Assessment of the European legal framework of facial recognition technology

MANON CAPLIER[1]
TALLINN UNIVERSITY OF TECHNOLOGY, ESTONIA

Abstract: *In an era where half of our face is hidden by a mask, facial recognition technology keeps improving. Despite the opportunities it represents in many fields, this innovative technology is far from winning unanimous support among European citizens and right advocates. Between abuses of use, security drifts and privacy breaches; many risks have been pointed out. The European Union institutions are thus increasingly aware of the importance to provide facial recognition with its own legal framework, so that it is no longer governed solely by the broader framework of data protection legislation.*
Keywords: *artificial intelligence; biometric data; facial recognition technology; remote biometric identification; sensitive data.*

INTRODUCTION

Back in 1975, the French philosopher and historian Michel Foucault already foresaw the electronic surveillance that is currently ongoing in our societies. In his book *Discipline and Punish*, he used the metaphor of the panopticon[2] – a specifically designed prison that enables the guard to monitor all the prisoners without them being able to see if they are being observed or not – to describe a modern technique of observation used in schools, factories, hospitals, and military institutions.[3] This is what led Gilles Deleuze to state, a few years later: "There is no need for science fiction to conceive of a control mechanism that gives the position of an element in an open environment, an animal in a reserve, a man in a company, at every moment".[4] And he got it right.

Indeed, the current state of artificial intelligence technology has made it belong to the "infra-ordinary"[5]; more specifically facial recognition technologies (FRT) and artificial intelligence (AI) software, which are now part of our daily lives. As one all knows, it is possible to use our face to unlock your phone, pay, enter a place or even prevent tiredness while driving. And the use of facial recognition goes much further: it allows the police to identify criminals, brands to adapt their advertising to consumers' facial reactions, universities to track students during remote exams, etc.

Faces are distinctive, difficult to alter and, in most cases, publicly visible; which make them particularly useful for identification purposes.[6] AI software is able to create templates of people out of the characteristics of their face (distance between the eyes, between the nose and the mouth...). Then this unique template is compared with what is available in the database of the software.

[1] TalTech Law School, Tallinn University of Technology, Estonia, manon.caplier@gmail.com
[2] Idea theorised by the English philosopher and social theorist Jeremy Bentham in the late 18th century.
[3] Michel Foucault, *Surveiller et punir*, Paris, Gallimard, 1975.
[4] Maša Galič, Tjerk Timan and Bert-Jaap Koops, "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation" in *Philosophy & Technology*, vol. 30, no. 1, 2017, pp. 9-37.
[5] Georges Perec, *L'infra-ordinaire*, Paris, Seuil, 1989. The infra-ordinary can be seen as a contrary of the 'extra-ordinary'. It the sphere of existence that lies beneath notice or comment, and within which "we sleep through our lives in a dreamless sleep".
[6] Yana Welinder, "A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks" in *Harvard Journal of Law and Technology*, vol. 26, no. 1, Fall 2012, p. 167.

Facial recognition technology is defined in the EU as the "automatic processing of digital images which contain the faces of individuals for identification, authentication/ verification or categorisation of those individuals".[7] The data processed are thus so-called 'biometric data'.

It is essential not to confuse authentication with identification when it comes to the purpose of facial recognition use. On the one hand, authentication is referred to as one-to-one matching. It enables the comparison of two biometric templates, in order to determine if they belong to the same individual. On the other hand, identification means that the template of a person's facial image is compared to many other templates stored in a database to find out if his/her image is stored there. This second application of FRT can be carried out remotely, usually via video cameras (CCTV), and is commonly called 'live facial recognition technology' or 'remote biometric identification'.

The expansion of this omnipresent technology is reflected in the figures: the global facial recognition market size was valued at USD 3.4 billion in 2019 and is anticipated to expand at a CAGR (Compound Annual Growth Rate) of 14.5% until 2027.[8]

Everything can seem to head towards a society based on the concept of "smart city". i.e. a highly efficient system that incorporates disparate sources of data, from drones, cars, roads, tracks (etc.) into a complete and up to date network.[9] This is a dream world for many private companies that promise a simpler, safer, and smoother environment; an ideal shared by some governments who see it as an opportunity to strengthen security.

This innovation, although impressive, and considered by some as a technological revolution, raises many concerns in many legal aspects.[10] Among other issues like discrimination, ethics or accuracy, this paper will focus here on the controversies of FRT from a legal point of view. The question is not whether reasoned use of facial recognition is still possible or whether we are condemned to live in a world where anonymity has disappeared, but to understand how it is handled by the European Union in terms of legislation. The main problem being that this multifaceted technology seems to evolve faster than the rules that govern it.

This research paper seeks to assess the past, current and future legal framework of facial recognition technology in Europe. More precisely, in a first part will be discussed the evolution of this legal framework, to understand the legislation applied at present. The second part will deal with what makes FRT difficult to govern. The third and last part will attempt to provide ideas for improving the situation and overcoming the identified issues.

1. EVOLUTION OF FACIAL RECOGNITION TECHNOLOGY AND ITS GOVERNING RULES IN EUROPE

1.1 First attempts to regulate the processing of biometric data

At the dawn of the 21st century, as information and communication technologies were taking off, European institutions began to address the issue of how the personal data of European citizens were being handled. It is in this perspective that the Article 29 Working Party (WP) was launched in

[7] Opinion 02/2012 on facial recognition in online and mobile services, Article 29 Working Party, 2012, p. 2.

[8] Market Analysis Report entitled "Facial Recognition Market Size, Share & Trends Analysis Report By Technology, By Application, By End Use And Segment Forecasts, 2020 – 2028". Summary retrieved from: https://www.grandviewresearch.com/industry-analysis/facial-recognition-market

[9] G. B. Praveen and Dakala Jayachandra, "Face Recognition: Challenges and Issues in Smart City/Environments" in *12th International Conference on Communication Systems & Networks (COMSNETS)*, 2020, pp. 791-793.

[10] On contract-law matters raised by algorithm-based decision-making see Thomas Hoffmann, „The Impact of Digital Autonomous Tools on Private Autonomy", *Baltic Yearbook of International Law Online*, vol 18, 2020, pp. 18–31; On legal and ethical concerns when applying AI solutions for people with disabilities, please see *e.g.* Joamets, K.; Chochia, A. (2021). Access to Artificial Intelligence for Persons with Disabilities: Legal and Ethical Questions Concerning the Application of Trustworthy AI. *Acta Baltica Historiae et Philosophiae Scientiarum*, 9 (1), 51–66.

1996, to deal with issues relating to the protection of privacy and personal data.[11] At the same period, the Council of Europe was adopting its Convention No.108[12] that was one of the first legally binding international instrument in the data protection field. In the course of the various opinions and reports published in the following years, it has been highlighted that biometric data should be considered as "sensitive" data that presents risks because it contains information about racial and ethnic origin or health.[13] Special safeguards[14] were therefore recommended to be applied in addition to the general data protection principles of the 95/46/EC Directive as well as to assess the sensitivity of data processed by biometric systems, taking into account the context of the processing.

Despite the risks identified, the general data protection framework and most national legislation did not contain specific binding provisions on the use and processing of biometric data, and guidelines remained limited while these technologies were expanding. Nevertheless, some national supervisory authorities have attempted to overcome this, for example by applying the principle of proportionality to determine whether the use of biometrics is proportionate to the legitimate objective sought.[15]

It was not until 2016 that a definition of the term was provided in a legally binding EU act. 'Biometric data' then 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".[16]

1.2 The slow emergence of specific regulations on FRT

Most of the legal texts on the protection of personal data mentioned above refer to artificial intelligence or FRT at some point. For instance, Article 29 Working Party provides a non-exhaustive list of biometric technologies that can be considered as mature technologies, which includes facial recognition (Opinion 3/2012, 4.2). However, very few acts – if not any – specific to facial recognition itself have emerged yet. One can only mention the focus paper issued by the EU Agency for Fundamental Rights (FRA) in 2019 which rather deals with the fundamental rights implications of relying on live FRT rather than how to regulate it from a legal point of view.[17]

The White Paper on Artificial Intelligence published by the European Commission in February 2020 is more relevant as it makes some interesting comments on our topic.[18] According to the commissioners, some AI applications have to be considered as "high-risk" as such (i.e. without any need of "risk-based" assessment[19]) and require the application of some specific requirements in addition to already existing legislation. Among these exceptional instances, one can find the AI applications for purposes of remote biometric identification. The facial recognition technology is

[11] The composition and purpose of Article 29 WP was set out in Art.29 of the Data Protection Directive 95/46/EC. Since the entry into force of the GDPR in 2018, it was replaced by the European Data Protection Board (EDPB).

[12] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), opened for signature on 28 January 1981. Even if the Council of Europe is distinct from the European Union, it is relevant to take its work into account as part of this research paper.

[13] Opinion 3/2012 on developments in biometric technologies, Article 29 WP, 27 April 2012, p. 3 and "Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data" commissioned by the Council of Europe, 2005, p.6.

[14] Provided by article 8 of the Data Protection Directive 95/46/EC.

[15] Els Kindt, "A First Attempt at Regulating Biometric Data in the European Union", chapter 4 of the compendium "Regulating Biometrics: Global Approaches and Urgent Questions" in *AI Now Institute*, 2020, p.63.

[16] Article 4(14) of the General Data Protection Regulation 2016/679 (GDPR) and Article 3(13) of the Directive 2016/680.

[17] FRA Focus, "Facial recognition technology: fundamental rights considerations in the context of law enforcement", 27 November 2019.

[18] White Paper on Artificial Intelligence, "A European approach to excellence and trust", COM/2020/65.

[19] *Ibid*. p.17. A risk-based assessment should be carried out to differentiate between the different AI applications, in order to check whether they are 'high-risk' or not.

therefore part of it, as it deals with the gathering of biometric identifiers (facial images) of multiple persons at a distance, in a public space and in a continuous or ongoing manner and the check of these features against data stored in a database.[20]

At the end of January 2021, the Council of Europe published guidelines on facial recognition addressed to governments, developers, manufacturers, service providers and "entities using FRT".[21] The document is well-detailed and sheds light on the implementation of principles enshrined in European Union law. Although they are not binding, these guidelines help rekindle the debate on the multiple applications of facial recognition and underline the complexity of the subject.

1.3 Current legal framework applicable to the FRT

As facial recognition technology deals with the processing of personal data, it is governed by the current EU data protection rules, namely the GDPR and its law enforcement Directive.[22] The Regulation officially entered into force on 25 May 2018 and the Member States had until 6 May 2018 to transpose the provisions of the directive into their national legislation.

According to the letter of the Regulation, "processing of biometric data for the purpose of uniquely identifying a natural person […] shall be prohibited".[23] This general prohibition is subject to some ten exceptions, exhaustively listed in Article 9(2).

First, processing such a sensitive category of personal data can be lawful when the data subject has given its "explicit consent" to it "for a specific purpose".[24] The notion of consent is defined and clarified several times throughout the text, its main characteristics being that it must be freely given, informed and unambiguous.[25] Recital 43 lays down a relevant exception: it states that consent will be presumed not to have been freely given "in a case where there is a clear imbalance between the data subject and the controller". Even if the provision lacks precision, one can understand that the consent given by an ordinary citizen to a public authority therefore not provides a valid legal basis for the processing of the citizen's data, given the manifest balance of power between the actors involved.

Another main legal ground is when processing is "necessary for reasons of substantial public interest".[26] In this case, it must take place on the basis of Community or national law and be subject to the requirements of proportionality, respect for the essence of the right to data protection and appropriate safeguards such as the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data.[27]

Finally, there are some further exceptions including the protection of "the vital interests of the data subject"[28] or "where the where such processing relates to data which are manifestly made public

[20] *Ibid*. p.18. Definition of 'remote biometric identification' given by the White Paper. It should be distinguished from "biometric authentication" which is a security process that relies on the unique biological characteristics of an individual to verify that he/she is who he/she says he/she is.

[21] "Guidelines on facial recognition*"* from the Consultative committee of the Convention for the protection of individuals with regard to automatic processing of personal data, 28 January 2021.

[22] "Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data", OJ L 119, 4.5.2016.

[23] GDPR Article 9(1).

[24] GDPR Article 9(2) a).

[25] GDPR Recitals 32 & 43 ; Article 4 (11).

[26] GDPR Article 9(2) g).

[27] Directive 2016/680, Recital 37.

[28] GDPR Article 9(2) c) and Directive 2016/680 Article 10 b).

by the data subject"[29], for example social networks' posts. The latter raises the issue of the origin of the images contained in the databases used to compare and identify facial images obtained through AI technologies. This issue, along with others, will be discussed in the second part of the paper.

All in all, one can argue that the legal framework for FRT seems quite clear so far, based on an initial prohibition coupled with limited exceptions. Any entity wishing to use this technology must therefore carefully justify the legal ground to rely from in order to process sensitive data lawfully. But we will see that these rules actually show shortcomings and that there is room for improvement, especially by creating a text specifically dedicated to facial recognition, or AI in general.

2. A TECHNOLOGY THAT EU LAW STRUGGLES TO HANDLE

2.1 The issue of facial recognition databases

It should be borne in mind that the GDPR was first and foremost created to deal with the constantly evolving state of technology, as well as its attendant risks. Many people believe that Snowden's disclosures on global surveillance had a huge influence on the drafting and content of the text, as studies showed that some EU member states were also the scene of the large-scale surveillance practices.[30] Since this scandal, and all the similar cases that are now part of our daily lives, it is not surprising that artificial intelligence systems, and especially facial recognition, frighten many people about their privacy.

One of the biggest concerns in the context of FRT being used for identification purposes is the origin of the images contained in the softwares databases. Not when public authorities refer to official national files but when private entities collect data from social networks in order to create their own facial recognition database. That is what the controversial company Clearview did: over the years, the firm has collected no less than 3 billion images of individuals, retrieved from Twitter, Facebook, Youtube, and other accounts, using the technique of data scraping[31]. The aim was to create an application that gives access to all the images and information related to a specific person, using a simple uploaded picture and a face analysis.

An article from the NY Times revealed in January 2020 that the tech company sold this tool to over 600 law enforcement agencies across the United States, which were using it to solve cases. Facing numerous lawsuits, the startup had to back down, promising to stop selling its technology to private companies and to cancel the subscriptions of non–law enforcement entities.

At the EU level, a question about the lawfulness of this data scraping was referred to the European Commission, which replied that the involvement of Member States authorities or the processing of EU citizens' data has not been confirmed.[32] The commissioner thus merely recalled the rules concerning data protection and privacy. Nevertheless, it is obvious that the latter are deeply incompatible with the facts of the case, which have led the company to shelve its plans for European expansion.

The only legal ground on which Clearview could have relied on in the event of a trial before a European court is that the personal data retrieved have been made publicly available by the data subject (Article 9(2) e) of the GDPR). However, this is not a sufficient justification for data scraping, which is in fact a practice manifestly prohibited by Facebook and other social media in their terms

[29] GDPR Article 9(2) e) and Directive 2016/680 Article 10 c).

[30] Didier Bigo *et al.*, "Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law" in *Liberty and Security in Europe Papers*, No. 62, November 2013 ; referenced in: Hallie Coyne, "The Untold Story of Edward Snowden's Impact on the GDPR" in *The Cyber Defense Review*, vol. 4, no.2, 2019, p.70.

[31] Scraping: practice which consists of using a software program to extract a whole bunch of data from websites automatically, with the aim of recovering it and using it, often for profit.

[32] Answer given by Ms Johansson on behalf of the European Commission (17.07.2020) - question E-000507/20.

of service.[33] Especially since Clearview acted without obtaining any authorization or consent from the users. And more importantly, the company provided its customers with a large number of immediately available facial images of citizens who might never be in situations that could lead to criminal proceedings.[34] Clearview's methods could therefore only have been condemned by the European Union.

If a tool, such as the one developed by Clearview, is able to recognise people, it is thanks to the work done by social media users who have been tagging themselves on pictures for years. All the mainstream social networks use this type of feature for years now, enabling people who post pictures to tag everyone who appears on it. That is how AI software can then put together several pictures of the same individual and come up with precise patterns, thereby increasing the accuracy of identification algorithms. This is similar to how the human brain recognises and remembers facial images.[35]

Facebook went one step further by introducing in December 2010 a new feature called "Photo Tag Suggest", which uses face recognition technology. This tool is able to let users know when they appear in photos or videos without having been tagged and to suggest them to tag people in the new photos they add to their profile. In 2012, Facebook's photo collection already contained around 220 billion images and was increasing by up to 300 million per day.[36]

2.2 The rise of mistrust due to abuses in the use of FRT

Nowadays, biometric identification is increasingly used in public space for surveillance and security purposes. Police forces, for instance, use facial recognition devices in crowded places like stadiums or concert halls to detect potential terrorists among spectators. At first glance, this situation seems to offer much benefits, both to citizens who feel safer and to law-enforcement organizations who see their work simplified. On second thought, it turns out that the risks of infringements on individual civil rights are huge. The fear that these security-oriented systems will reduce our freedom is growing, and legitimate.

In China, a programme called "Sharp Eye" was launched to strengthen the national security system in rural areas. With nearly 300 million cameras equipped with facial recognition software, the Chinese population is constantly being observed. This "Big Brother" can now be found at the entrance to places of worship and enables the population's religious beliefs to be monitored.[37] That is how the Chinese government tracks the Uighurs and constantly watches where they come and go, contributing to their ongoing oppression.

The example of China is obviously extreme and cannot be compared with the situation in European countries, but it does show what kind of drift can happen when it comes to crossing the line between hyper-security and mass surveillance. Because even if installing this type of cameras does not, strictly speaking, reduce freedoms. As we have seen with the example of the panopticon, the feeling of being watched can lead to a form of self-censorship on the part of citizens, particularly

[33] See *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html* Accessed: 27.03.2021

[34] Isadora Neroni Rezende, "Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective" in *New Journal of European Criminal Law*, vol. 11, no. 3, 2020, p.389.

[35] Christopher S. Milligan, "Facial recognition technology, video surveillance, and privacy" in *Southern California Interdisciplinary Law Journal*, vol. 9, no. 1, winter 1999, p. 304.

[36] Yana Welinder, *op. cit.*, p. 173.

[37] See https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/ Accessed: 03.03.2021

with regard to their participation in public life and, more broadly, the exercise of their fundamental freedoms.[38]

It is therefore not surprising that citizens' distrust is the FRT is reflected in the public consultation about artificial intelligence launched by the European Commission in February 2020.[39] Respondents to the online survey published along with the White Paper voiced doubts on the public use of remote biometric identification systems: 28% were in favour of its general ban while another 29% required a specific EU guideline or legislation before such systems may be used in publicly accessible spaces.[40] In the final report, it was noted that civil society is aware that biometric identification threatens fundamental rights, endangers privacy, enables mass surveillance and leads to imbalances in power. Citizens also argued that biometric surveillance can interfere with the freedom of movement, expression and assembly.

3. PROSPECTIVE SOLUTIONS TO SHAPE A BETTER REGULATORY FRAMEWORK TO FRT

3.1 The pressing need to set up a specific framework for facial recognition

As we have seen in this article, facial recognition technology is definitely evolving faster than the legislation that regulates it. Moreover, it deals with such a specific category of data that it calls for the application of a much tighter regime. But above all, in the absence of a common European framework, Member States are developing their own legal systems on the matter, which is likely to cause fragmentation in the internal market.

The European institutions seem to have understood this need, as shown by their latest publications on the topic; notably the online consultation introduced by the European Commission, which was presented as being part of a broader stakeholder consultation process that will contribute to the preparation of various regulatory options. Following an in-depth analysis of the consultation results as well as a detailed impact assessment, a regulatory proposal on artificial intelligence should be presented. A spokesperson for the EU executive interviewed said that the Commission is considering introducing specific provisions on facial recognition.[41]

3.1.1 The content of such future system

The guidelines on facial recognition published by the Council of Europe at the end of January 2021 provide a good overview of the main measures to be implemented for a more appropriate framework for the use of FRT. It gives recommendations to decision-makers as well as developers and manufacturers.

Firstly, the Council recommends legislating by category of use. It specifies that any legal framework must include a detailed explanation of the intended use and purpose, the minimum reliability and accuracy of the algorithm used, the length of time the photos used are kept, the possibility of auditing these criteria, the traceability of the process and safeguards (p.4). The legislator should also indicate the different phases of the use of facial recognition technologies (including the creation of databases and deployment phases), the sectors in which these technologies are used and the intrusive nature of some of them, while providing clear guidance on lawfulness (p.5).

[38] Jameson Spivack and Clare Garvie "A Taxonomy of Legislative Approaches to Face Recognition", Chapter 7 of the compendium "Regulating Biometrics: Global Approaches and Urgent Questions" in *AI Now Institute*, 2020, p.88.

[39] Public consultation towards a European approach for excellence and trust Consultation on the White Paper on Artificial Intelligenc, European Commission White Paper on Artificial Intelligence.

[40] Consultation's Final Report, November 2020, see https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence Accessed 03.03.2021

[41] See https://www.euractiv.fr/section/economie/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/ Accessed: 06.03.2021

The guidelines also stress the need to systematically consult the supervisory authorities before initiating any project (p.6) and encourage the use of certification mechanisms (p.7).

With respect to the different actors of the facial recognition industry, the document introduces some obligations. For developers, manufacturers and service providers, the emphasis is placed on the need to ensure the quality of data and algorithms, to guarantee the reliability of the tools used as well as data security, and to raise awareness among users. For "user entities", i.e. data controllers and processors (p. 10), it is recalled that they are subject to compliance with the basic data protection principles: legitimacy of processing, transparency, fairness, accuracy, minimisation, limited storage time, data security, impact assessment, etc. Finally, the rights of individuals must be guaranteed. For example, in case of false matches, they should be able to request rectification (p. 15-16).

The European Commission finally published on 21 April 2021 its "Proposal for a Regulation laying down harmonised rules on artificial intelligence"[42], which it introduced as "the first ever legal framework on AI, which addresses the risks of AI and positions Europe to play a leading role globally". The main challenge was to decide how to approach this technology and its heterogeneous applications. While this approach could have been sectoral (according to the industrial sector concerned) or legal (according to the branch of law concerned), the Commission favoured a third option already foreshadowed by its previous writings: a risk-based approach.[43] The proposal, also known as the "Artificial Intelligence Act", therefore distinguishes between unacceptable, high, limited and minimal risk.

The text refers to facial recognition already in its Title 2 on prohibited artificial intelligence practices. After carefully defining remote biometric identification system (Art. 3, 36), and distinguishing between 'real-time' analysis (Art. 3, 37) and 'post' remote biometric identification system (Art. 3, 38); Article 5 of the proposal introduces a prohibition principle on the use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement. Exceptions remain open. These are the targeted search for for specific potential victims of crime, including missing children (i); the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; (ii); the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence punishable by a custodial sentence of at least three years (iii). These grounds must take account of defined assessment criteria (§ 2) and the use of such systems must be authorised by a judicial or administrative authority (§ 3), subject to prior legislation (§ 4).

On governance, the Commission proposes the creation of national competent authorities designated by each Member State to ensure enforcement of the Act. A new Artificial Intelligence Committee will be created to contribute to the effective cooperation of national supervisory authorities. Finally, the penalties are very high and can be up to €30 million or, if the offender is a company, up to 6% of its total worldwide annual turnover in the previous financial year (Articles 71 and 72).

It remains to be seen whether this model, observed all over the world, will make it through the EU legislative process.

3.1.2 The scenario of a complete ban

Given the many abuses and criticisms of the FRT, one might think that the most effective solution would be to simply ban it, or at least its most worrying use: remote biometric identification in public spaces. European citizens seem to hold this view[44], as well as the Council of Europe which

[42] COM/2021/206 final "Proposal for a 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"

[43] Cécile Crichton, "Projet de règlement sur l'IA (II) : une approche fondée sur les risques" in *Dalloz actualité 4 mai 2021*, pp. 19.

[44] Public Consultation's Final Report, *loc. cit.*

advocates that private entities should not be allowed to use this technology in uncontrolled and freely accessible environments for marketing or private security purposes (guidelines p.7).

This idea, although radical, has tempted the European Commission, which let the rumour of a five-year ban on FRT in public areas spread while commissioners were drawing up the White Paper released in February 2020.[45] This ban, which was eventually dropped, would have given them time to assess the impacts of this technology, develop potential risk management measures and determine how to prevent abuses. It would have acted more like a moratorium than a straight ban.

However, the arguments put forward by the European institutions do not seem to convince everyone, as proven by the movement "Reclaim Your Face" which describes itself as "a European movement that brings people's voices into the discussion around biometric data used to monitor the population". [46] It gathers digital rights advocates of six European countries and calls for a Europe-wide ban on the use of "dangerous facial recognition". On 17 February 2021, this coalition has joined forces with the EDRi organization (European Digital Rights) to launch a petition based on the European Citizens' Initiative (ECI) mechanism[47]. The aim is to reach 1 million signatures during a period of 12 months, in the hope of establishing an "official" communication with the Commission in order to ask for a debate in the Parliament.

3.2 Temporary solutions pending the establishment of a future legal framework

3.2.1 Make facial recognition devices more GDPR compliant

While waiting for European lawmakers to adopt and bring into effect a specific bill on facial recognition, improvements to the current system can still be considered. The first step would be to work on making the existing FRT devices more compliant with the GDPR, ensuring that their use in the public space has an appropriate legal basis and additional safeguards adapted to the risks involved and the interests to be protected.

When the processing of biometric data from live FRT is based on consent, the challenge would be to ensure that the data subject has understood the full implications of such processing. As the lack of trust in the devices is compounded by the difficulty for a user to really grasp the consequences of the collection and uses that will be made of his personal data. The objective would be to present, technically, what facial recognition is and what it is used for, but also to highlight the risks associated with it.

It is with this awareness-raising perspective that Facebook updated its "Photo Tag Suggest" feature in 2019. This update implies that users receive a notice in their News Feed with information about the face recognition setting and options to learn more about how the social network uses it. It also includes a button to turn it on or keep it off.[48] This is a good example of how to raise awareness among data subjects to ensure the most informed consent possible.

As regards surveillance cameras used for remote identification, time limits for the retention of recordings should also be set and transparently indicated.

3.2.2 Toward a common European facial recognition database?

In Mai 2019, in accordance with the provisions of Regulation 2019/817 establishing a framework for interoperability between EU information systems in the field of borders and visa, the European Commission has announced the creation of a common network of facial recognition

[45] Chee F. Y. (2020). *EU mulls five-year ban on facial recognition tech in public areas*. Retrieved from https://www.reuters.com/article/idUSL8N29L61I.

[46] See https://reclaimyourface.eu/the-movement/ Accessed 06.03.2021

[47] The European Citizens' Initiative (ECI) is a unique tool provided by the European Union mechanism to increase direct democracy by allowing citizens to participate directly in the development of EU policies. It was introduced by the Treaty of Lisbon in 2007.

[48] See https://about.fb.com/news/2019/09/update-face-recognition/ Accessed: 13.03.2021

databases for European law-enforcement forces. This new system, called shared biometric matching service (shared BMS), will replace the actual five different central systems with a common platform where the data is queried and compared simultaneously.[49] The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) has been was mandated to develop the shared BMS and ensure its technical management.

By 2022, the shared BMS will be one of the largest biometric systems in the world, integrating a database of over 400 million third-country nationals with their fingerprints and facial images. Based on European biometrics technology, this new system will generate substantial benefits in terms of security, cost, maintenance and operation. Moreover, the biometric template will remain stored in one location. It promises to become the cornerstone of the protection of European borders.

This tool should help the EU to avoid scandals such as the Clearview case, when it is known that the FBI's biometric database contained four times fewer images than the one created by the company.[50]

4. CONCLUSION

Facial recognition is an increasingly popular technology for both identification and identity verification solutions. It is now part of our daily environment, sometimes without even realising it. As it softly imposed itself in our societies, it is difficult to realize the major turning point this innovation represents for humanity. So much so that the legislators were unable to anticipate it and are now struggling to adapt to it.

The European Union has been particularly slow to grasp the challenges of this rapidly developing technology and to set the necessary steps to reduce its impact. FRT in Europe is today still governed by the broader legal framework of data protection, which appears to be not specific and clear enough to ensure an optimum control of its use. However, we know that an unsupervised use can be damaging and infringe people's rights and freedoms. Abuses of this kind have already occurred.

The most problematic area is that of remote biometric identification, as it can easily amount to a permanent identity check. Even if its use in European countries is far from being as widespread as in China for example; trials are multiplying, with the aim of gradually including it in our cities. And despite the strong reactions, nothing has yet been done to stop this progression. Neither should we claim a technological emergency, but there is indeed a real need to adopt binding laws on the matter.

One can then conclude by keeping in mind that facial recognition is both a fascinating and frightening technology that should not be underestimated. It is also clear that legislating in this area is especially hard, given all the elements at stake. The biggest challenge is thus to find the right balance between, innovation, security and privacy.

BIBLIOGRAPHY:

1. COYNE, Hallie, "The Untold Story of Edward Snowden's Impact on the GDPR" in *The Cyber Defense Review*, volume 4, no.2, 2019, pp. 65-79.
2. CRICHTON, Cécile, "Projet de règlement sur l'IA (II) : une approche fondée sur les risques" in Dalloz actualité 4 mai 2021, pp. 19-23.
3. FOUCAULT, Michel, *Surveiller et punir*, Paris, Gallimard, 1975.
4. GALIČ, Maša *et. al.*, "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation" in *Philosophy & Technology*, vol. 30, no. 1, 2017, pp. 9-37.

[49] Regulation 2019/817, Recital 17.

[50] See https://www.lexpress.fr/actualite/sciences/clearview-l-application-proscrite-par-la-france-pour-proteger-notre-vie-privee_2115879.html Accessed 13.03.2021

5. HOFFMANN, Thomas, „The Impact of Digital Autonomous Tools on Private Autonomy", in *Baltic Yearbook of International Law Online*, vol 18, 2020, pp. 18−31.
6. JOAMETS, K.; CHOCHIA, A. (2021). Access to Artificial Intelligence for Persons with Disabilities: Legal and Ethical Questions Concerning the Application of Trustworthy AI. Acta Baltica Historiae et Philosophiae Scientiarum, 9 (1), 51−66.
7. KINDT, Els, "A First Attempt at Regulating Biometric Data in the European Union", chapter 4 of the compendium "Regulating Biometrics: Global Approaches and Urgent Questions" in *AI Now Institute*, September 2020, pp.62-68.
8. MILLIGAN, Christopher S., "Facial recognition technology, video surveillance, and privacy" in *Southern California Interdisciplinary Law Journal*, volume 9, no. 1, winter 1999, pp. 296-333.
9. PEREC, Georges, *L'infra-ordinaire*, Paris, Seuil, 1989.
10. PRAVEN, G. B. and DAKALA, Jayachandra, "Face Recognition: Challenges and Issues in Smart City/Environments" in *2020 12th International Conference on Communication Systems & Networks (COMSNETS)*, pp. 791-793.
11. REZENDE, Isadora Neroni, "Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective" in *New Journal of European Criminal Law*, volume 11, no. 3, 2020, pp. 375-389.
12. SPIVACK, Jameson and GARVIE, Clare, "A Taxonomy of Legislative Approaches to Face Recognition", Chapter 7 of the compendium "Regulating Biometrics: Global Approaches and Urgent Questions" in *AI Now Institute*, 2020, pp. 86-94.
13. WELINDER, Yana, "A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks" in *Harvard Journal of Law and Technology*, vol. 26, no. 1, Fall 2012, pp.166-237.

European legislation and associated materials:

14. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).
15. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.
16. Directive 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, OJ L 119, 4.5.2016.
17. Final Report of the Public Consultation on the AI White Paper, November 2020. Available at: https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence.
18. Focus Paper, "*Facial recognition technology: fundamental rights considerations in the context of law enforcement*, EU Agency for Fundamental Rights, 27.11.2019.
19. Guidelines on facial recognition, Consultative committee of the Convention for the protection of individuals with regard to automatic processing of personal data, 28.01.2021.
20. Opinion 2/2012 on facial recognition in online and mobile services, Article 29 Working Party, 22.03.2012.
21. Opinion 3/2012 on developments in biometric technologies, Article 29 Working Party, 27.04.2012.
22. Parliamentary question E-000507/20, answer given by Ms Johansson on behalf of the European Commission, 17.7.2020.
23. Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data, Council of Europe, 2005.
24. Proposal for a 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/2021/206 final, European Commission, Brussels, 19.4.2021.
25. Regulation 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, OJ 2016 L 119/1.

26. Regulation 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa, OJ L 135, 22.5.2019.
27. White Paper on Artificial Intelligence - A European approach to excellence and trust, COM/2020/65, European Commission, Brussels, 19.2.2020.

Web materials:
28. Chee F. Y. (2020). EU mulls five-year ban on facial recognition tech in public areas. See https://www.reuters.com/article/idUSL8N29L61I Accessed: 13.03.2021.
29. Fossat M. (2020). Vie privée : pourquoi l'application Clearview ne devrait pas arriver en France (trad: Privacy: why the Clearview application should not be available in France). See https://www.lexpress.fr/actualite/sciences/clearview-l-application-proscrite-par-la-france-pour-proteger-notre-vie-privee_2115879.html Accessed: 06.03.2021.
30. Harwell D. & Dou E. (2020). Huawei tested AI software that could recognize Uighur minorities and alert police, report says. See https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/ Accessed 06.03.2021.
31. Hill K. (2020). *The Secretive Company That Might End Privacy as We Know It*. See https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html Accessed 03.03.2021
32. Market Analysis Report (2020). *Facial Recognition Market Size, Share & Trends Analysis Report By Technology, By Application, By End Use And Segment Forecasts, 2020 – 2027*. Summary available at: https://www.grandviewresearch.com/industry-analysis/facial-recognition-market. Accessed: 03.03.2021.
33. Narayanan S. (2019) An Update About Face Recognition on Facebook. See https://about.fb.com/news/2019/09/update-face-recognition/ Accessed: 17.03.2021.
34. Stolon S. (2020). Bruxelles se penche sur le scandale Clearview AI sur la reconnaissance faciale (trad: Brussels looks into AI facial recognition scandal). See https://www.euractiv.fr/section/economie/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/ Accessed: 06.03.2021.