington Law Review* **79**, no. 1 (2004).
10. E. Stoycheff, J. Liu, K. Xu, W. Kunto. Privacy and the Panopticon: online mass surveillance's deterrence and chilling effects. *New Media & Society* **21**, no. 3 (2019)
11. AI HLEG. Ethics Guidelines for Trustworthy AI. (2019) Available: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

12. EDPB. Guidelines 3/2019 on processing of personal data through video devices. (2019) Available: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf
13. B. Leong, Facial recognition and the future of privacy: I always feel like horizontal ellipsis somebody's watching me. *Bulletin of the Atomic Scientists* **75**, no. 3 (2019).
14. EDPS. Opinion 3/2018. EDPS Opinion on online manipulation and personal data. (2018) Available: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
15. B. Schneier. *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World.* New York, London: W.W. Norton & Company. 159-164 (2015)
16. F. Liang, V. Das, N. Kostyuk, M. M. Hussain. Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy and Internet* **10**, no. 4 (2018)
17. European Parliament. European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics. (2019) Available: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.html
18. European Union. Charter of fundamental rights of the European Union. Luxembourg: Office for Official Publications of the European Communities. OJ C 364 (2000)
19. D. Murray, F. Pete. Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data. *Israel Law Review* **52**, no. 1 (2019)
20. A.F.T. Winfield, J. Marina. Ethical governance is essential to building trust in robotics and artificial intelligence systems. *Philosophical Transactions of the Royal Society a-Mathematical Physical and Engineering Sciences* **376**, no. 2133 (2018)
21. N. Ashrafi, J.P. Kuilboer. A comparative study of privacy protection practices in the US, Europe, and Asia. *International Journal of Information Security and Privacy* **12,** no. 3 (2018)
22. W.G. Voss, A. H. Kimberly. Personal data and the GDPR: providing a competitive advantage for US companies. *American Business Law Journal* **56**, no. 2 (2019)
23. M. Whitener, R. Aragon. How should we regulate facial-recognition technology? (29 January, 2019) Available: https://iapp.org/news/a/how-should-we-regulate-facial-recognition-technology/
24. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.198(a) (2018)
25. P. Nemitz. Constitutional democracy and technology in the age of artificial intelligence. *Philosophical Transactions of the Royal Society a-Mathematical Physical and Engineering Sciences* **376**, no. 2133 (2018)