URBAN AGENDA FOR THE EU

WORKING TOGETHER FOR BETTER CITIES

SECURITY IN PUBLIC SPACES

New Surveillance Technologies in Public Spaces

Challenges and Perspectives for European Law at the Example of Facial Recognition

April 2021

EN

NEW SURVEILLANCE TECHNOLOGIES IN PUBLIC SPACES

CHALLENGES AND PERSPECTIVES FOR EUROPEAN LAW AT THE EXAMPLE OF FACIAL RECOGNITION

ABSTRACT

At the dawn of the 21st century, the European Union committed to the development and deployment of responsible, inclusive, and humane technology. On the ongoing debate over so-called high-risk technologies for surveillance in public spaces, facial recognition technology (FRT) is a typical case for European scrutiny. The assessment of the experiments already conducted in cities helps to clarify the contemporary stakes and offers the first answers. This study defines FRTs, discusses current experiments, catalogues the applicability of European law, and concludes with recommendations.

AUTHOR
Ass. Prof. Dr. Caroline Lequesne Roth, Université Côte d'Azur

LINGUISTIC VERSIONS
Original: EN

Manuscript completed in April 2021

Table of Contents

List of Abbreviations

ABC	Automated Border Control
ADP	*Autorité de protection des données* (Be)
AEPD	*Agencia Española de Protección de Datos*
AFR	Automated Facial Recognition technology
AI	Artificial Intelligence
AR	Augmented Reality
BfDI	The Federal Commissioner for Data Protection and Freedom of Information
BIPA	Biometric Information Protection Act
BPoIG	German Federal Police Law, Bundespolizeigesetz
CAI	*Commission d'accès à l'information du Québec*
CAS	Crime Anticipation System
CCPA	California Consumer Privacy Act
CCTV	Closed-Circuit Television
CILIP	Library and Information Association
CJEU	Court of Justice of the European Union
CNPD	Portuguese Data Protection Authority (*Comissão Nacional de Protecção de Dados*)
CNIL	*Commission Nationale Informatique et Libertés*
CoE	Council of Europe
DNN	Deep Neural Network
DPA	Data Protection Authority
DPIA	Data Privacy Impact Assessment
ECHR	European Court of Human Rights
ECHR	European Convention on Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EES	Entry-Exit System
EFF	Electronic Frontier Foundation
EU	European Union
FBI	Federal Bureau of Investigation
FRA	European Union Agency for Fundamental Rights
FRT	Facial recognition technology
GDPD	*Garante Per La Protezione Dei Dati Personal*
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
IDEC	Brazilian Institute of Consumer Protection
IfmPt	*Institut für Musterbasierte Prognosetechnik*
IMY	*Integritetsskyddsmyndigheten*
IoT	Internet of Things

IPOC AB	Information and Privacy Commissioner of Alberta
IPOC BC	Information and Privacy Commissioner of British Columbia
ITU	International Telecommunications Union
ISF	Internal Security Fund of the European Commission
LED	Law Enforcement Directive
NGO	Non-Governmental Organisation
NIST	U.S. National Institute of Standard & Technology
OHCHR	United Nations Human Rights Council
OPC	Privacy Commissioner of Canada
PARAFE	French acronym for “rapid automated passage at the Schengen external borders”
PIPA	Personal Information Protection Act (Canada, Alberta or British Columbia)
PIPEDA	Personal Information Protection and Electronic Documents Act
PNR	European Passenger Name Record
TCN	Third Country National
UAV	Unmanned Aerial Vehicle
UK	United Kingdom (The ISO abbreviations list has been followed for the other European countries).
UN	United Nations

List of Boxes

List of Figures

List of Tables

Executive summary

Background

At the dawn of the 21st century, the European Union committed to the development and deployment of responsible, inclusive, and humane technology. The commitment contributed in particular to the development of one of the most protective personal data protection laws in the world. Today, the commitment continues around the ongoing debate over so-called "*high-risk technologies*", which have uses that are likely to transform our individual and collective lives in prosaic and profound ways.

At the same time, the EU is committed to stepping up the fight against terrorism and violent extremism and boosting the EU's resilience to terrorist threats, including through investments in new technologies. On the front line, local and regional authorities are committed to better protecting public spaces. Commissioned by the Urban Agenda Partnership on Security in Public Spaces, the present study deals with a typical case of high-risk technologies for European scrutiny: facial recognition technology (FRT) in public spaces. Its application for security purposes has sometimes been received with opposition and there are multiple questions regarding the assessment of existing experiments involving the use of FRT.

Aim

This study aims to analyse the challenges and prospects of European law for a responsible FRT framework. The assessment of the experiments already conducted helps to clarify the contemporary stakes and offers the first answers. This study first succinctly defines FRTs main features and risks (I), discusses current experiments (II), catalogues the applicability of European law and draw guidelines for entities using facial recognition technologies, notably cities (III), and concludes with recommendations for European legislators (IV).

Findings

Surveillance new technologies raise expectations from public authorities to strengthen security. Implementing FRT to secure public space is, however, not trivial. On the one hand, it touches upon core issues of the relation between the individual and the public authorities. On the other hand, the technology involves processing particularly sensitive data, such as biometric data, which distinguishes it from other surveillance technologies.

The social and political impacts of FRT thus require increasing vigilance from legislators and policymakers.

This study:

- Defines FRT as the automatic processing of digital images containing individuals' faces to identify or authenticate those individuals. FRTs use algorithms to analyse the faces in photographs or videos based on a probabilistic model.

- Shows FRTs can be used for various purposes, which imply two types of risks:
  - Risks can result from technological vulnerabilities of image processing or the database components. Technological risks consist of mismatches, bias, and security flaws.
  - FRT also carries specific risks for fundamental rights: risk of a chilling effect on freedom of expression, freedom of association, and peaceful assembly; risk of interference with the right to privacy and data protection; and a threat to the principle of equality between all human beings and the dignity of the human person.

- Documents that FRT in public spaces is already a practical reality in Europe. The study provides an overview of experiments and practices in thirteen European countries. Rollouts took place in various areas (transportations, public events, schools) for two primary purposes (authentication and identification) involving different systems and industrial solutions. Most of the experiments were carried out between 2016-2020. The global COVID pandemic did not change the trajectory of the FRT in Europe; it instead accelerated the widespread of technology.

- Points out that the deployment of technology also has societal underpinnings. Its social acceptance varies upon the uses, as do the public authorities' expectations that shape its deployment.

- Analyses the European legal framework for deploying FRT systems. This framework consists of two sets of rules whose application depends on the purposes of the data processing: the Law Enforcement Directive (LED) and the General Data Protection Regulation (GDRP).

- Warns about the legal definition of biometric data flaws and the legal basis's weakness for the deployment of FRT in the public space.

- Reviews specific safeguards surrounding the deployment of FRT relate to the data processing, the data controller, the technical features of the recognition system, the human involvement, and the rights of the data subject. Good

practices for entities using facial recognition technologies that reflect compliance to these guarantees are listed.

- Cautions that the processual proof of data process's compliance, albeit critical, suffers from weakness: the compulsory nature of data protection impact assessment (DPIA) for FRT rollout is debated, and its content remains uncertain.

- Recommends (1) to amend the biometric data legal definition, (2) adopt a specific framework and clarify biometric prohibition exemption, (3) enhance the DPIA and its effectiveness.

List of recommendations

Recommendation n°1

The study recommends amending the biometric data legal definition. The definition should offer adequate protection to unique human characteristics that fits the various purposes of FRT and restricts the storage of this data in databases. An alternate definition could be: "*all personal data (a) relating directly or indirectly to unique or distinctive biological or behavioural characteristics of human beings and (b) used or fit for use by automated means (c) for purposes of identification, identity verification, or verification of a claim of living natural persons.*"[1]

Recommendation n°2

The study recommends for the legislator to adopt a specific framework to guarantee legal certainty and the respect of fundamental and data protection rights.

Recommendation n°3

The study recommends for the legislator to clarify biometric prohibition and sweeping exceptions. In this respect, compliance with fundamental rights requires some uses to be prohibited.

For the CoE "*the use of facial recognition for the sole purpose of determining a person's skin colour, religious or other beliefs, sex, racial or ethnic origin, age, health condition or social condition should be prohibited unless appropriate safeguards are provided for by law to avoid any risk of discrimination*."[2] The study also, and more specifically, recommends prohibiting the deployment of all RF systems implementing mass surveillance, such as the real-time FRT, and the deeply flawed emotional recognition

Recommendation n°4

The study recommends for the European supervisory authority, to issue restrictive interpretative guidelines concerning "made public data." As found by the Canadian DPA, it should be clear that information from sources such as social media or professional profiles, collected from public websites and then used for an unrelated purpose, does not fall under the publicly available exception.

[1] Based on the research work of Kindt E. A First Attempt at Regulating Biometric Data in the European Union, *AI Now*, Regulating Biometrics: Global Approaches and Urgent Questions, 2020, p.66.

[2] CoE, *op. cit.*, p. 5

Recommendation n°5

DPAs should be involved in assessing the appropriateness of a DPIA (co-regulation model).

Recommendation n°6

DPIAs for FRT, as well as their publication – at least their summary, should be expressly made mandatory.

Recommendation n°7

A standard methodology, with a specific set of expectations, should be established for FRT's use through audit chain's introduction.

Recommendation n°8

The black box system is not compatible with a democratic transparency regime, and stakeholders' participation in the process should be clarified.

1. Introduction

At the dawn of the 21st century, the European Union committed to the development and deployment of responsible, inclusive, and humane technology. The commitment contributed in particular to the development of one of the most protective personal data protection laws in the world. Today, the commitment continues around the ongoing debate over so-called "*high-risk technologies*," which have uses that are likely to transform our individual and collective lives in ways prosaic and profound.

Among identifiable high risks technologies, surveillance technologies have a unique position. Far from bringing consensus, these technologies strongly polarize the public debate: European law enforcement agencies call for their adoption and the European industry sees them as a driver to innovation, while human rights associations and public opinion show concerns. This study has been commissioned by the Urban Agenda Partnership on Security in Public Spaces, which intends to take part in the debate over surveillance technology as part of its overall mission. Created in 2016 under the aegis of the Council of the European Union[3], The Urban Agenda aims to bring together public actors around urban security issues. The Security in Public Spaces Partnership enables local authorities, Member States, and European institutions to work together to assert the place of cities in European security policy, strengthen knowledge sharing and exchange best practices, and propose legislative changes and new funding frameworks at the European level.

This study focuses on an important and illustrative development of high-tech surveillance: facial recognition technology (FRT). The application of FRT for security purposes has seen considerable opposition and there are multiple questions regarding the assessment of existing experiments involving the use of FRT. The assessment of the experiments already conducted helps to clarify the contemporary stakes and offers the first answers. This study defines FRTs (I), discusses current experiments (II), catalogues the applicability of European law (III), and concludes with recommendations (IV).

[3] Based on the Amsterdam Pact adopted on the 30 May 2016 at the informal meeting of ministers in charge of Urban affairs.

I. Definitions

FRT is a generic term, covering a wide range of applications. The study presents its technical features (I.1) and identifies the main risks of letting FRT continue without specific safeguards (I.2).

I.1 Technical features

FRT is the automatic processing of digital images containing individuals' faces to identify or authenticate those individuals. More precisely, FRT uses algorithms to analyse the faces in photographs or videos: they extract distinctive features, such as the distance between the eyes or the chin's shape, code them as mathematical representations (the "face templates"), and store – or compare – them to those contained in a database.[4] These applications are based on a probabilistic model, aiming to evaluate the correspondence between digital images and existing face templates.

The processing performed by the recognition algorithm requires two components: a software application and the hardware (hereinafter referred to as "recognition system"). The software application runs on a processor, realizes the hardware's initialization and control, and the recognition algorithms.

Processing of biometric data

FRT involves processing biometric data: the facial features that allow the system to "recognize" a person. The use of this data distinguishes FRT from other types of video recording, such as standalone surveillance cameras, although they exist within the same "*technological continuum*."[5]

FRT can be used for identification or authentication purposes.

Identification, in connection to FRT, 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 or her image is stored there."[6] The database comprises the information used as a reference to compare live or captured images. It can be either centralized or distributed on devices (such as identity cards or mobile phones), controlled by a single or several entities.[7]

Such a procedure has been used, for example, to monitor public space during a public event (based on watchlists) or during an investigation, including the forensics.[8]

[4] Castelluccia C., Le Métayer D., *Impact Analysis of Facial Recognition: Towards a Rigorous Methodology*, Inria, 2020, hal-02480647f.
[5] In the words of the French DPA. See, e.g., CNIL, *Reconnaissance Faciale: pour un débat à la hauteur des enjeux*, 15 November 2019, p.4.
[6] COM(2020)65 *White Paper on Artificial Intelligence - A European approach to excellence and trust*, 2020, p. 21.
[7] Castelluccia C., Le Métayer D., *Impact Analysis of Facial Recognition: Towards a Rigorous Methodology*.
[8] See the intervention of HartmannM., fundamental rights implications of recent trends in digital forensics, Bonn's Staatsanwaltschaft, CPDP 2021.

Authentication (or verification) *"is often referred to as one-to-one matching. It enables the comparison of two biometric templates, usually assumed to belong to the same individual. Two biometric templates are compared to determine if the person shown on the two images is the same person."*[9] For example, FRT authentication is used for border control at airport gates (Automated Border Control - ABC).

FRT can also be used either "in real-time" (live captured images comparison) or "a posteriori" (recorded images analysis).

Figure I.1: Examples of applications of facial recognition[1]

Application	*Inputs Received*	*Inputs Provided*	*Data stored in a centralized database*	*Outputs*	*Mode of operation: T: Real Time P: A posteriori*
Secure Online Authentication – Alicem (Facial authentication)	A video or a photo	Identity and a photo	0	Failure (identity not verified) or Identifier (verified identity)	T
Access to the station platform (Facial identification)	A video or a photo	0	N pairs (identity; face)	0 (not allowed) 1 (authorized)	T
Access control with badge (Facial authentication)	A video or M photos	Identifier extracted from the badge	N pairs (identity; face)	0 (identity not verified) 1 (identity verified)	T
Identification by the police (Facial identification)	A video or M photos	0	N pairs (identity; face)	0 or identity	T or P
Search for people (lost or criminal) in public spaces (Facial identification)	A video or M photos	0	N pairs (identity; face)	0 or list of identities	T or P
Follow-up of a person (Facial recognition for tracking)	A video or M photos	A video or M photos	0	N images	T or P

I.2 Risks

FRT uses involve two types of risk: the first results from technological vulnerabilities (I.2.A) while the second consists of a threat to fundamental rights (I.2.B).

[9] *Ibidem.*

I.2.A Technological vulnerabilities

There are two categories which are likely to affect systems: mismatches and bias (I.2.A.1) and security flaws (I.2.A.2). It is essential to mention that vulnerabilities can result from image processing or the database components choices. When analysing the risks associated with FRT, the whole system should then be taken into account.[10]

I.2.A.1 Mismatches and bias

Error rates in FRT are variable but can be significant, especially for particular populations.[11] As a consequence, human discretion remained critical during, for example, the London Metropolitan Police Service's trial of real-time FRT. To avoid and limit misidentification, officers were informed that "*a computer derived match was not sufficient to confirm an identity in and of itself*" and "*expected to conduct further checks to confirm their [the matched individual's] identity*".[12]

Many studies have shown, more broadly, that the risk of false positives and false negatives is significant. The false-negative corresponds to an identification failure: a face, previously recorded, is not recognized by the device. A false positive is the result of an identification error: a person is wrongly identified as the proper recipient of benefits or access, or as a person of interest. The consequences of a false positive are particularly worrying, given the risk of impersonation or wrongful arrest. Precedents have been reported in the United States, where the use of FRT by police forces is more widespread than in Europe. At least three men of colour have been wrongly arrested and jailed based on FRT misidentification.[13]

Reliability tends to vary across environment (angles, light, weather conditions, image resolution). For example, while the reliability level of the Parafe system (gates airports) can be higher than 99.5%, results are significantly lower in uncontrolled environments. Reliability may also vary based on demographic parameters: age,[14] skin colour,[15] or gender.[16] The faces of black women were falsely identified more often white men in some studies. These errors may result from difficulties intrinsic to biometric recognition, or biases in the constitution of datasets (i.e., insufficiently diverse training data).[17]

---

[10] Castelluccia C., Le Métayer D., *Impact Analysis of Facial Recognition: Towards a Rigorous Methodology*, ,See above n°8a.
[11] Several American studies underline that fact (see below note n°16), also observed during some British experiments, like in Cardiff.
[12] University of Essex, *London Metropolitan Police & Trial of Facial Recognition*, Report, p.116.
[13] One of them is suing the police, the prosecutor, and the City for false arrest, false imprisonment, and violation of his civil rights, as the "police department was relying solely on the faulty and illegal Clearview FR App or some analogous program." Superior Court Of New Jersey Law Division, Nijer Parks Lawsuit, 25 November 2020.
[14] NIST, *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, Washington DC: US Department of Commerce, 2018, p.7.
[15] NIST, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, Washington DC: US Department of Commerce, 2019.
[16] Buolamwini J., Gebru *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research* 81:1–15, 2018, p12. The study was the subject of criticism from Amazon, to which Buolamwini answered in a detailed note: Buolamwini J., Response: Racial and Gender bias in Amazon Rekognition — Commercial AI System for Analyzing Faces', *Medium*, 25 January 2019.
[17] This is a difficult issue to be managed and contained. Indeed, many facial recognition datasets that have been taken down due to bias concerns are still used for identification and free for anyone to download. Peng K., Facial recognition datasets are being widely used despite being taken down due to ethical concerns. Here's how, *Freedom to tinker*, 21 October 2020. See also: Charpenet J., Lequesne Roth C., Discrimination et biais genrés, Les lacunes juridiques de l'audit algorithmique, *Dalloz*, 2019, p. 1852.

Studies conducted by the U.S. National Institute of Standards & Technology (NIST) show a trend toward the reduction in error rates since 2010, presumably due to advances in deep neural networks. Some algorithms – such as Idemia or NEC3 – are held up as free of demographic biases; indeed, they will be used to identify athletes of many different ethnic origins at the Tokyo Olympic Games.[18] Significant performance differences exist however in the market, in part due to costs.

I.2.A.2 Security flaws

Facial recognition systems raise at least two types of security concerns: recognition can be evaded and manipulated, and the large databases that such systems rely upon could be breached.

Facial recognition systems can be spoofed and hacked. Studies demonstrated that many systems are vulnerable to spoofing techniques: photos, videos, and 3D models or deep fakes[19] of a face could be used for impersonation.[20] The issue is all the more concerning insofar as the face, of all biometric data, is easy to access and reproduce. But at the same time, the face is "immutable": once compromised, an individual has no way to remedy the consequences of the breach[21] i.e. to restore a *status quo ante*. Recent studies have also demonstrated that Deep Neural Network (DNN) classifiers can be fooled by adversarial examples.[22] If only a few pixels at the corner of a person's eye are adjusted [23] or if printed paper stickers are added to a hat[24] and the system is no longer efficient.

Since 2018, many biometric data breaches were reported. In August 2019, a security breach in a database used by banks, defence contractors, and UK metropolitan police allowed access to biometric data from over 1 million people.[25] The database belonged to the South Korean company Suprema, a market leader in biometric identification in Europe,[26] the Middle East, and the Africa Continent. In 2020, the controversial Clearview AI database, made up of billions of biometric data scrapped on social media, also experienced a significant security breach. The

[18] Shankland S., Tokyo 2020 Olympics using Facial Recognition system from NEC, Intel, *CNET*, 1 October 2019.
[19] Tariq S., Jeon S., Woo S. S., *Am I a Real or Fake Celebrity? Measuring Commercial Face Recognition Web APIs under Deepfake Impersonation Attack*, 2 March 2021.
[20] Khan J. K. and Upadhyay D., *Security issues in face recognition*, 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence), Noida, India, 2014, pp. 719-725.
Sudeep S.V.N.V.S., Venkata Kiran S., Nandan D., Kumar S. An Overview of Biometrics and Face Spoofing Detection, In: Kumar A., Mozar S. (eds) ICCCE 2020. *Lecture Notes in Electrical Engineering*, vol 698. Springer, Singapore, 2021.
[21] "*If a hacker succeeds in seizing the 35,000 points that make up your face and sells it on the darkweb, it will be almost impossible to recover your digital identity*." Dechaux D., 'La vérité sur les failles de la biométrie faciale', *Challenges*, 23 January 2021.
[22] Alparslan Y., Alparslan K., Keim-Shenk J., Khade S., Greenstadt R., *Adversarial Attacks on Convolutional Neural Networks in Facial Recognition Domain*, 2021.
See also: Evtimov I. et al, What if a facial recognition system is too easy to fool? Is Tricking a Robot Hacking? *Berkeley Technology Law Journal 34*, 2019, p. 891.
[23] Bose A. J., Aarabi P., *Adversarial Attacks on Face Detectors using Neural Net based Constrained Optimization*, 2018.
[24] Komkov S., Petiushko A., *AdvHat: Real-world adversarial attack on ArcFace Face ID system*, 2019.
[25] VPN Mentor, Report: Data Breach in Biometric Security Platform Affecting Millions of Users reported in 'Major breach found in biometrics system used by banks, UK police and defence firms', *The Guardian*, 14 August 2019.
[26] The company notably supplied Belgium, Finland and Germany.

source code and some of its private keys became publicly accessible, allowing anyone to access the database.[27]

While the FRT industry claims it is improving security, no security system is perfect, and there is no reason to distinguish FRT from most other sectors (health, finance) where breaches occur regularly.

Box 1: Creation of risky and illegitimate biometric databases

Creation of risky and illegitimate biometric databases

1) The Clearview case

Clearview was founded in 2016. The company has since gathered a database of over three billion photos scraped from public social media profiles[28] without users' consent.[29]

It allows the company to create an FRT application that identifies persons from web photos and links them to social media. The software was later developed to be implemented in surveillance cameras and AR glasses.[30] The company activity was revealed by a New York Times investigation. Six hundred law enforcement agencies (now 1,300) and private companies reportedly used its services. It would have included national law enforcement agencies, government agencies, and police forces in twenty-seven countries (Australia, Belgium, Brazil, Canada, Denmark, Finland, France, Ireland, India, Italy, Latvia, Lithuania, Malta, the Netherlands, Norway, Portugal, Serbia, Slovenia, Spain, Sweden, Switzerland, the United Kingdom, and the United States).[31]

In the United States, class action lawsuits have been filed against Clearview AI in Illinois, New York, California, and Vermont. The applicants allege a breach of the California Consumer Privacy Act (CCPA) or the Biometric Information Privacy Act (BIPA). In return, Clearview AI promised to avoid any transactions with non-government customers, including Bank of America, Macy's, and Walmart.[32] The company also promised to cancel all accounts belonging to any Illinois-based entity. Yet, the implementation of these initiatives has not actually been demonstrated.

In Canada, Clearview announced the end of its activity in 2020. Regardless, a joint investigation was launched in February 2020 by the Privacy Commissioner of Canada (OPC), the *Commission d'accès à l'information du Québec* (CAI), the Information and Privacy Commissioner of British Columbia (IPOC BC), and the Information and Privacy Commissioner of Alberta (IPOC AB). The investigation concluded that Clearview violated numerous principles of federal and

[27] Whittaker Z., Security lapse exposed Clearview AI source code, *TechCrunch*, 16 April 2020.

[28] In comparison, this is roughly seven times larger than the FBI's own photo database of 411 million; See: Faces Fourth Lawsuit Alleging Biometric Privacy Violations, *Expert Institute*, 25 June 2020.

[29] In January 2020, Twitter filed a formal notice against Clearview AI, asking them to delete all data collected on their site. YouTube, Facebook, Google, LinkedIn and Apple then followed this request.

[30] 'The Facial Recognition Company That Scraped Facebook And Instagram Photos Is Developing Surveillance Cameras', *Buzzfeednews*, 2 March 2020.

[31] 27 pays ont testé l'application de reconnaissance faciale de Clearview, *Nextinpact*, 28 February 2020.

[32] Clearview AI to stop selling controversial facial recognition app to private companies, *The Verge*, 7 May 2020.

provincial privacy laws.[33] Among the recommendations made, Clearview must cease offering facial recognition services to customers in Canada; it must also cease collecting, use, and disclosure biometric facial images and delete biometric facial images collected from individuals in Canada.

In Europe, the EDPB expressed doubts about the legal basis for using a service such as Clearview AI software. The Swedish DPA, the IMY, fined the local police authority € 250,000 for unlawful use of the facial recognition software to breach the country's Criminal Data Act.[34] Other DPAs also initiated investigations in France,[35] Germany,[36] and the United Kingdom.[37] The case raises as much concern about the legality as about the technical aspects. Security flaws have been identified, exposing millions of people without their knowledge.[38]

2) The PimEyes case

In Europe, a Polish company, PimEyes, launched a similar venture. They also built up an alleged database of 900 million faces from public social media profiles.[39] Unlike Clearview AI, however, PimEyes is openly available on the web.

I.2.B Fundamental rights

As the European Commission points out, the "*gathering and use of biometric data for remote identification purposes, for instance through deployment of facial recognition in public places, carries specific risks for fundamental rights*".[40] Institutions, NGOs, and human rights associations warn about the potentially detrimental effects of the technology.[41] The possibility of automated FRT risks a chilling effect on freedom of expression, freedom of association and peaceful assembly;[42] it creates an interference with the right to privacy and data

[33] *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*, 2 February 2021.

[34] Police unlawfully used facial recognition app, *IMY*, 11 February 2021.

[35] An action has been filed with the CNIL by the organization Jumbo Privacy. Jumbo Privacy brings a formal GDPR complaint against Clearview, *Jumbo Privacy*, 14 July 2020.

[36] According to the German DPA, Clearview AI's data processing activities are illegal under the European Union's General Data Protection Regulation. Clearview AI Data Processing Violates GDPR, German Regulator Says, *Bloomberg*, 29 January 2021.

[37] The British DPA (ICO) announced a joint investigation into Clearview AI with the Office of the Australian Information Commissioner (OAIC). The Office of the Australian Information Commissioner and the UK's Information Commissioner's Office open joint investigation into Clearview AI Inc, ICO, 9 July 2020.

[38] Z. Whittaker, Security lapse exposed Clearview AI source code, 16 April 2020.

[39] A Polish company is abolishing our anonymity, *Netzpolitik*, 10 July 2020.

[40] COM (2020) 65 final, p. 21.

[41] See e.g. Rodriguez K., Activists Worldwide Face Off Against Face Recognition: 2019 Year in Review, *EFF*, 30 December 2019.

[42] OHCHR *Rights to freedom of peaceful assembly and of association - Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, 17 May 2019, A/HRC/41/41; OHCHR, *Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 28 May 2019, A/HRC/41/35.
UN Human Rights Commissioner, *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, Report of the United Nations High Commissioner for Human Rights*, 24 June 2020, A/HRC/44/24; International Network of Civil Liberties Organizations (INCLO), *Facial Recognition Tech Stories and Rights Harms from around the World*, January 2021, pp. 5-8; pp 13-17.

protection,[43] and it threatens to undermine the principle of equality between all human beings and the dignity of the human person.[44]

The infringements of fundamental rights can result from flaws (I.2.B.1) and, regardless of the technical accuracy, from the technology's invasive uses (I.2.B.2).

[43] See, e.g.: FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27 November 2019; Amnesty International, *Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance*, 11 June 2020.; INCLO, Facial Recognition Tech Stories and Rights Harms from around the World, *op. cit.,* pp. 17-26.

[44] *Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, 10 November 2020*, A/75/50289; INCLO, *Facial Recognition Tech Stories and Rights Harms from around the World*, *op.cit.*, pp. 8-12.

I.2.B.1 Flaws as infringements of fundamental rights

The potential for FRT to make errors or to render individuals vulnerable harms fundamental rights, particularly when the recognition system works less well for people based on demographic qualities.[45] Thus, recognition systems that misidentify people of colour more frequently during criminal investigations violates rights of equality and non-discrimination. It is important to note however that the recognition system could work fully as expected and still undermine fundamental rights and human dignity. For example, conditioning the provision of public services on biometric identification violates right of access even if the recognition system is accurate.

I.2.B.2 Risk from the technology's invasive uses

The unchecked adoption of FRT could lead to a profound transformation of democratic societies. As identified in the literature,[46] mass surveillance is creating a "paradigm shift" for the UN Human Rights Commissioner: from targeted surveillance of specific individuals to the surveillance of all to identify some. Issues are particularly acute with live FRT in an uncontrolled environment, which permits identifying all or many people in a crowd in real-time. This system puts an end to anonymity by overturning our criminal law due process model: monitoring everyone means every citizen is a potential criminal and presumed guilty. This paradigm shift is reached by the question of the retention of the collected data threatening privacy through other freedoms.[47] In that respect, a distinction shall be made between one-to-many identification involved in surveillance systems to one-to-one authentication. Council of Europe (CoE) underlines risks are higher with identification as a database is required, while not necessarily for authentication.[48] The developments to follow concern the identification function, which presents distinct risks when deployed for mass surveillance (I.2.B.2.1) or targeted surveillance (I.2.B.2.2).

I.2.B.2.1 Mass surveillance

European Courts have yet to adjudicate the lawfulness of FRT. The Court of Justice of the European Union (CJEU) has however already ruled against devices allowing citizens' mass surveillance. In joined Cases Tele2 Sverige, the CJEU ruled that the general and indiscriminate retention of electronic communication entailed a "particularly serious" interference with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights. Electronic monitoring cause the individual "*to feel that their private lives are the subject of*

[45] See supra on bias and on the poor dataset.
[46] See e.g. Angwin J., *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, Times Books, 2014.
[47] EPDB, Guidelines on connected cars, January 2020, p.12, §60 stating on the risk of endangering privacy information through location data.
[48] CoE, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data*, recommendation 7, 2005.

constant surveillance."[49] General retention of traffic and location data should remain exceptions to the rule.[50]

The European Court of Human Rights (ECtHR) came to a substantially similar conclusion about covert surveillance generalization for counter-terrorism purposes. While the Court granted that the severity of the communications surveillance is allowed up to the context. The Court also noted that the law must provide strong safeguards against abuse. In this case, the fact that all Hungarians could be subjected to secret surveillance and that "*new technologies enable the Government to intercept masses of data easily concerning even persons outside the original range of operation*" contravenes privacy rights.

In sum, the ECtHR is likely to, and should, characterize the use of FRT for mass surveillance as an infringement of fundamental rights.

I.2.B.2.2 Targeted surveillance

Deployments of FRT to locate individuals on watchlists or to identify suspects is also a matter of concern, although the breach of fundamental rights may be more challenging to characterize. European Courts have generally adopted a casuistic approach, assessing uses and safeguards by reference to existing principles.

In other words, the Courts assess the legality of a targeted surveillance system:

- on a case-by-case basis
- based on the guarantees provided by the legislator.

The decisions from CJEU on communications data retention are instructive. According to European law, the default is that the interception of communications and related data is prohibited. Article 15(1) of Directive 2002/58 enables the Member States to introduce an exception "*where this constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security.*" In its decision, the Court affirmed that "*Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on one of those grounds."* In a case concerning electronic communications service providers, however, the Court ruled that a French law permitting mass collection of communication data by the State was unlawful because the legal safeguards provided were not sufficient to comply with the protection of privacy, personal data right, and freedom of expression.[51] The UK Court of Appeal came to similar conclusions concerning the South Wales Police's use of automated FRT.[52] The recognition system permitted capturing footage, detecting and isolating human faces, and instantaneously assessing facial measurements against a pre-established watchlist database of

[49] CJEU, *Joined cases C-203/15 and C-698/15*, §100.
[50] *Ibidem*, §104.
[51] CJEU, C-623/17, *Ibidem*, §60.
[52] [2020] EWCA Civ 1058,*Bridges R. v Chief Constable of South Wales Police*, 2020.

custody photographs. The Court acknowledge that the interference was proportionate to the state's goal of preventing and detecting crime. Nevertheless, in the Court's opinion, the legal framework was insufficient and the uses, therefore, in breach of Article 8 of European Convention on Human Rights (ECHR). Thus, the lack of adequate safeguards – rather than the targeted surveillance itself – is what is likely to determine whether there has been an infringement of fundamental rights.

European case law suggests that courts will find a violation of fundamental rights for uses of technology that:

- implement mass surveillance; or
- engage in targeted surveillance, if the legal safeguards are not sufficiently robust and adequate.

This conclusion suggests that some FRT uses are incompatible with fundamental rights (for example, real-time FRT in public spaces), and that others must be proportionate and strictly supervised.

Box 2: The Cardiff Case

The Cardiff Case

South Wales Police first experimented with automated FRT in June 2017, at the UEFA Champions League final in Cardiff. This pilot experiment was reiterated for a Six Nations tournament match, at Kasabian and Liam Gallagher's concerts and Cardiff Stadium. Civil rights activist Edward Bridges was present at one of the protests. He filed a lawsuit against the police, claiming his biometric data processing through the recognition system interfered with his privacy rights.

The High Court decision was favourable to the police.[53]

The Court held that:
1. The police's powers were sufficiently broad to justify and allow the use of the technology;[54] FRT was not considered more intrusive than CCTV on the streets;[55]
2. The British legal framework was sufficiently clear as to whether, when, and how AFR could be used;[56]
3. The use of AFR was not disproportionate and struck a fair balance.[57] The High Court argued that AFR was deployed transparently, for a limited time and a specific purpose. Furthermore, the algorithmic processing was instantaneous, and no data have been retained. The High Court also noted that no complaints about the processing were carried out, and that the three persons arrested were indeed wanted by the police.

[53] [2019] EWHC *R (Bridges) v. Chief Constable of the South Wales Police* §39.
[54] *Ibidem*, §§ 68-78.
[55] *Ibidem, loc. cit.*
[56] *Ibidem*, §§ 79-.97.
[57] *Ibidem*, § 101.

As such, the High Court dismissed the claimant on all grounds. The applicant appealed against this decision.

Following the decision, the Surveillance Camera Commissioner[58] and the British DPA[59] both issued a notice to ensure that the decision was not construed as a blanket authorization to use FRT under any circumstances.

Edward Bridges appealed the decision. In August 2020, the Court of Appeal overturned the High Court ruling.

The Court of Appeal found that South Wales Police's use of FRT breached privacy rights, data protection laws, and equality laws.[60]
For the Court of Appeal, FRT is a novel technology that involves higher risks than current CCTV.

The Court of Appeal notably held that:
1. There were "fundamental deficiencies" in the legal framework, leading to a breach of Edward Bridges' privacy rights (based on Article 8 ECHR).[61]
2. The South Wales Police did not take reasonable steps to guarantee the recognition software was bias-free on racial or gender-related grounds, whereas any public authority has to respect the equality duty.[62]

[58] *Statement on the High Court judgment on the use of Automatic FRT by South Wales police*, 11 September 2019.
[59] *Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places*, 31 October 2019, p. 5.
[60] *[2020] EWCA Civ 1058.*
[61] *Ibidem*, §§ 54-130.
[62] *Ibidem*, 163-202.

II. Facial recognition in context: cases studies and practices in public space

FRT is already a practical reality in Europe. This part presents a technical and legal overview of the uses of FRT and clarifies the challenges and limits. The aim is to address both current practices (II.1) and legal expectations (II.2) of facial recognition systems.

II.1 Practices

The following developments map out the uses of FRT (II.1.A) and describe three case studies of specific facial recognition systems (II.1.B).

II.1.A Mapping and figures

This study is based on empirical work carried out in thirteen European countries. This section discusses our methodology (II.1.A.1), provides information on the cities involved in the experiments (II.1.A.2), the contexts where FRT is deployed (II.1.A.3), the functionalities of recognition systems (II.1.A.4), the preferred industrial solutions (II.1.A.5), and, finally, a timeline of the cases (II.1.A.6).

II.1.A.1 Method

Scope of the study

This study is not exhaustive. It examines cases and the legal environment of thirteen countries: Belgium, the Czech Republic, Denmark, Finland, France, Germany, Greece, Italy, the Netherlands, Portugal, Slovenia, Spain, and Sweden. These choices were based on the national data available.

The study also refers to cases in the United Kingdom, which makes extensive use of FRT. British cases are, however, not included in the general statistics.

Sources

The sources are multiple and diverse; they consist of:

- Previous empirical studies;[63]
- Legislation, positions of the competent DPAs of the Member States, and, more rarely, law cases;
- Institutional reports;
- Official press releases;

[63] See: Lequesne-Roth C. (dir), *La Reconnaissance Faciale dans l'Espace Public – Une cartographie juridique européenne*, Rapport Fablex, 2020; also data collected by Carnegie, Carnegie Endowment for International Peace, Electronic Frontiers Foundation, Algorithm Watch, 2020. Castets-Renard C., Guiraud E. et Avril-Gagnon J., *Cadre juridique applicable à l'utilisation de la reconnaissance faciale par les forces de police dans l'espace public au Québec et au Canada Éléments de comparaison avec les États-Unis et l'Europe*, Rapport de recherche Obvia, September 2020.

- Interviews with stakeholders.[64]

The record is necessarily incomplete, due to a lack of transparency or communication in some instances.

Cases selected

The study focuses on the use of FRT in public spaces. The cases selected do not include:

- Uses of FRT in a police or judicial investigation. The study reports on police use, but not during an active investigation. Forensic use of facial recognition does not necessarily involve surveillance of the public space. It may consist of an *a posteriori* search based on a photo taken at a crime scene. The practices overlap but also raise distinct and specific issues.
- Uses of FRT by or in a private entity. Private entities are involved in making public spaces safe. However, the study focuses on FR's rollouts by public authorities (or that require their support). The study does, therefore, not address the use of FRT in workplaces. It does not either review private and commercial uses of FRT, such as unlocking systems for smartphones.

There is no clear-cut distinction between public and private space. Thus, the studies covers:

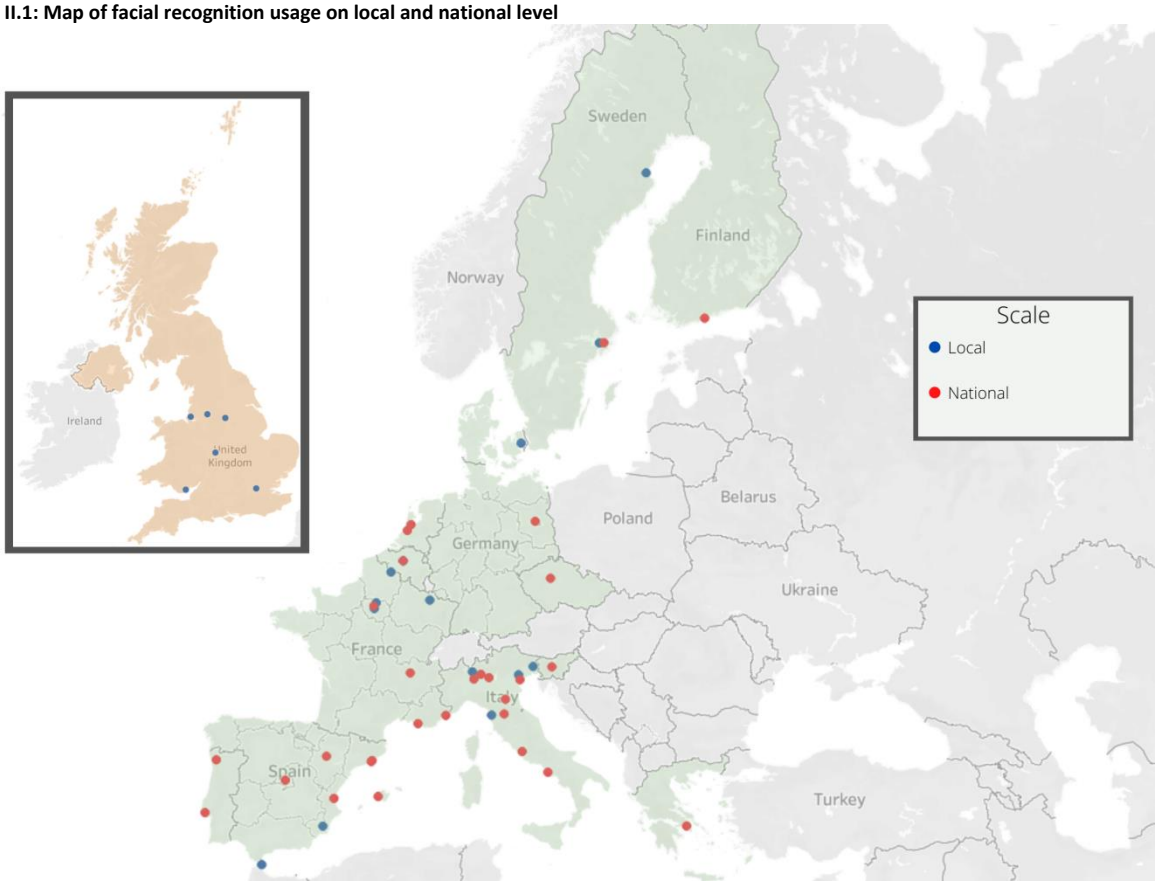
- Cases where FRT was used to manage or monitor a crowd;
- Cases that provided (or required) collaboration from public authorities.

Thus, the study focuses on FRT rollouts to secure airports, public events such as sports competitions (stadiums), or large shopping centres.

[64] See Annex B, List of Interviewees.

II.1.A.2 Facial Recognition and cities

Figure II.1: Map of facial recognition usage on local and national level



In the Member States studied, FRT has been experimented or/and introduced mainly at a local level. Experiments have also been launched at a national level,[65] but most of the time put in place at a local level or, at least, in a specific place.

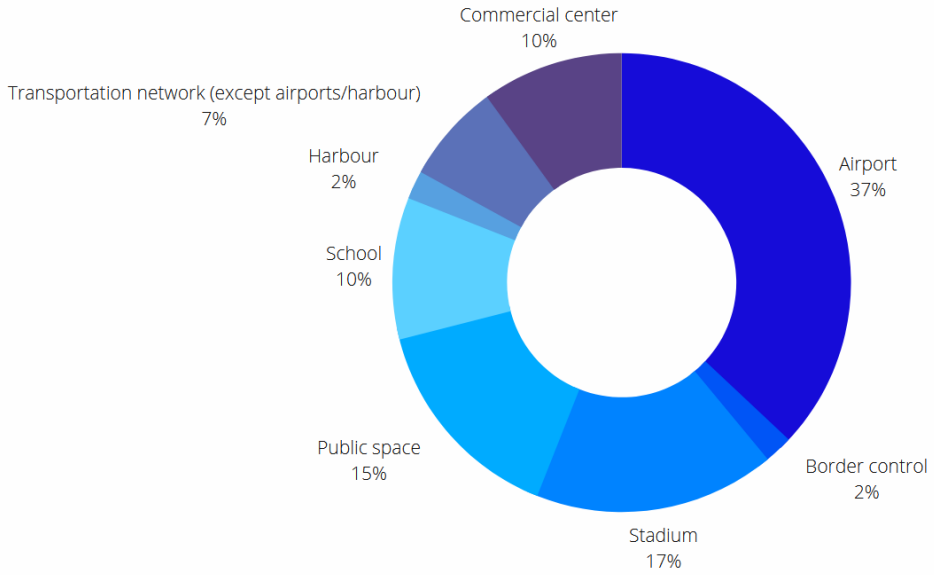
Most of the cities involved are medium-sized cities[66] or major cities,[67] even though the municipalities themselves are not always behind the experiments. There are only few public examples involving smaller cities, but some smaller cities have shown interest in FR[68] and include the technology in their smart city projects and plans. Plans by the cities of Como (83,320 inhabitants, IT)[69] and Valenciennes (43,466 inhabitants, FR)[70] provide for installing three hundred cameras with intelligent analysis functions as part of experimental projects with Huawei.

[65] In Germany, Greece, Netherlands, Czech Republic, Sweden and Portugal.
[66] With a population of less than 200,000 inhabitants. Cities concerned are: Molenbeek (BE), Ceuta (ES), Costa de Blanca (ES), Roissy (FR), Orly (FR), Metz (FR), Valenciennes (FR), Treviso (IT), Pisa (IT), Udine (IT), Como (IT), Skavsta (SW), Skelleftea (SW), Brondby (DK), Alphen aan den Rijn (NL).
[67] With a population of more than 200,000 inhabitants. Cities concerned are: Brussel (BE), Badalona (ES), Mallorca (ES), Saragossa (ES), Valencia (ES), Nice (FR), Paris (FR), Lyon (FR), Marseille (FR), Brescia (IT), Roma (IT), Napoli (IT), Bologna (IT), Venezia (IT), Milano (IT), Florence (IT), Bergamo (IT), Helsinki (FI), Ljubljana (SK), Guimaraes (PT), Lisbon (PT).
[68] See below n°72.
[69] Privacy International, How facial recognition is spreading in Italy: the case of Como, 17 September 2020.
[70] City of Valenciennes, Video-protection equipment. Huawei, Safe city Valenciennes Project., Libert M., Reconnaissance faciale: Les caméras de vidéosurveillance offertes à Valenciennes par Huawei posent question, *20 minutes*, 29 January 2020.

All the projects listed have been developed in urban areas; in rural areas, FRT is so far only considered for private and/or agricultural purposes.[71]

II.1.A.3 Areas

Figure II.2: Use of facial recognition by area



As shown in the diagram above, FRT have been used in various areas: airports, border control, ports, public spaces (streets), schools, stadiums and other public transport networks (train stations, harbours). The areas fall into three broad categories: transportation (48%), events (42%) and, more incidentally, schools (10%).

Cases in airports account for more than a third of the experiments carried out (37%, twenty-four use cases in the European Union).
According to project managers, FRT in airports meets three primary purposes:

- The control of the external borders of the European Union;
- The security of passenger transit (passenger authentication, self-boarding);
- The regulation of passenger flows.

In France, the authentication system by FRT called PARAFE[72] has played an increasing role in checking identity. It verifies travellers' identities by comparing

[71] In China and the United States, agriculture is a field of application. FRT has been experimented with to optimize cattle care and beef/dairy production.
[72] PARAFE is a French acronym for "rapid automated passage at the Schengen external borders". Decree No. 2007-1182 of 3 August 2007 on the creation of an automated processing of personal data relating to passengers of French airports crossing the external borders of the States parties to the Convention signed in Schengen on 19 June 1990 (called PARAFES), JORF No. 181 of 7 August 2007; Decree No. 2010-1274 of 25 October 2010 creating an automated processing of personal data called PARAFE, JORF n°0250 of 27 October 2010; Decree No. 2016-414 of 6 April 2016 modifying the automatic processing of personal data known as "PARAFE"; Decree No. 2019-238 of 27 March 2019 on various provisions relating to the automatic processing of personal data, known as PARAFE, JORF No. 75 of 29 March 2019.

photos taken at checkpoints with biometric passports.[73] In 2009, PARAFE gateways were set up at Roissy Charles de Gaulle airport and Orly airport. They have since been deployed at airports in Marseille-Provence, Nice, and Lyon Saint-Exupéry. The French DPA has issued clear guidance for the use of FRT at the airport.[74]

eGates with FRT have also been widely implemented in Italy,[75] in Brussel airport (BE), Ceuta border crossing (ES), Helsinki airport (FI), Ljubljana airport (SI), Skaysta airport (SE), and Greek airports.

Other transports areas include Madrid, which implemented FRT in its South Station in 2016. It is one of the most advanced deployments in Europe.[76] Recognition systems are also used in the Gare du Nord in Paris and the Eurotunnel bus departure zone (FR). Germany experimented with FRT in a train station, and Greece plans to do so in train stations and harbours in 2021. The city of Nice also mulled deploying facial recognition systems for public transport, but the experiment could not be carried out due to legal concerns.

In the United Kingdom, King's Cross Station experimented with FRT in 2018, and the technology is now implemented in Saint Pancreas train station (London), London-Gatwick, and London-Heathrow airports.

Public events

Public authorities have also tested FRT during sports and cultural events.

In Nice (FR), the experiment took place during the 2019 Carnival, which welcomes an average of 200,000 spectators each year.[77] London (GB) also experimented with FRT during the Notting Hill carnival in 2016. A 2017 FRT experiment involved the Champion's League in Cardiff.

Looking ahead, many French officials support the use of this technology as a critical component of security safeguards for the Rugby world cup in 2023 and the Olympic games in 2024.

Different stadiums have experimented with the technology to ease access or identify possible perpetrators.[78] These include AFC Ajax (NL), Brøndbyernes IF Fodbold club (DK) and Molenbeek Stadium (BE). Many countries or clubs mull widespread adoption of FRT in football stadiums. Last year, the Czech Republic announced the enactment of a new law to frame this particular use.[79] In France,

[73] Image stored in the chip.
[74] CNIL,*Reconnaissance faciale dans les aéroports: quels enjeux et quels grands principes à respecter ?*, 9 October 2020.
[75] In airport cities of Roma, Napoli, Bologna, Trevise, Venezia, Milano, Pisa, Florence, Milan.
[76] N. B. López-Molina, Spain's largest bus terminal deployed live face recognition four years ago, but few noticed, *Algorithm Watch*, 11 August 2020.
[77] This case is described below II.1.B.1.
[78] Like violent supporters banned from stadiums attending matches.
[79] Draft ministry bill allows facial recognition at sports stadiums, *Radio Prague International,* 16 February 2020.

the FC Metz also expressed a desire to use FRT to stop people banned from their stadium, to detect weapons, and to fight against terrorism. It was the opinion of the French DPA, however, that implementing such a scheme by a sports club to "*fight against terrorism*" was unlawful."[80] Italy also considered equipping football stadiums with the technology as "*an essential tool in the fight against racism*."[81]

The use of FRT has sometimes been reported in commercial centres. Cases include the second-largest supermarket chain in the Netherlands[82] and some Spanish[83] and British malls (Westfield commercial centre in London, Trafford Centre in Manchester, and Meadowhall in Sheffield).[84] The latter required collaboration with police authorities.[85]

In the United Kingdom, and for the same purpose, FRT was also implemented in a museum (The World Museum in Liverpool).[86]

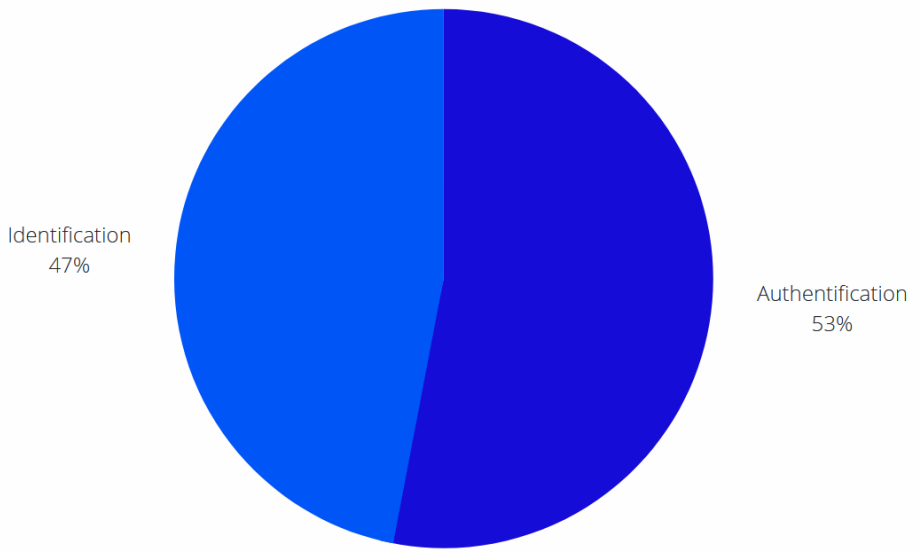
Schools

Experiments in schools were planed - or carried out (but not renewed) – in Spain,[87] France (in Nice and Marseille) and Sweden (in Skellefteå). DPAs ruled the last two to be unlawful.[88]

[80] CNIL, *Reconnaissance faciale et interdiction commerciale de stade: la CNIL adresse un avertissement à un club sportif*, 18 February 2021.
[81] Chiusi F., In Italy, an appetite for face recognition in football stadiums, *Algorithm Watch*, 2020.
[82] Panasonic,Case study, 2018.
[83] Protección de Datos investiga el sistema de reconocimiento facial de Mercadona, *El Diario*, 6 de julio de 2020.
[84] Lequesne-Roth C. (dir), *La Reconnaissance Faciale dans l'Espace Public – Une cartographie juridique européenne*, *op. cit*, pp.118-119.
[85] Notably in Manchester where the experiment led to arrests. What Do They Know, *Freedom Of Information Request Reference No: 002927/18*, Great Manchester Police, November 2018.
[86] According to the museum however, the system would not have been used to date: WHAT DOES THEY KNOW, *FOI request 19/06*, National Museums Liverpool, September 2019.
[87] Asenjo A., « Un instituto catalán está usando reconocimiento facial para controlar la asistencia a clase, algo por lo que ha sido multado con 19.000 euros un colegio sueco », *Business Insider*, 19 September 2019.
[88] See below n°84.

II.1.A.4 Functionalities

Figure II.3: Functionalities of implemented FRT



A primary use (53%) FRT is authentication, that is, to verify identities in a controlled environment. Yet identification systems (47%) are a bit less deployed (or renewed after an experiment). Two factors can explain this discrepancy: reliability and legal impediment. Facial recognition systems are indeed more vulnerable to technical vulnerabilities in uncontrolled environments, and identification raises additional legal challenges, as it may lead to mass surveillance.

Researches also widen FRT to emotion detection.[89] The technology is currently used to assess job applicants[90] and presented by the industry as a crime detection tool. Such systems purport to recognize anger and distress by reading facial expressions and behaviours.[91]

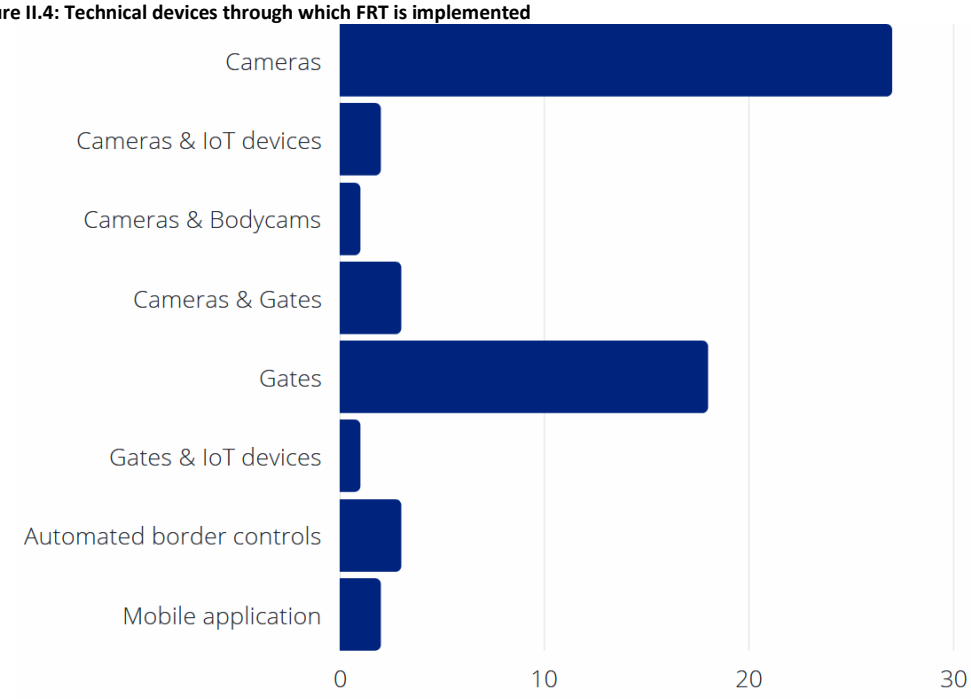
According to the French media, the city of Nice considered experimenting with such functionality in public transports,[92] but the project never materialized. The city has been experimenting with the technology[93] within its internal services, but the tests carried out were not conclusive enough to consider further deployments.[94] In the United Kingdom, an experiment supported by the Home Office would be ongoing in the Lincolnshire Police. The recognition system would allow searching for specific moods and facial expressions on CCTV.[95]

[89] On the subject, see: K. Crawford, « Time to regulate AI that interprets human emotions », *Nature*, April 6, 2021.
[90] Harwell D., A face-scanning algorithm increasingly decides whether you deserve the job, *The Washington Post*, 6 November 2019.
[91] Harris M., An Eye-Scanning Lie Detector Is Forging a Dystopian Future, *Wired,* 12 April 2019.
[92] Ill V., Un logiciel pour décoder les émotions des usagers du tramway de Nice, *France Bleu*, 4 January 2019.
[93] Which it distinguishes from FRT.
[94] According to the Municipal Police.
[95] Hamilton F., Police facial recognition robot identifies anger and distress, *The Times*, 15 August 2020.

These programs raise concerns as the method is contested, or "*deeply flawed*" as the American Association for Psychological Science put it.[96] A study reviewing more than a thousand papers on emotions detection concluded that "*it is very hard to use facial expressions alone "to tell how someone is feeling" accurately*".[97]

II.1.A.5 Industrial aspects

Figure II.4: Technical devices through which FRT is implemented



Recognition systems and devices

FRT may be implemented through different systems and devices. For authentication purposes, like in airports, special gates or automated border controls have been broadly adopted. In all other cases, FRT has been deployed in connection with closed-circuit television (CCTV). It is worth noting that acquiring new cameras is not necessarily required. In Nice, software allowed experimentation with FRT using the current CCTV system. Cameras could also be connected to other devices like IoT, bodycams, or a mobile application.

Box 3: The future of facial recognition

The future of facial recognition

The latest FRT innovations result from technological convergence: industrial developments concern video analytics with FRT (1) and FRT in drones (2).

1. Video analytics with facial recognition

[96] Feldman Barrett L. et al., Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, *Psychological Science in the Public Interest 20*, 2020, no.1: 1–68. cited by CHENARCHIVE A., Computers can't tell if you're happy when you smile, *MIT Technology Review*, 26 July 2019.
[97] *Ibidem*.

According to the Electronic Frontier Foundation (EFF), video analytics in law enforcement or private security context refers to "*using machine learning, artificial intelligence, and computer vision to automate ubiquitous surveillance.*"[98] This type of technology is widespread in the United States. In 2020, thirty-five American law enforcement agencies used it. Software such as "Briefcam" can identify all video sequences where a face appears.[99] Other software, like "Aviglion," offers to detect and "*predict unusual events*."[100] The implementation of FRT allows the creation of watch lists to facilitate identifying individuals and tracking movement.

A similar system has also been deployed in Brazil. ViaQuatro, the vendor for the São Paulo public metro system, implemented an AI crowd analytics system from AdMobilize, that claims to "*predict the emotion, age, and gender of metro passengers without processing personal data*."[101]

The effectiveness, ethics, and legality of these tools are highly controversial. According to the EFF, law enforcement agencies should not rely on this or any technology whose validity and reliability remain uncertain. The risk of infringement of fundamental rights is all the more significant insofar as these systems increase reliance on automation. In August 2018, the Brazilian Institute of Consumer Protection (IDEC) filed a public civil action against ViaQuatro, claiming it violated the consumer and personal data legislation. The judge ruled on a precautionary measure, requesting ViaQuatro to stop collecting data and to remove the cameras. ViaQuatro complied with the order, while the case continued.

In Europe, the detection of demographic characteristics (like gender or age) to display targeted advertising raised similar legal concerns. The Dutch DPA recalled that the consent of passers-by was systematically required for this type of processing.[102] In France, the Conseil d'Etat refused JCDecaux the right to study the flow of pedestrians using their mobile phones, since data anonymization was not guaranteed.[103]

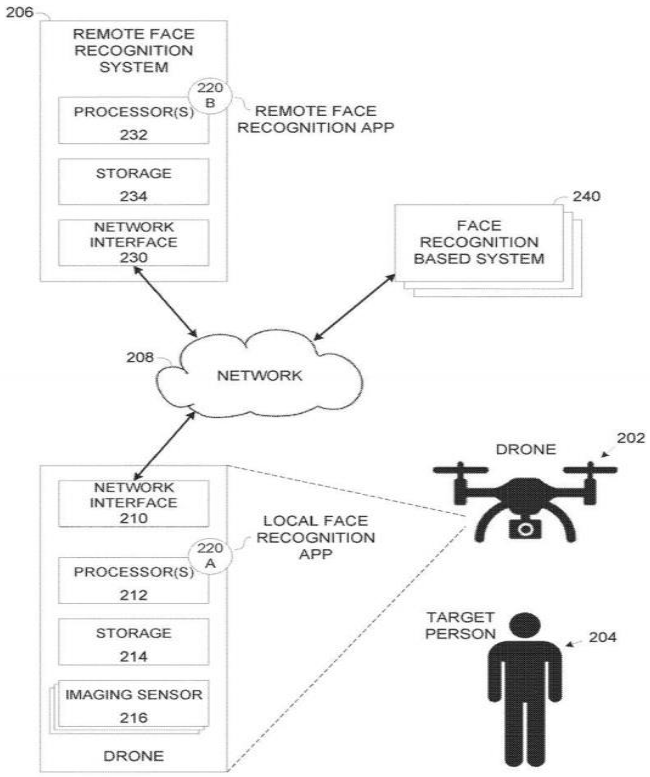
In summary, video analytics raise many concerns, and their deployment is likely to be legally disputed.

2. Drones with facial recognition (drones combined with aerial cameras)

The arms industry has initiated research into drones with FRT systems. In 2019, AnyVision, an Israeli company, filed a patent application on the "*adaptative positioning of drones for enhanced face recognition*."[104] The technology aims to help the military find targets. The military drone captures and analyses images. The machine learning model seeks to identify whether the person photographed is the wanted person through a "*classification probability score*."[105]

[98] Maass D., Guariglia M., Video Analytics User Manuals Are a Guide to Dystopia, *EFF*, 19 November 2020.
[99] *Ibidem.*
[100] *Ibidem*
[101] Arroyo V., Leufer D., Facial recognition on trial: emotion and gender "detection" under scrutiny in a court case in Brazil, *Access now*, 29 June 2020.
[102] Autoriteit Persoonsgegevens, *Brief branche normkader digitale billboards*, 25 June 2018.
[103] CE, JC Decaux n°393714, 8 February 2017, confirming the CNIL's veto Délibération 2015-255, 16 July 2015.
[104] Anyvision Interactive Technology, Adaptive Positioning of Drones for Enhanced Face Recognition, *United States Patent & Trademark Office*, 4 February 2021.
[105] Bates Ramirez V., Facial Recognition Drones Will Use AI to Take the Perfect Picture of You, *Singularity Hub*, 23 February 2021.

Figure II.5: FRT in drones[106]



In addition to weapons, the first commercial applications of drone FRT have emerged over the past two years. In 2019, Amazon.com Inc. obtained patents related to a delivery drone equipped with FRT.[107] These "Prime Air" drones would seek to determine whether the customer is the right person by asking for a code, scanning their retinal fingerprint, or using a FRT.

These systems have not been adopted in Europe, but some countries have used drones to monitor compliance with pandemic containment measures.[108] As a legal matter, the Court of Justice's case law on the capture of images by an electronic device,[109] such use of drones constitutes processing of personal data and thus requires necessity and proportionality for each use. In the absence of a specific law, these systems' adoption led to divergent positions from DPAs, ranging from authorization (Spain) to prohibition (France).

Technical operators[110]

Information about providers was not available for some cases (in Sweden and Portugal). Interviewees for this report expressed concerns about European technological sovereignty and dependency on foreign providers. For European

[106] Brewster T., Drones With Facial Recognition Are Primed To Fly—But The World Isn't Ready Yet, Forbes, 15 February 2021.
[107] Capriel J., Drones that recognize you? Amazon has a patent for that, *Biz journals*, 21 August 2019.
[108] In fight against coronavirus, governments embrace surveillance, *Politico*, 24 March 2020.
[109] CJEU, case C-212/13, *Frantiscaronek Rynescaron; c/ Úrad pro ochranu osobních údaju*, 11 December. 2014; CJEU case C-345/17, 14 February 2019.
[110] Lequesne-Roth C. (dir), *La Reconnaissance Faciale dans l'Espace Public – Une cartographie juridique européenne*, *op.cit.*, pp. 40-41.

institutions, providing a legal framework is required to support a competitive emerging technology industry in Europe.

The table below lists the nationality of FRT providers. Most companies are European (domestic), but public authorities have also made extensive use of recognition systems from Japanese companies (seven countries) and, more incidentally, Israeli and American companies.

Table 1: Nationality of providers of FRT to European countries

Country	Domestic Providers	European Providers	Non-European Providers
Belgium	Yes		Japanese
Czech Republic	Yes		Japanese
Denmark			Japanese
France	Yes	Monegasque, Dutch	Israeli, American, Chinese
Finland	Yes		
Germany	Yes	French, English, Swiss	Japanese, American
Greece	Yes		
Italy	Yes	Spanish, Portuguese, German	Japanese, Israeli, Chinese
Netherlands	Yes	French	Japanese
Portugal			
Slovenia		Spanish, Dutch	
Spain	Yes		Israeli
Sweden			
UK	Yes	Portuguese	Japanese

Chinese technology raises particular concerns around fundamental rights. China has engaged in a proactive policy to shape FRT standards and submitted a new ITU standard. Human rights lawyers criticized the proposal as a "*crossing the line from technical specifications to policy recommendations*" that would "*restrict human rights*". Thus far only one Chinese company (Huawei) has played a role in just two of the cases (Valenciennes, FR; and Como, IT) identified. Some concerns remain, however, as many European companies,[111] looking for a testing ground, may comply with Chinese market standards to deploy their technology in China.[112]

In-house solutions

In addition to the provider's nationality, there is also the question of using external vendors for public functions. The use of commercial tools offers a quick solution

[111] These are the French company Morpho (now Idemia) that provided facial recognition to the Shanghai Public Security Bureau, the Swedish company 'Axis Communications' that delivered surveillance cameras for the Skynet and Sharp Eyes projects, and the Dutch company 'Noldus Information Technology' that sold emotion recognition and behaviour analysis tools to various Chinese bodies, including the Chinese Ministry of Public Security; Amnesty International, *Out of control: Failing EU Laws for Digital Surveillance Export*, 2020, p.7.
[112] [2020] EWCA Civ 1058 §199.

and allows the mobilization of sharp expertise. This choice has consequences in terms of dependency, transparency, and responsibility. On the one hand, industrial secrecy can restrain recognition systems' audits and compromise the obligation of transparency incurred to administrations. The problem arose during the dispute about Cardiff police use of FRT. An audit was requested to establish evidence of potential biases. The company which provided the recognition system refused, invoking business secrecy. The Court recognised that details of the training dataset could not be made public due to "*commercial confidentiality*", but also held that "*it [did] not enable a public authority to discharge its own, non-delegable, duty*".[113] In addition, public authorities can be locked into possible evolutions and updates of the company's systems, which may also trigger additional costs. Finally, a commercial solution implies that a company may be in charge of police law enforcement and sensitive data processing. This delegation could contravene some national principles[114] and involves risky data practices.

Conversely, in-house solutions present several advantages. In particular, the involvement of field stakeholders in constructing the tools increased understanding of the technology and its limits. They allow for a reduced technological and data dependency on the private actor and offer more levers to guarantee transparency.

Among the cases studied, in-house solutions are less developed for now but are growing. There are at least two examples, in Sweden and the Netherlands. For the project at Skavsta airport, the Swedish Police planned to develop its own facial recognition system. The in-house solution was supposed to be adopted as well for external border control. The project was, however, cancelled by the Swedish DPA due to insufficient guarantees.[115] For its identification program ("Catch"), the Dutch police also used an in-house solution developed by the *Dienst Landelijke Operationele Samenwerking* (Biometric Centre of the National Office for Operational Cooperation).[116]

In addition to the cases studied, other interesting initiatives (including research partnerships) were carried out in connection with FRT uses.

In the Netherlands, the National Police Lab AI - a cooperation initiative between the Dutch police, Utrecht University, and the University of Amsterdam - aims to develop "*state-of-the-art AI techniques*." The current project involves machine-learning techniques for extracting relevant information from different sources such as photos, text, and video.[117]

[113] *Ibidem*.
[114] In France, delegating police missions is prohibited. See: CE, Ass., Ville de Castelnaudary, 17 June 1937.
[115] Datainspektionen, *Lagändring krävs för att polisen ska kunna utföra testverksamhet av ansiktsverifiering på flygplats*, 16 December 2019.
[116] Lequesne-Roth C.(Dir), *La Reconnaissance Faciale dans l'Espace Public – Une cartographie juridique européenne*, *op.cit.*, p.39.
[117] Innovative Center for Artificial Intelligence, Police Lab AI.

In Germany, after the assaults on women outside a train station on New Year's Eve 2015, the Cologne police have entered into a partnership with Microsoft to develop their own AI tools. The collaboration strives to improve crowd and online police identification systems. According to the Cologne prosecutor's office, the unit did not hire in-house data-scientists, but prosecutors would be able to review "*the steps Microsoft and other partners take in writing code for the tools*."[118]

Box 4: In-house solutions for AI-based predictive policing tools

In-house solutions for AI-based predictive policing tools

A growing number of in-house solutions have been developed for predictive policing[119] in Europe.

In France, the national *gendarmerie* has developed software ("*Paved*") to assist in decision analysis in the fight against crime.[120] It provides a map of burglary and violence crime to assist the gendarmerie in deploying resources. The national gendarmerie intends to extend this tool to "*all crises that require its intervention.*"[121]

Other in-house predictive police systems include:

- the CAS system (Crime Anticipation System) implemented in 2015 in the Netherlands by the Amsterdam police;[122]
- Precobs (Pre-Crime Observation System), developed by the German Institute for Pattern-based Prediction Technique (*Institut für Musterbasierte Prognosetechnik* (IfmPt)) (www.ifmpt.de) in 2011 and deployed in Germany (*Länder of Bavaria and Baden- Württemberg, Berlin and Munich*) and in Zurich (*Switzerland*);[123]
- The police's Keycrime software in Milan, Italy, which also results from a partnership with the police.[124]

While it has advantages, the development of in-house solutions faces a double impediment:

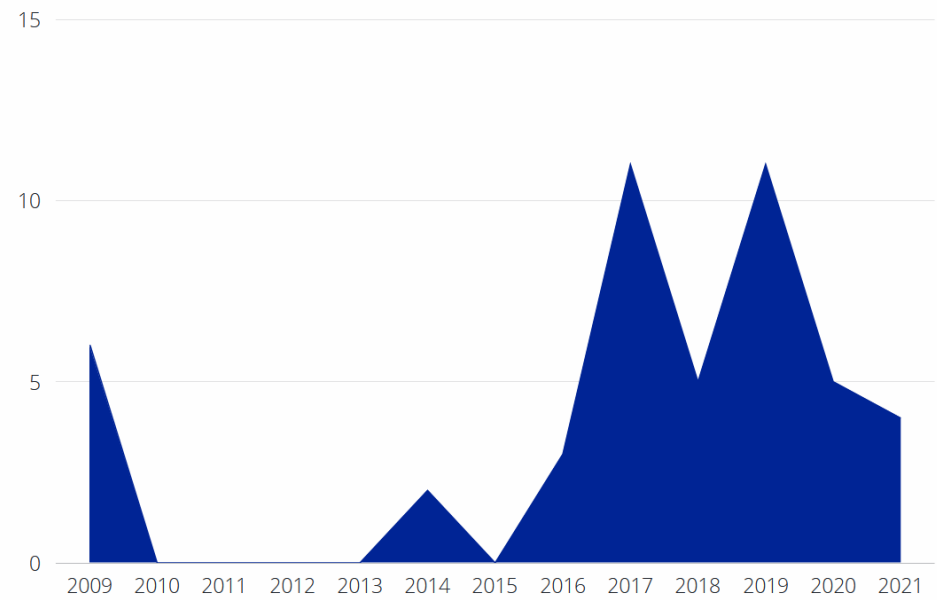
- **Recruitment:** In some countries, the public sector would be less attractive for data-scientists than the private sector. Several institutional underlined the difficulty, especially in France.
- **Budgetary constraints:** Researchers also mention budgetary constraints, which would impede technological investments.[125]

[118] Stupp C., German Prosecutors Are Building AI In-House, *Wall Street Journal*, 26 February 2021.
[119] Even though commercial applications' use remains primary.
[120] Castets-Renard C., Besse P., Loubes J.-M. et PerrusselL., *Encadrement des risques techniques et juridiques des activités de police prédictive*, Rapport 2019 CHEMI, ministère de l'Intérieur, 12 July 2019, p.13.
[121] Sénat, *Rapport n° 621*, 9 July 2020, p. 36.
[122] C. Castets-Renard, P. Besse, J.-M. Loubes et L. Perrussel,*op.cit.*, 2019, p.32
[123] *Idbidem*, p.33.
[124] *Ibidem*.
[125] Stupp C., German Prosecutors Are Building AI In-House, *op. cit.*

II.1.A.6 Timeline

Although some experiments were carried out before 2010, most of the cases studied took place over 2016-2020.

Figure II.6: Timeline of experiments with the use of FRT



It is worth noting that the global Covid-19 pandemic did not change the trajectory of the FRT in Europe; it instead accelerated the widespread of technology.

On the one hand, the crisis contributes to accelerating the implementation of current authentication systems – for example, to facilitate contactless boarding at airports[126] or to implement vaccine passports.[127] On the other hand, the crisis has contributed to renewing the uses. Several researches and companies reported training algorithms on masked faces databases,[128] and the technology was used, on an experimental basis, to ensure masks were worn. The city of Cannes[129] and

[126] See e.g.: Tamir I., *Facial Recognition at a Crossroads: Transformation at our Borders and Beyond*, 30 September 2020, Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC), 2020.

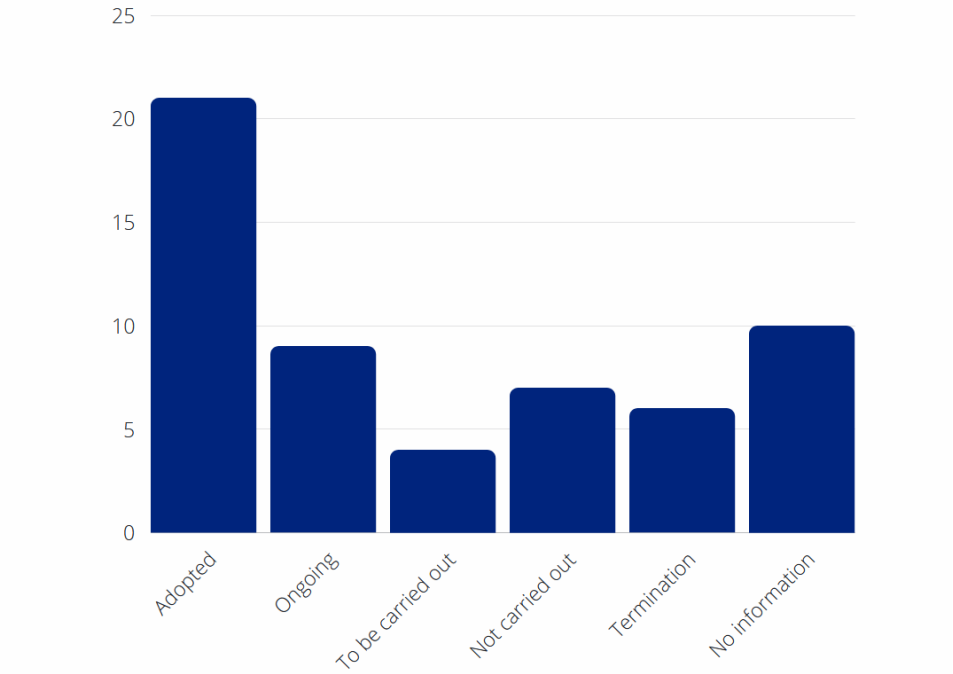
[127] Face-scanning at pubs could offer key to vaccine passports, *The Times*, 27 March 2021.

[128] See e.g.: Mundial I. Q., et al, Towards Facial Recognition Problem in COVID-19 Pandemic," *4rd International Conference on Electrical, Telecommunication and Computer Engineering (ELTICOM)*, Medan, Indonesia, 2020, pp. 210-214.

[129] A Cannes, des tests pour détecter automatiquement par caméras le port du masque, *Le Monde*, 28 April 2020.

the Paris metro[130] both rolled out experiments.[131] The French DPA position contributed to stop them,[132] but a Decree later regularized their use.[133]

Figure II.7: State of play for on-going and completed FRT projects



The figure above shows the status of the projects. It distinguishes six statuses:

1. Adopted: project implemented permanently.
2. Ongoing: experiments in progress
3. To be carried out: projects or experiments announced but not yet conducted;
4. Not carried out: experiments abandoned before their completion;
5. Termination: experiments completed but not renewed or implemented permanently
6. No information was given on the state of progress.

It is interesting to note that the majority of cases did not result in a permanent deployment. The implementation of FRT in the public space remains experimental, and the deployment dynamic is slow.

Among the known causes of suspension or non-deployment, the DPA's unfavourable opinion or investigation are the most common reason given.[134]

---

[130] La RATP va tester des caméras « intelligentes » pour mesurer le taux de port du masque dans la station Châtelet, *Le Monde*, 7 May 2020.

[131] It is important to note that these systems do not necessarily involve identifying individuals (only identifying faces, without recognition system), thus distinguishing themselves from the recognition systems discussed above. For the French DPA, they are more akin to video analysis systems. CNIL, *La CNIL appelle à la vigilance sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques*, 17 June 2020.

[132] According to the CNIL, the use of these systems in the public space is not compliant with the GDPR as it does not allow individuals to exercise their right to object. *Ibidem*.

[133] Décret n° 2021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports, 10 March 2021.

[134] Authorities are often reluctant to communicate the reasons for project termination.

II.1.B Use cases

The deployment of FRT in public space is a process. The three cases described below illustrate its challenges and impediments from a field perspective: the experiment carrying out during the Nice Carnival (FR) (II.1.B.1), the experiment in Berlin's transport system (DE) (II.1.B.2), and the equipment of Athens police force (GR) (II.1.B.3).

II.1.B.1 Nice, France

What

Experimentation with facial recognition software implemented within a surveillance camera network, aimed at identifying certain individuals in an uncontrolled environment.[135] This case was the first experiment carried out in public space in France.

Main objectives

Leveraging technology to:

- Locate a vulnerable person: a lost child, a person with dementia;
- Locate a fleeing suspect;
- Identify a person of interest banned from an event.

The police tried out different scenarios to assess the added value of the technology for the field agents.

Where

At the Nice Carnival.

When

February 16, 19 and 20, 2019.

Technical details

The report does not provide many technical details.[136] Two kind of control were tested:

- *One-to-one access control*, to identify people authorized to access the event in the queue.

[135] Nearly 5,000 people passed through the gates housing the facial recognition software. City of Nice, Facial Recognition Experiment, 2019.
[136] The city stated that the report did not aim to provide these details.

- *On-the-fly control,* to locate and identify certain people in the crowd. In this case, the Urban Supervision Centre informed the field agents when the system recognized a person of interest.[137]

The experiment was carried out in different environments and contexts: daytime, night-time, in a lighted or darker area.

The facial recognition software was provided by the Monegasque company Confidentia, which used Israeli company AnyVision's technology. According to the municipal police director, the experiment hoped to assess whether significant advances by AnyVision resulted in better performance in uncontrolled environment.[138]

Data & databases

The experiment consisted in identifying volunteer local agents in the crowd using a database pre-loaded with their pictures. According to the police, biometric data collected were kept for 0.2 seconds, the time required to query the database. They were then deleted, except when there was a match. In their words, the company provided a "*privacy by design solution*": storage time was "*configurable*", data were "*encrypted*", "*hosted in GDPR countries*" and "*could be anonymized*".[139]

Notice

The police implemented three notice measures:

- Information displayed at the entrance concerned by the experiment, in four languages;
- Distribution of notice to people who consented to participate and a bracelet to embody the consent;
- Distribution of a bracelet to signify consent.

Costs

The city and the company entered into a loan equipment agreement. The city did not pay for its use for the pilot. The city decided to experiment with this specific technology because it offers the prospect of low additional investment: the software can be deployed in the existing camera network, obviating the need for new investments. If the city wished to adopt this system at the end of the

[137] Interview with Sandra Bertin, Nice Municipal Police Director, February 2020, reported in LEQUESNE-ROTH C. (dir), *La Reconnaissance Faciale dans l'Espace Public – Une cartographie juridique européenne*, *op. cit.* Annexe.

[138] "*This technology has optimal characteristics since it can recognize a person from a database, in record time, under optimal conditions. The minimum condition for the photo to be usable is that it be 45x45 pixels. It is a very low resolution. It can identify people at 300 meters, at night, in a lit area, in a less well-lit area, as long as you can still see the face, of course. In three years, [AnyVision] was the first that interested Nice's city and which stood out. From a technical point of view, it seemed bluffing. Today, we know very well that facial recognition and the biometric system of airports work very well., The city's challenges are however specific, and it is interesting to see in real and delayed time, in the general and daily context, what added value this type of tool with artificial intelligence has*", *Ibidem*.

[139] *Ibidem*.

experiment, a tender procedure in accordance with public procurement law should however be opened.

Results

The report makes no mention of any mistake or mismatch. Police said there were no false positives.[140] In their report, police forces and local authorities underlined the "*speed of biometric identification*", "the proper functioning and the efficiency of the software", and its "*high reliability*".[141]

Legal concerns

Even though no authorization is formally required, exchanges with the French DPA guided the City in shaping the experiment. Based on CNIL recommendations, the police narrowed the scale to a predefined area. While the police intended to equip all gates of one entrance with the software, CNIL considered this solution did not provide free and informed consent required. The City had to offer an immediate alternative that did not involve going to another entrance. As a result, two entrances (on five) were involved in the experiment, and in each, the gates with FRT were marked. Police said that the time scale was also reduced on the CNIL's recommendations (three days instead of fifteen expected).

The Mayor of Nice declared the experiment was endorsed by the CNIL. According to the municipal police, the DPA local correspondent helped the city design the experiment at each stage, and the city "*complied with all recommendations*." After the experiment, the CNIL formally asked for further details concerning the software's effectiveness and any impacts of possible bias.[142] It regretted "*the urgency in which its services were solicited*" - less than a month before the planned experiment – and under "*circumstances not likely to favor analytical work*".[143]

At the end of the experiment, both the City and the CNIL publicly deplored the lack of clear and adequate legislation.

II.1.B.2 Berlin, Germany

What

The project aimed at experimenting with live FRT in a train station. The German Federal Police, the Federal Criminal Police Office, and the Ministry of the Interior carried out the project in collaboration with Deutsche Bahn.[144]

---

[140] *Ibidem*.
[141] *Ibidem*.
[142] Untersinger M., Reconnaissance faciale: la CNIL tique sur le bilan de l'expérience niçoise, *Le Monde*, August 2019.
[143] *Ibidem*.
[144] Big brother in Berlin: Face recognition technology gets tested, *Deutsche Welle*, 31 July 2017.

Where

Berlin Südkreuz train station.

When

From August 2017 to February 2018.

Technical details

Three cameras from different suppliers filmed a specific entrance and an escalator leading to the station platform. Facial recognition software compared the surveillance images collected with the photos stored in the database.

Who

The experiment involved 300 volunteers, mainly commuters. The experiment consisted of testing the system's reliability by comparing volunteers' photos stored in a database with the surveillance images.[145] The volunteers wore small transmitters to inform the system that they were in the camera's field of vision. An incentive mechanism was provided: volunteers who visited the experimental area most often were rewarded (Amazon gift vouchers, Apple Watch).[146]

Results

According to the Ministry of the Interior, 80% of the people were correctly identified. The Chaos Computer Club challenged these results. The hacker activist association raised various inconsistencies in the reported results (notably similar success rates between cameras from different providers).[147]

Legal action and concerns

In the aftermath of the 2016 Berlin Christmas market attacks, the experimentation was presented as part of the fight against terrorism and crime.[148]

The experiment did not meet with strong support from Berliners, and some civil rights groups challenged its legality. According to Netzpolitik and CILIP, the use of FRT violated paragraph 27 of the Federal Police Act (*Bundespolizeigesetz* – BPolG). In their view, this provision only allowed the authorities to use cameras to zoom in on people and not to process their biometric data through an automated processing system.[149]

---

[145] *Ibidem.*
[146] German police seek volunteers for facial recognition surveillance, *Deutsche Welle*, 19 June 2017.
[147] Germany and facial recognition tech: a love affair, *Fairplanet*, 11 January 2019.
[148] Big brother in Berlin: Face recognition technology gets tested, *op.cit.*
[149] German police seek volunteers for facial recognition surveillance, *op.cit.*

The extension of paragraph 27 of the BPolG to intelligent video surveillance is not unanimously construed within legal literature.[150] The Bundestag, however, found out in 2016 that rolling out such technology required a legislative revision,[151] as did the German DPA.[152] The Federal Minister of the Interior supports a different interpretation. In his view, Article 27 allows for the automated processing of facial images. [153]

The DPA authorized the experiment but expressed "*fundamental reservations*" about the technology's further use.[154] The DPA also criticized the authorities' lack of transparency[155] and failure to provide the final report, despite repeated requests.[156] In 2019, the DPA s firmly recommended not to use video surveillance with biometric FRT in public spaces. The DPA is concerned about the risk of surveillance expansion that FRT would allow.[157]

In 2020, a bill authorizing FRT in one hundred and thirty-five German railway stations and fourteen airports was discussed but finally abandoned.[158]

II.1.B.3 Athens, Greece[159]

What

Real-time FRT during police patrols, implemented in smartphone-like devices for police officers.

According to the press releases, the device "*consists of core building blocks related to face recognition, automated fingerprint identification, security documents processing and verification of authentication, complex information searches to legacy and new databases, as well as correlation of information from the aforementioned records*".

Where

It is a national-scale project. No information on the first cities/regions concerned with the roll-out was provided, but the headlines mention Athens.

---

[150] Deutscher Bundestag, *Rechtsgrundlage für den Einsatzsog. intelligenter Videoüberwachungdurch die Bundespolizei*, 2 September 2016, p. 3.
[151] *Ibidem.*
[152] *Ibidem.*
[153] Monroy M., German authorities improve face recognition, *Digit,* 31 January 2020.
[154] Big brother in Berlin: Face recognition technology gets tested, *op. cit.*.
[155] For example, some of the details were reportedly made known to the DPA through the press, such as the use of active transponders.
[156] BfDI *Extracts from the 2017/2018 Activity Report of the Federal Commissioner for Data Protection and Freedom of Information*, 27th Activity Report, p.42-43.
[157] BfDI, *Activity Report 2019,* 28th Activity Report on Data Protection, p. 47-48.
[158] Seehofer verzichtet auf Software zur Gesichtserkennung, *Der Spiegel,* 24 January 2020.
[159] It should be mentioned that the research work only relies here on two sources of information: Algorithm Watch Annual report (Automating society, January 2021) and Homo Digitalis association publications (EDRi, Homo Digitalis calls on Greek DPA to speak up, 1 April 2020). The official documents were only published in Greek.

When

The project is supposed to start in the summer of 2021. In the first phase, the police will receive one thousand mobile devices, with an option of nine thousand more in the future.

Technical details

Police officers will use the smartphone-like devices on patrol to identify individuals in a two-steps process:

- First, the device will take close-up photos of an individual's face and collect their fingerprints.
- Secondly, the collected biometric data will be compared with stored data, and the identification results displayed on their devices.

Database

The operating system relies on a network of twenty databases held by national and international authorities. Among the databases listed are those of the Greek Ministries of Transport, Interior and Foreign Affairs, Europol, Interpol, the FBI, and Teiresias, a credit bureau owned by Greek banks (this list is not exhaustive).

Costs

Following a public tender, the €4 million project was ordered in March 2019 from Intracom Telecom, a Greek-based telecommunications company. Through its Internal Security Fund (ISF), the European Commission covered 75% of the costs.

Legal action and concerns

On 19 March 2020, Homo Digitalis requested the Greek DPA's opinion regarding the contract between the Hellenic Police (EL.AS) and INTRACOM TELECOM.[160] Based on the provisions of Greek law 4624/2019, transposing Directive 2016/680 (LED), the association requested the following clarifications:

- Was the DPA consulted in advance by the Hellenic police?
- What safeguards had been adopted to prevent and limit the infringement of fundamental rights?
- On what legal provisions were the data processing based?

According to the association, based on the contract:[161]

- The processing and collection of biometric data during police controls were not legally founded.

[160] *Homo Digitalis' request for opinion to the Hellenic DPA* (only in Greek), 19 March 2020.
[161] *The technical specifications of the smart policing contract* (only in Greek), 12 April 2018.

- The system's necessity was not characterized, as current identification methods were less invasive.

Furthermore, the association argued that before any processing, the police had to carry out a data protection impact assessment (DPIA) and consult the DPA.

In February 2020, the Greek police published an open letter in which the questions raised were not answered, particularly regarding the conduct of a DPIA.[162]

The Greek DPA then announced the opening of an investigation, which was concluded in August 2020. The authority stated that the police cooperated, but the results have not yet been published.[163]

[162] *Press Release of Hellenic Police* (only in Greek), 14 December 2019.
[163] Homo Digitalis calls on Greek DPA to speak up, See above *n°61.*

II.2 Social acceptability and local expectations

The deployment of technology also has societal underpinnings. From this point of view, its social acceptance appears decisive (II.2.A), as do the public authorities' expectations that shape its deployment (II.2.B).

II.2.A Public reception

There are no Europe-wide studies that assess the social acceptability of FRT. Such a study would be difficult given national differences that rest on cultural beliefs,[164] values, and history.[165] For instance, while Germans reacted adversely to the government's plan to use automatic FRT at railway stations and airports,[166] most participants in a United Kingdom study (80%) felt comfortable with the same use case "because it is beneficial for the security of society."[167] Another survey indicates that only 3,8% of 900 respondents interviewed during Nice's experiment were opposed to the use of FRT.[168]

Social acceptability also depends on the type and purpose of the uses. The same British survey concludes that 70% of the respondents support the use of FRT by police in criminal investigations, but only 6% support it to monitor pupils' expressions and behaviour at school, and 4% to monitor candidates' personality traits and mood when hiring a job.[169] In the survey carried out in Nice (FR), 83,1% of the respondent were in favour of the use of FRT for locating lost children, 80% for providing assistance to a vulnerable person, 80,3% for securing a gathering place, 78,5% for checking the identity of individuals in transit areas such like an airport and 81,7% for locating a wanted person;[170] however 96,5% consider these uses should only be allowed within the bounds of strict regulations.[171] The European Agency for Fundamental Rights (FRA) also suggests that acceptability might change rapidly over time, regarding both the fast development of the technology and people's exposure to such technology.[172]

Nevertheless, there is evidence of the public's increasing concerns about fundamental rights interference. This has led to legal campaigns and action against surveillance experiments. In January 2021, the European Commission has registered a European Citizenship Initiative for a ban on biometric mass surveillance. The movement *Reclaim your Face* calls on the Commission to

---

[164] Privacy as a cultural consideration is an issue and a challenge that go well beyond biometrics. See: National Research Council, Cultural, Social, and Legal Considerations (Chapter: 4) in *Biometric Recognition: Challenges and Opportunities*, 2015, pp. 90-93.

[165] It is important to emphasize that those national differences shall respect the European values and that the Charter of Fundamental rights of the European Union shall prevail in case of contradiction In other word, a national social acceptability shall be respectful of the European rule of law. Serena Rossi L., Droits fondamentaux, primauté et autonomie: la mise en balance entre les principes « constitutionnels » de l'Union européenne, RTDE, 2019, p. 67. Gaudin H., Les droits fondamentaux constituent-ils un frein ou un moteur de l'intégration européenne ? in Andriantsimbazovina J. (dir.) *Droits Fondamentaux Et Intégration Européenne: Bilan Et Perspective De L'union Européenne*, éd. Mare et Martin, 2020.

[166] Germany's plans for automatic facial recognition meet fierce criticism, *Euractiv.de*, 10 January 2020.

[167] Ada Lovelace Institute, *Beyond face value: public attitudes to facial recognition technology*, September 2019, p. 8.

[168] City of Nice, *Facial Recognition Experiment*, Report from the City of Nice, 2020.

[169] Ada Lovelace Institute, *Beyond face value: public attitudes to facial recognition technology*, *op. cit.*, p.8.

[170] City of Nice, *Facial Recognition Experiment*, *op. cit.*, p.17.

[171] *Ibidem*, p.19.

[172] FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* , op.cit.p.. 19.

"*permanently end indiscriminate and arbitrarily- targeted uses of biometric data in ways which can lead to mass surveillance or any undue interference with fundamental rights*."[173] The consultation that followed the European Commission White Paper on Artificial Intelligence also showed that a "*high number of companies*" were "*aware that AI may be breaching fundamental rights which could lead to discrimination*".[174]

Moreover, in spring of 2020, the Black Lives Matter movement triggered a global debate on the use of FRT by public authorities, leading some big companies to implement a moratorium. Even though moratoria were temporary, partial, and sometimes controversial, they were grounded in a concern that some uses of new surveillance technologies, and more specifically FRT, could infringe "basic human rights and freedoms."[175]

There are limits to public knowledge about FRT. In the British survey already mentioned, over 90% of respondents say they are aware of the use of FRT and 53% declare to be that are familiar with the technology. Yet when asked why they are comfortable with the police using FRT, 24% answered that they believed technology used by police did not discriminate (e.g. by race or gender), and 18% because it was accurate.

II.2.B Local authorities' demands and expectations

Just as there is no consensus from citizens about FR's acceptability, there is no consensus among cities as to its propriety. Interviews and surveys revealed various approaches to and expectations about surveillance new technologies.

Some cities, such as Nice (FR), Madrid (ES), or Helsinki (FI) are very favourable to their deployment: new technologies represent "an opportunity to strengthen security" and relevant tools to current threats. In this regard, Helsinki's police coordinator stressed that "criminals are constantly developing their own skills and have already introduced artificial intelligence. We need to keep up with developments to keep crime under control". These cities also insist on the need to experiment in order "to figure out what works best". Other cities are more reserved, in light of concerns raised by the public regarding data protection. Either way, the tools are considered as assistance to detection and human decision-making.

It is worth emphasizing that the appetite of cities for FRT is not contingent on their size. As part of the ISF project, small towns like Larissa (GR) or Brașov (RO) have

[173] Europa, *ECJ*, 2021.
[174] World Economic Forum, EU push for human-centered AI regulatory framework to build trust, *Biometric update*, 20 July 2020.
[175] In IBM's words. See IBM, Letter from IBM to the US Congress, IBM, 8 June 2020; See also: AMAZON, We are implementing a one-year moratorium on police use of Rekognition, 10 June 2020, and Microsoft bans police from using its facial-recognition, *Washington Post,* 11 June 2020.

also expressed interest and carried out experiments, as well as medium-sized towns such as Eindhoven (NL) or Mechelen in (BE).

In practice, the study revealed three main impediments that prevent cities from deploying FRT:

1. The lack of information and knowledge of the uses

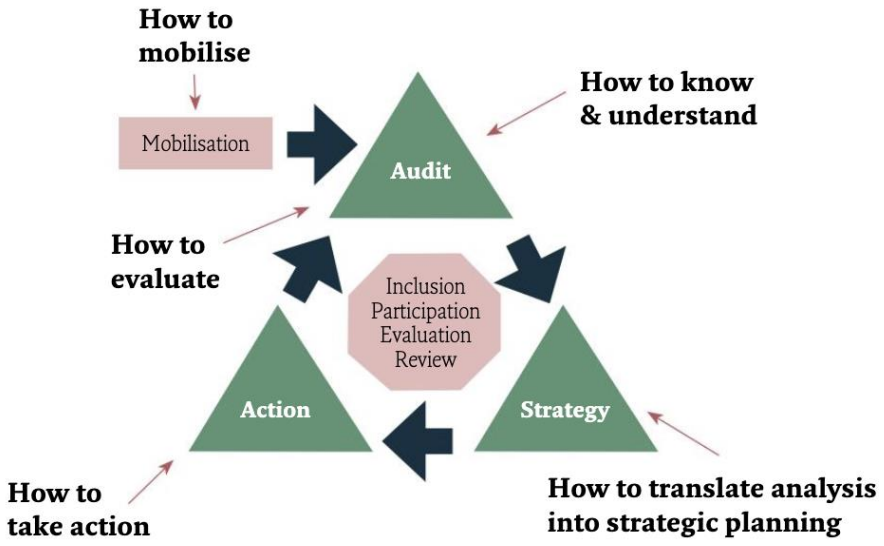
Some cities experience difficulty in determining both: their own needs and what the market offers.

Box 5: Methods and tools for a strategic approach to Urban Security

Methods and Tools for a Strategic Approach to Urban Security

To address this challenge, *Efus* has established an assessment tool for selecting projects based on their own specific needs and technologies sustainability for the city. This involves a local safety audits, that consists in "a systematic analysis undertaken to gain understanding of the crime and victimization-related problems in a city; to identify assets and resources for preventive activity; to enable priorities to be identified; and to help shape a strategy that will enables those priorities to be tackled".

Figure II.8: The strategic approach to Urban Security[176]



[176] Source: Efus, Publication, May 2016.

2. Regulatory impediments

The absence of clearly defined procedures and guarantees is one of the main impediments identified. In some countries – notably, France – there is also a difficulty in identifying a competent authority to promulgate regulations.

3. Costs

The financial cost involves the technology itself, technical debts, and the cost of data security. It also became essential, considering the social challenges at stake, that cities plan to invest in expensive democratization processes such as public insight and audits.

Some local authorities, even more rarely, also mention public procurement processes as inadequate.

III. Facial recognition in public space: the European legal environment

Despite the lack of specific legislation and other legal obstacles in practice, European data protection laws provide a basic framework for deploying facial recognition systems. This framework consists of two sets of rules whose application depends on the purposes of the data processing. The Law Enforcement Directive (LED)[177] "*lays down the rules relating to 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, including the safeguarding against and the prevention of threats to public security*." Any other personal data processing falls under the General Data Protection Regulation (GDRP).[178]

Facial recognition systems imply the processing of biometric data. The European legislation defines biometric data, the processing of which is limited or even prohibited, (III.1) and provides special requirements for biometric data controllers (III.2). Specific provisions also apply to the use of biometric data for external borders' control (III.3). Yet these provisions are ultimately inadequate and inappropriate for FRT in public spaces.

III.1 Facial recognition as biometric data processing

Regarding the risks previously identified, the legal definition of biometric data presents flaws (III.1.A). Regardless, there are still uncertainties concerning the legal basis for FRT deployment in public space (III.1.B).

III.1.A The flaws of biometric data definition

Definition

Biometric data is a legally recognized sub-category of personal data defined 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*".[179]

[177] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework.

[178] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[179] Article 4 GDRP.

Recital 51 of GDPR states, however, that the "*processing of photographs should not systematically be considered to be processing of special categories of personal data*".[180] Legislation and EDPD guidelines exclude from the definition raw data and data not processed for identification or authentication of a natural person.[181]

A particularly significant implication of the definition is that collected data fall out of the definition if they are not processed. As a result, facial images captured on CCTV are subject to specific protection and requirements, whereas facial images collected in large publicly available databases of facial images[182] generally are not. Researchers point out the risks entailed by such a distinction: under European legislation, public authorities and companies can build up biometric databases that might be used later without noticing the individuals concerned or to the public.[183] For instance, the Law Enforcement Directive states that "*Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data*" to protect public or national security.[184] GDPR also admits the restriction of these rights on the basis of Article 23 related to the limitation of its application.

This definition also contravenes the ECtHR requirements, which has consistently affirmed that the capture, collection, and storage of unique human characteristics in databases infringe the right to privacy.[185] In *Gaughran v. The United Kingdom*, the Court confirmed that retention of facial images could interfere with privacy rights.[186] Similarly, the French Constitutional Council (le *Conseil Constitutionnel*) observed in 2012 that "*the creation of a biometric identity file covering almost the entire French population and whose characteristics make it possible to identify a person to from his fingerprints constitutes an unconstitutional infringement of the right to respect for private life*."[187]

In response to this loophole, some national data protection authorities (DPAs) construed raw data as sensitive whenever used to fulfil identification purposes. A Belgian DPA, the Supervisory Body for Police Information (*Organe de contrôle de l'information policière*), reach a similar conclusion, prohibiting the linking of smart

[180] Rec. 51 GDPR. See also EDPB, Guidelines 3/2019 on Processing of Personal Data through Video Devices, on Video Surveillance, 29 January 2020, §74).

[181] They are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.

[182] Like facial images collected by governments to issue identity documents, or images collected by companies such as Clearview or Pimeye. See below box n°6.

[183] Kindt E. A First Attempt at Regulating Biometric Data in the European Union, *op.cit.*, p.66.

[184] Article 13.3 LED.

[185] [2008] ECtHR 1581, *S. and Marper v United Kingdom*, 4 December 2008, §86; 2013] ECtHR, *M.K. v France*, 18 April 2013, § 26.

[186] [2013] ECtHR, Gaughran v. *The United Kingdom*, 13 February 2020, §70.

[187] Cons. const., 2012-652 DC, 22 mars 2012, §6. The scope of this censorship was, however, weakened by a subsequent decision concerning the registration of unaccompanied foreign minors: the constitutional judge admitted that the collection of biometric data provided for by law resulted from a proportionate conciliation between the safeguard of public order and the right to respect for private life to the extent that this was necessary, and that the retention of data over time was limited, Cons. Const., 2019-797 QPC, du 26 juillet 2019, §11.

cameras to biometric databases.[188] These national provisions and interpretations, while promising, are insufficient to guarantee adequate and harmonized protection in Europe.

In summary, the definition of biometric data is a critical factor: it conditions the application of a more protective regime, which is likely desirable given the risks generated by FRT. The legal definition should be reviewed to offer adequate protection to unique human characteristics that fits the various purposes of FRT and restricts the storage of this data in databases. Recommendation n°1 proposes, in that regard, an alternate definition of the notion.[189]

III.1.B The uncertainties of the legal basis for facial recognition deployment

The processing of biometric data "*shall be prohibited*" under GDRP (Article 9), while "*allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject*" under the LED (Article 10).

Legislations provide several exceptions, four of which apply to FRT uses in public spaces. Public authorities are allowed to process biometric data 1°) when authorized by the law (national or European), 2°) to protect vital interests, 3°) when processing relates to personal data that are manifestly made public by the data subject and 4°) when the data subject has given explicit consent.

Some exemptions appear to be inapplicable (III.1.B.1) and explicit consent does not suit all use cases (III.1.B.2). Accordingly, the legislative exemption is ineffective in the absence of special legislation(s) (III.1.B.3).

III.1.B.1 Inapplicable exemptions

Of the four exceptions identified, the vital interest's protection and the exception relating to data made public do not constitute a legal basis for the deployment of FRT in public space.

LED and GDRP both mention "*vital interest protection of data subject or another natural person*"[190] as another exemption for biometric data processing. This legal basis could have been relevant in the context of a pandemic. Indeed, recital 46 of GDRP specifies that the exemption may concern processing necessary "*for monitoring epidemics and their spread*". Some cities experimented with facial recognition systems to ensure health safety. In Cannes (Fr), FRT turned out as a way to combat the spread of the virus, identifying people not wearing a mask.[191]

---

[188] The Supervisory Body for Police Information is bound by professional secrecy; its opinion was not officially published,but reported in the Belgian press. Ds Avond, Federale politie moet gezichtsherkenning stopzetten , *De Standaard*, September 2019.

[189] Based on the research work of Kindt E. A First Attempt at Regulating Biometric Data in the European Union, *op.cit.*

[190] Article 9.2c GDPR and 10b LED.

[191] A Cannes, des tests pour détecter automatiquement par caméras le port du masque, *Le Monde*, 28 April 2020.

The same experiment was carried out in a Parisian metro station.[192] Nevertheless, according to the European Data Protection Board (EDPB)[193] – and in line with article 46 of the GDPR – this condition only applies if the data subject is incapable (in law or practice) of giving consent to the processing, implying that the data subject lack capacity. As such, it is less likely that this legal basis would apply outside of an emergency.

This exemption does not, therefore, provide a general legal basis for deploying FRT in public spaces.

LED and GDRP also allow the processing of biometric data relating to data "*manifestly made public by the data subject*".[194] This provision's meaning is debated and suffers from a "*relative paucity of information*"[195] from European DPAs. In its guidelines, however, the EDPB excludes this provision as a legal basis to deploy live FRT in public spaces. EDPB argues that the "*mere fact of entering into the range of the camera does not imply that the data subject intends to make public special categories of data relating to him or her*".[196] The Board accordingly concludes that "*data controllers processing those data [biometric data] in the context of videos surveillance cannot rely on Article 9(2)(e)*".

This exemption remains a concern insofar as it allows database development that puts sensitive data at risk. As noted above, Clearview and Pimeyes built their database from web scraped data on social media. To avoid this pitfall, the Canadian regulator made an interesting move by strictly construing the meaning of "made public" by the data subject. According to Canadian data protection regulation, personal information can be collected and used without individuals' consent, on an exceptional basis, only if the information appears in a publication, available to the public, and provided by the individual. The OPC found that the conditions were not met in a Company's re-use of millions of Canadian Facebook user profiles case: "*the exception should be interpreted restrictively. In the case of Facebook profiles, it is not clear, in our view, that individuals would have intended to make their information public (...). [I]ndividuals may post information on Facebook for a variety of reasons (for example to be found and contacted by friends), and not necessarily to disseminate information to the public at large*".[197] That interpretation resulted in a finding of illegality for the data collection in the Clearview case:

---

[192] La RATP va tester des caméras « intelligentes » pour mesurer le taux de port du masque dans la station Châtelet', *Le Monde*, 7 May 2021. Those experiments were, however, suspended following the CNIL's position. See above n°41b.

[193] Article 9 (2) (c) "could – in theory and exceptionally – be used, but the data controller would have to justify it as an absolute necessity to safeguard the vital interests of a person and prove that this "[…] data subject is *physically or legally incapable of giving his consent*.". In addition, the data controller won't be allowed to use the system for any other reason". EDPD, Guidelines 3/2019 on processing of personal data through video devices (2020), Version 2.0, January 29, §69.

[194] Article 9.2e GDPR and 10c LED.

[195] Dove E.S., Chen J., What does it mean for a data subject to make their personal data "manifestly public"? An analysis of GDPR Article 9(2)(e), *University of Edinburgh School of Law Working Paper,* No 2020/18.

[196] EDPD, Guidelines 3/2019 on processing of personal data through video devices (2020), *op. cit.* §70.

[197] Complaints under the Personal Information Protection and Electronic Documents Act (the "Act" or "PIPEDA") against Profile Technology Ltd, PIPEDA Report of Findings #2018-002, June 12, 2018, §91-92.

"45. Information from sources such as social media or professional profiles, collected from public websites and then used for an unrelated purpose, does not fall under the "publicly available" exception of PIPEDA (...). Similarly, the respective regulations of both PIPA AB and PIPA BC(...) prescribe sources of public information that include directories, registries, and publications. Social media websites and search engines are not listed as prescribed sources of publicly available information under either of these Acts. As such, collection from these sources would only be authorized with consent and only if the purposes are what a reasonable person would consider appropriate.

47. As such, our Offices do not recognize the personal information collected, used or disclosed by Clearview to be "publicly available" as envisioned by the Acts, or as information "which by law is public," and thus the exception does not apply".[198]

The EU, and particularly the EDPB, should issue clear interpretative guidelines along the same lines.

III.1.B.2 The fragile legal basis of explicit consent

Explicit consent is another legal exemption that may allow the deployment of FRT in public spaces. Yet this exemption only applies under the GDPR, namely, to any matter to the exclusion of investigation, detection, or prosecution of criminal offences. Recital 35 of the LED states that in such a case "*the consent of the data subject, (...) should not provide a legal ground for processing personal data by competent authorities" since "the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes*".

On any other circumstance (management, traffic flows, experimentation), explicit consent may provide a legal basis (Article 9(2)(a) GDRP). Yet differences in function and environment can make explicit consent unworkable. Explicit consent appears inappropriate for FRT identification in an uncontrolled environment: consent may be difficult or impossible to collect for the controller and withdraw for the data subject.[199] Under those circumstances, the data subject's consent "*can only serve as a legal basis (...) in exceptional cases*" for the EDPS.[200] By contrast, for authentication purposes in a controlled environment, explicit consent is relevant and required.

This consent has to meet the conditions of Article 7 GDPR; it must be "*freely given, specific, informed and unambiguous indication of the data subject's agreement to*

[198] Joint investigation of Clearview AI, Inc. by the OPC, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta, *PIPEDA Report of Findings #2021-001*, 2 February 2021.

[199] In that sense, see: EDPD, Guidelines 3/2019 on processing of personal data through video devices (2020), *op. cit.* §46.

[200] *Ibidem*, §44.

the processing of personal data relating to him or her" (GDPR Recital 32). The data subject shall be "*able to withdraw consent without detriment*", at any time (Recital 43). These requirements have many implications for the data controller. First, consent must be shown by clear, affirmative action. For instance, entering a marked monitored area does not constitute a statement of consent for EDPB.[201] Second, the data controller must offer an alternative solution that does not involve biometric processing. Third, any clear imbalance between the data subject and the controller prevents characterizing consent as freely given. On this basis, the administrative tribunal of Marseille (Fr) ruled that the experiment carried out in two high schools to facilitate access to schools lacked a legal basis. Given the school's authority exercises on students, the consent could not be considered free and informed.[202] Fourth, consent implies also the use of the right of portability, created by Article 20 of the GDPR. This right enabling the data subject "*to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format"* is not enforceable when the process is "*necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."* (Article 20, §.3).

Thus, consent constitutes a fragile legal basis for the deployment of FRT.

III.1.B.3 The lack of national and European laws

GDPR provides that national and European laws may authorize the use of FRT for reasons of "*substantial public interest*".[203] The LED also lays down that the "*processing of biometric data shall be allowed where authorized by Union or Member State law*", where strictly necessary and subject to appropriate safeguards.[204]

It should be noted that these exceptions are broad. Legislation does not specify any indication of how public interest or public necessity may be assessed.[205] European legislation leaves the door open to national interpretation, covering a wide range of values relating to the public good. This poses a twofold problem. First, the protection granted is likely significantly to vary from country to country. Second, having defined the public interest broadly, some jurisdictions may pursue risky projects.

The lack of specific legislation can itself be considered an infringement of privacy rights guaranteed by Article 8 ECHR. In the UK Wales Police case, for example, the

[201] *Ibidem*, §46.
[202] TA Marseille, *La Quadrature du Net*, n° 1901249, 27 February 2020.
[203] Article 9g (GDRP).
[204] Article 10a (LED)
[205] GDPR only mentions safeguards that should be followed (Rec 45).

Court held that "*the legal framework currently in place (…) was insufficient*"[206] as "*too much discretion is currently left to individual police officers*".[207]

To date, in Europe, there is still no national legislation on FRT. Different bills, mostly sectoral, have been proposed but not adopted. Notably, several bills have been proposed in France: a draft law[208] and different amendments[209] on FRT for terrorist investigations and the prevention of attacks have been filed there since 2017. A law would also allow the use of FRT for 2024 Olympic Games security.[210] In the Czech Republic, the Home Secretary announced new legislation aimed at helping sports clubs ban rowdy fans from entering stadiums.[211]

During the past two years, some countries outside Europe have adopted – or at least debated – legislation and measures to limit FR's uses. They include China,[212] India,[213] and the United States. Some American cities and states have imposed bans and moratoria (see Box n°7) on FRT in some contexts. However, it should be noted that the legal environment is entirely different from Europe, where data rights are supposed to be more protected.

Box 6: US measures on facial recognition

US measures on Facial Recognition

In the United States, public calls for regulation lead to different enacted and proposed legislation/measures. The following table presents a non-exhaustive list of the most important examples in U.S. municipalities and states.[214]

Position	Municipalities/States
Complete Bans	Alameda (California), Berkeley (California), Oakland (California), San Francisco (California), Jackson (Mississippi), Boston (Massachusetts), Brookline (Massachusetts), Cambridge (Massachusetts), Northampton (Massachusetts), Somerville (Massachusetts), Springfield (Massachusetts) and Portland (Oregon) decided to implement a complete prohibition on using face recognition technologies by state actors. A Michigan bill (SB 342) proposes to ban law enforcement use and information obtained from face recognition technologies.

[206] [2020] EWCA Civ 1058 §90, §91.

[207] *Ibidem*, §91.

[208] Proposition de loi n°194 relative à la reconnaissance faciale dans les enquêtes terroristes et la prévention des attentats, 27 September 2017.

[209] Proposition de loi Sécurité globale, Amendement N° COM-83 rect. quinquies, 2 March 2021. This amendment aimed at allowing live facial recognition to prevent terrorist attacks. A second amendment, based on the same ground, was supposed to allow and normalize facial recognition in public transports.

[210] See: Parliamentary Office of Science & Technology, 'Facial Recognition', *Science and Technology Briefings* , No. 14, July 2019.

[211] 'Draft ministry bill allows facial recognition at sports stadiums', Radio Prague International, 16 February 2020.

[212] 'Law on collection of facial recognition data to be proposed at two sessions', *Global Times,* 2 March 2021.

[213] 'Fears for children's privacy as Delhi schools install facial recognition', *Reuter*, 2 March 2021.

[214] See, e.g.: Policing Project, *The Growing World of Face Recognition Legislation: A Guide to Enacted and Proposed Legislation*, NYU School of Law, September 2019, pp. 4-5; Miller K., *Facial Recognition: Current Uses, Concerns, and State Action*, 19 February 2020.

Partial Bans	A Pennsylvania bill (SB 797) proposes prohibiting educational entities or third parties from collecting biometrics on students, a New York bill (A 08373), the use of face recognition on school premises, and a Connecticut bill (HB 5333), retailers from using facial recognition software for marketing purposes.
Moratoria	Legislators in California (AB 1215), Massachusetts (S. 1385; H. 1538), Michigan (HB 4810), and Washington (SB 5528, HB 1654, HB 2856) proposed a temporary ban on state use of face recognition technologies.
Democratic Approval Prior Requirement	Berkeley (California), Davis (California), Seattle, and Yellow Springs (Ohio) adopted ordinances creating a democratic oversight for surveillance technologies[215]. This democratic movement has been initiated by civil law associations, like the American Civil Liberties Union (ACLU), to promote Community Control Over Policing Surveillance (CCOPS).[216]
Studies & Task Forces	New York (S 06623; A 08042) and New Jersey (AJR 206) legislators propose to create task forces to study the impact of face recognition. Another New Jersey bill (AB 5300) would require the Attorney General to obtain independent third-party testing and auditing. A Massachusetts bill (H. 2120) proposed to create a task force to develop a uniform code for body cams.
Limited authorization	In New Jersey, two bills have been submitted. The first one requires public hearings before law enforcement agencies use FRT (NJ AB 1210). The second one requires the state attorney general to test (NJ AB 989) and restrict the use of facial recognition systems (NJ SB 116).[217] A Maryland bill (MD SB 857) proposes to enhance the obligation for transparency by public bodies using FRT. They would have to publish an accountability report on their websites[218] and submit it to the Department of Information Technology. This bill proposes creating internal policies for data management, testing the FRT service in operational conditions before deployment, making available an application programming interface to enable independent tests, and making community consultation meetings. The bill also proposes prohibiting FRT services from engaging in ongoing surveillance or specific criminal procedures (with exceptions). Utah recently passed a bill (SB 0034) that allows public agencies to use FRT, provided that some guidelines are met. The bill notably requires law enforcement officers to submit a written request before performing an FRT search. They must also provide a valid reason for using so, like supporting a "fair probability" the person is connected with the crime. This request can only be granted for limited purposes (felony and violent crime investigation,

[215] Policing Project, *The Growing World of Face Recognition Legislation: A Guide to Enacted and Proposed Legislation*, *op. cit.*

[216] ACLU, Community control over police surveillance ccops model Bill.

[217] By government entities without safeguards such as standards for the use and management of information derived from the facial recognition system, audits to ensure accuracy, implementing protections for due process and privacy, and compliance measure

[218] Which include a description of the technology being used, name of the vendor, scope of use, and the type of data collected and generated, a description of the purpose and proposed use of the facial recognition service, etc.

	a threat to human life, identification of a dead body or an incapacitated person).

The lack of legislation on FRT leads to hesitation and divergence among national DPAs. Several requests have been addressed to the national DPAs regarding the deployment of recognition systems.[219]

Two kinds of opinion have been issued:

- Direct opinion: formulation of recommendations or decision relating expressly to the technology (Netherlands, Italy, France, United Kingdom, Sweden, Germany).
- Indirect opinion, most of the time about biometric data (Belgium, Spain, Czech Republic).

DPAs have not adopted a standard position; rather, four distinct positions can be identified. These are: unfavourable, reserved, mixed or favourable.

Table 2: Positions of DPAs on FRT

Unfavourable	Reserved	Mixed	Favourable
Refusal to implement	No ban, but a constant reminder of the risks and a request to limit uses while respecting the rights and freedoms of citizens.	Discrepancy between assertive public positions condemning the use of FRT, and decisions or opinions authorising widespread experimentation and use.	Approval without nuances

[219] In 2020 and so far in 2021, we note an increase in positions published by the national DPA regarding FR's use in Covid-19-related issues (such as the Spanish AEPD report on FR use during exams, which are not part of the study).

Germany[220]	France;[221] Sweden;[222] Spain;[223] Belgium.[224]	United Kingdom;[225] Netherlands.[226]	Italy[227]

Many DPAs called for legislators and decision-makers to identify acceptable uses and provide clear guidelines.

In addition to the DPAs, other organisations have been called upon to express their views in the context of public order enforcement. Their positions have proven divergent in some cases and concordant or complementary in others.[228] In Belgium, for example, the Police Information Control Authority issued a complementary unfavourable opinion on the Brussels National airport project, based on the intrusiveness of FRT.[229]

The analysis of exceptions shows the legal basis's weakness for the deployment of FRT in the public space. It also explains the uncertainties expressed by the relevant stakeholders.

This assessment leads to a twofold recommendation. It appears necessary to:
- Adopt a specific framework to guarantee legal certainty and the respect of fundamental and data protection rights (recommendation n°2); and
- Clarify exemptions to limit risky practices (recommendation n°3).

III.2 Specific requirements for biometric data processing

Under European law, biometric data processing through FRT requires implementing safeguards (I.1.A) and conducting a data protection impact assessment (DPIA) (I.1.B).

III.2.A Guaranties

The safeguards surrounding the deployment of FRT relate to the data processing (III.2.A.1), the data controller (III.2.A.2), the technical features of the recognition

[220] *Bundesdatenschutzbeauftragter mahnt Zurückhaltung bei Gesichtserkennung an*, BFDI, 24 January 2019.
[221] *Reconnaissance faciale: pour un débat à la hauteur des enjeux*, Rapport de la Commission Nationale de l'Informatique et des Libertés, November 2019.
[222] Datainspektionen, *Polisen får använda ansiktsigenkänning för att utreda brott* , 24 October 2019.
Datainspektionen, *Lagändring krävs för att polisen ska kunna utföra testverksamhet av ansiktsverifiering på flygplats* , 16 December 2019.
[223] AEDP, Orientaciones para centros educativos - Informe sobre la utilización por parte de profesores y alumnos de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas, 6 March 2018.
[224] ADP, *Un choix de société*.
[225] ICO, AI blog human biais and discrimination.
[226] College bescherming persoonsgegevens, Beleidsregels cameratoezicht, 2016.
[227] GDPD, Decision n°9040256, 26 July 2018.
[228] Lequesne-Roth C. (dir), *La Reconnaissance Faciale dans l'Espace Public – Une cartographie juridique européenne*, *op. cit.*, p.27.
[229] Aéroport de Bruxelles : reconnaissance faciale et Dashboard, *Air Journal,* 11 July 2019.

system (III.2.A.3), the human involvement (III.2.A.4) and the rights of the data subject (III.2.A.5).

III.2.A.1 Data processing guaranties

The processing of biometric data must rely on a legal basis (III.2.A.1.1), be limited in its purposes (III.2.A.1.2), and proportional (III.2.A.1.3), minimize data (III.2.A.1.4), guarantee accuracy (III.2.A.1.5) and limit storage (III.2.A.1.6).

III.2.A.1.1 Lawfulness and necessity of the processing

According to GDPR and LED, personal data shall be "*processed lawfully*" (Article 5.1.a GDPR; Article 4.1.a LED). Different legal grounds (Article 9 RGPD; Article 10 LED) can justify the processing of biometric data. The specific legal basis of FRT, however, appears questionable.[230] New legislation is likely needed to permit facial recognition – or, at the very least, clarify current exemptions allowing FRT processing.

Any legal basis - or legislative measure - should "*be clear and precise*".[231] Given the high risks of FRT processing[232], specific legal rules should strictly prohibit or limit some uses. For instance, the Council of Europe (CoE) recommended "*the use of facial recognition for the sole purpose of determining a person's skin colour, religious or other beliefs, sex, racial or ethnic origin, age, state of health or social condition*" not be allowed.[233] To be precise, the law should also provide different necessity and proportionality tests, depending on the processing parameters (purpose, environment, time, etc). In the light of ethical and societal issues raised above, European Union cannot sweep a relevant debate on FRT democratic uses.[234]

If adopted at a national level, new legislation will require the DPA's prior consultation (Article 36.4 GDPR; Article 28.2 LED).

---

[230] See above III.1.B.

[231] Recital n°41 GDPR, recital n°33 LED. The lack of specific legislation was the basis for the UK Court of Appeal's position in E. Bridges v. the South Wales Police case, and the CNIL's position concerning facial recognition in Metz stadium.

[232] See above I.2.

[233] CoE, *Guidelines on Facial Recognition*, 28 January 2021 p.5.

[234] This view notably is put forward by the French DPA: "*This debate is crucial. Indeed, beyond its technicality, political choices have to be made in order to shape what our society will look like tomorrow (...)Such choices cannot be made behind closed doors, without democratic control, in fits and starts or by taking ad-hoc initiatives tailored to local contexts, with no overall perspective. Otherwise, there is a considerable risk that these choices will be lost, that gradual shifts will result in unexpected and unwanted societal change and that we will one day be faced with a fait accompli. Political choice should not be dictated simply by technical possibilities. And neither should the political debate be limited to the question of how to make certain digital transformations "acceptable" to our fellow citizens. No. The role of "politics" is to determine which of the possible uses of these technologies are really desirable, leaving the issue of acceptability until the end of the analysis – as a final step rather than as a postulate*". CNIL, Facial Recognition, For A Debate Living Up To The Challenges, 15 November 2019, p.2.

III.2.A.1.2 Purpose limitation

GDPR and LED both provide that personal data shall be "*collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes*" (Article 5.1.b GDPR; Article 5.1.b LED). Processing purpose limitations help to reduce the impact of collection on the data subjects' rights.

For CoE, "*legislators and decision-makers shall ensure that images available in a digital format cannot be processed to extract biometric templates or to integrate them into biometric systems without a specific legal basis for the new processing, when those images were initially captured for other purposes (from social media for instance)".*[235]

III.2.A.1.3 Proportionality

According to GDPR, biometric data processing can be allowed by Union or Member State law but "*shall be proportionate to the aim pursued*" (Article 9.2.g). The LED does not explicitly make the processing of biometric data subject to proportionality of use but implies as much in Recital 26: "[*a]ny processing of personal data* (...) *can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences* (...), *as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society*". The CJEU has established a three-steps proportionality test. The Court will assess (1) effectiveness (2) necessity (and subsidiarity) and (3) proportionality of the processing.

The intrusive nature of FRT requires particular vigilance. According to the case law and the positions adopted by the DPAs, the use of FRT is disproportionate when a less abusive alternative can be substituted. FRT in schools was, on that grounds, judged to disproportionate by the Swedish DPA[236] and a French administrative court.[237] In contrast, the French DPA found FRT at airport boarding proportionate to regulate traffic and help ensure safety.[238]

III.2.A.1.4 Data minimisation

Personal data shall be "*limited to what is necessary*" (Article 5.1.d GDPR) and "*not excessive*" (Article 4.1.d LED) in relation to the purposes for which they are processed. The principle of data minimization implies that the system only processes the required information, not all the information available.

---

[235] CoE, *Guidelines on Facial Recognition*, *op. cit.*, p.6

[236] Datainspektionen, *Lagändring krävs för att polisen ska kunna utföra testverksamhet av ansiktsverifiering på flygplats*, 16 December 2019.

[237] *TA Marseille*, 27 February 2020, n°1901249. See above n°84.

[238] CNIL, *Reconnaissance faciale dans les aéroports: quels enjeux et quels grands principes à respecter ?*, 9 October 2020.

The Italian DPA found that FRT to measure passenger flows at airports was compatible with the data minimisation principle as long as "*the images are kept for the time strictly necessary to encode them in a biometric template, and without any cross-checking with other identification data (e.g. name and surname) of the persons concerned*".[239] To enhance its implementation in video surveillance, the Spanish DPA recommends the use of "privacy masking" ("*máscaras de privacidad*"[240]) that limits data collected.

III.2.A.1.5 Data accuracy

Personal data shall be "*accurate*" (Article 5.1.d. GDPR) & (Article 4.1.d. LED). LED also stipulates that "*Member States shall provide for the competent authorities to take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available*" (Article 7.2). To that end, each competent authority shall "*as far as practicable, verify the quality of personal data before they are transmitted or made available*" (Article 7.2). In all transmissions of personal data, necessary information shall enable "*the receiving competent authority to assess the degree of accuracy*" (Article 7.2). If it emerges that incorrect or unlawful personal data has been transmitted, the recipient "*shall be notified without delay. In such a case, the personal data shall be rectified or erased or processing shall be restricted in accordance with Article 16*" (Article 7.3).

To ensure data accuracy, the CoE makes two interesting recommendations. The first concerns watchlists in support of the identification functions. The Council recommends checking "*the quality of images and biometric templates inserted in watchlists (...) to prevent potential false matches since low-quality images can cause an increase in the number of errors*."[241] The second applies more specifically to authentication purposes as implemented in airports. The CoE deems "*necessary to renew the training photos and therefore ask more recent photos to be provided. This will also enable to protect from the consequences of changes in the shape of faces (due to ageing, to accessories – piercing or other – or to other modifications)*."[242]

III.2.A.1.6 Data storage limitation

Personal data shall be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*" (Article 5.1.e. GDPR; Article 4.1.e. LED). Under GDPR, personal data may be stored only for "archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" (Article 5.1.e.). LED requires

[239] GDPD, *Verifica preliminare. Sistema di rilevazione delle immagini dotato di un software che permette il riconoscimento della persona (morfologia del volto)*, n°8789277, 15 March 2018.
[240] AEPD, *Guía sobre el uso de videocámaraspara seguridady otras finalidades*, 29 June 2018, pp. 8-9.
[241] CoE, *op. cit.*, p.12
[242] *Ibidem,* p.9.

that Member States "*provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data*" (Article 5). "*Technical*", "organizational" (GDPR) and "*procedural*" (LED) measures shall "*ensure compliance*" to the rule (Article 5 LED) and "*safeguard the rights and freedoms of the data subject*" (Article 5.1.e. GDPR).

For the Brøndby Stadium experiment, the Danish DPA required the Stadium not to store biometric data that did not match the information on Brøndby IF's internal watchlist.[243] Similarly, the immediate deletion of images relating to data subjects who were not on the wanted list, was a decisive element to approve FRT South Wales police experiments.

To clarify the implementation of the principle for FRT, the CoE proposes applying the following principles:

- "if there is no match of the biometric templates, the biometric template of individuals passing through an uncontrolled environment cannot be retained and have to be automatically deleted;
- if there is a match, the biometric templates can be retained for a strictly limited time provided by law with necessary safeguards and match reports including personal data can also be retained for a limited time;
- and in any case, the watchlist and biometric templates have to be deleted upon completion of the purpose for which live facial recognition technologies were deployed."[244]

III.2.A.2 Data controller guaranties

The data controller of FRT must ensure transparent (III.2.A.2.1) and accountable biometric data processing (III.2.A.2.2).

III.2.A.2.1 Transparency

Transparency is a critical principle since the exercise of rights and the collection of free and informed consent (when required) depend on its effectiveness. To be effective, the controller has a general information obligation (III.2.A.2.1.1) and must observe special requirements in case of a data breach (III.2.A.2.1.2).

III.2.A.2.2 The information obligation

GDPR and LED both establishes an obligation for the controller to inform the data subject about the processing, safeguards measures and right of the data subject (Article 12.1 GDPR; Article 12.1 LED). Even if Article 13.3 of the LED allows the adoption of legislative measures delaying, restricting, or omitting the information

[243] Datatilsynet, Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion, 24 May 2019.
[244] CoE, *Guidelines on Facial Recognition*, *op. cit.*, p.12

to the data subject high risks in the use of FRT require similarly a high transparency level.

Principles of fair and transparent processing require the data subject to be informed of the processing, its purposes, and its consequences. The controller must also inform the data subject about her/his rights.

On formal grounds, the principle of transparency requires any communication relating to processing to the data subject to be in a "*concise, intelligible, and easily accessible form, using clear and plain language*". The information shall be provided by any appropriate means, and necessary "*in writing*" under GDPR.
In practice, notices form depend on the rollout context (controlled or uncontrolled environment).

The South Wales police adopted, for instance, a three-tiered approach to meet this requirement:[245]

1. "prior to each AFR deployment, utilising Facebook and Twitter to advertise the deployment and its location and invite engagement with officers who are deploying the technology";
2. "displaying large A2-size "Fair Processing Notices" on the AFR equipped police vehicles on site and at approximately a 100 metre radius of the AFR cameras; and"
3. "handing out postcard-sized notices to members of the public in the vicinity of each AFR deployment and to every person that is spoken to as a result of an AFR intervention".

It should be noted that while the High Court found these measures sufficient,[246] the Court of Appeals did not: "*[w]hilst deployment of AFR is not covert, it is nevertheless reasonable to suppose that a large number of people whose facial biometrics are captured and processed by SWP's use of AFR are unaware of this taking place.*"[247]

In Nice, authorities in charge of the experiment distributed notice and indicated the experiment was conducted on trucks or FRT gantries; information was also available on their website.

To comply this obligation regarding facial recognition, the CoE identified four types of information to be communicated:[248]

- Potential FRT data transfer to third parties (whether, to which extent and where);
- Retention, deletion or de-identification of FRT data;

[245] Described in [2020] EWCA Civ 1058 §20.
[246] [2019] EWHC §39.
[247] [2020] EWCA Civ 1058 §20.
[248] *Ibidem*, p.11.

- Contact points available for individuals to ask questions about the collection, use and sharing of FRT data;
- An update policy when the collection, use, and sharing practices change significantly.

III.2.A.2.3 Special requirements for data breach

In case of a personal data breach, the controller shall notify the supervisory authority (III.2.A.2.3.1) and communicate the personal data breach to the data subject (III.2.A.2.3.2).

III.2.A.2.4 Notification to the DPA

In the case of a personal data breach, the controller (Article 33.1 GDPR) or the Member State (Article 30.1. LED) shall "*without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent",* unless the personal data breach *"is unlikely to result in a risk to the rights and freedoms of natural persons".* The same rules apply to the processor who shall notify the controller (Article 33.1 GDPR; Article 30.1.LED). Legislation specifies the forms of notification: the nature of the personal data breach, the name and contact details of the data protection officer, likely consequences, measures taken or proposed to address the personal data breach. That documentation "*shall enable the supervisory authority to verify compliance with this Article*" (Article 33.5 GDPR; Article 30.5.LED).

The Belgian DPA recalled the importance of this security rule on the occasion of the Suprema's "BioStar 2"[249] database breach, given the risks at stake. In this case, the authority was informed of the breach by a data controller company that used Suprema services.[250] Most of the time, however, the DPA is notified by the press (and not the controller). In the same case, the British DPA (ICO) initiated an investigation into the security breach, which affected some British law enforcement agencies, due to the media revelations.[251]

III.2.A.2.5 Communication to the data subject

The controller shall also communicate the personal data breach to the data subject, without undue delay, when "*the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons*" (Article 34 GDPR; Article 31 LED). The communication to the data subject shall not be required if (a) the controller has implemented appropriate technical and organisational protection measures, (b) the controller has taken subsequent measures which ensure that

[249] On this case, see box n°1.
[250] *Fuite de 2000 empreintes digitales: l'Autorité de protection des données suit l'affaire Adecco de près*, ADP, 21 August 2019.
[251] Scammell R., '*Suprema downplays biometric data leak of 'one million fingerprints''*, *Verdict*, 20 August 2019. On the Suprema case, se below box n°1.

the high risk to the rights and freedoms of data subjects is no longer likely to materialise; (c) it would involve disproportionate effort.

Notification is also a critical element of transparency. In a recent case concerning a sensitive data breach that occurred in connection with the video-conference examinations, the Polish DPA imposed a fine of PLN 25,000 on the Medical University of Silesia for failing to notify the supervisory authority, but also the persons affected by the incident. The controller had incorrectly assessed the risk involved and, therefore, decided it was not necessary to notify of the breach. In the controller's opinion, "*the risk to the rights or freedoms of the persons affected by the incident was low*". It is interesting to note that the authority did not consider the number of people accessing the database to be decisive: the sensitivity of the data and the lack of certainty that they will no longer be made available to unauthorised persons were sufficient to characterise the incident as high risk. The Polish DPA took into account, among others: "*the duration of the breach (from the breach to the issuing of the decision several months passed)*", "*the intentional action of the controller, who decided not to notify a breach and not to inform the students about it*", "*the unsatisfactory cooperation of the controller with the authority (the controller did not notify a breach despite the letters sent and the proceedings initiated)*".[252]

III.2.A.2.6 Accountability

The controller shall be responsible for, and be able to demonstrate compliance with, principles relating to processing of personal data (Article 5.2 GDPR; Article 4.4 LED). To this end, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with European Law (Article 24 GDPE; Article 19 LED). The accountability principle requires that authorities using FRT to demonstrate necessity, proportionality, and legality of the use. Even covert use of FRT by law enforcement authorities, allowed under Article 13.3 LED, must be documented before and during such a use (5.2 and 24 RGPD; Articles 4.4 and 19 LED).

Among other organisational measures, the CoE recommends that entities deploying FRT:

- Implement transparent policies, procedures and practices to ensure that the protection of the rights of data subjects underlie their use of FRT;
- Publish transparency reports about the concrete use of FRT;
- Set up and delivery training programs and audit procedures for those in charge of processing FRT data;
- Set up internal review committees to assess and approve any processing involving FRT data;

[252] EDPB, Polish DPA: University Fined for the lack of Data Breach Notifications, 26 January 2021. For the full decision (only in Polish): Urzędu Ochrony Danych Osobowych, DKN.5131.6.2020, Warszawa, dnia 05 stycznia 2021 r.

- Contractually extend applicable requirements to third-party service providers, business partners or other entities using FRT (and denial of the access to third parties that would not comply with them);
- In the public sector: prior evaluation constraints in public procurement procedures involving suppliers of FRT tools, assessment of minimum levels of performance in terms of accuracy, especially where law enforcement purposes are concerned.[253]

III.2.A.3 Technical guaranties

Technical guarantees involve security measures of processing (III.2.A.3.1) that shall be implemented by design and default (III.2.A.3.2).

III.2.A.3.1 Security of the processing

Given the sensitivity of biometric data and the high risk to the rights and freedoms of natural persons, biometric data should be processed in such a manner that ensures a high level of security and confidentiality of the data (Article 5.1.f. GDPR; Article 4.1.f LED).

These security measures shall be taken to prevent unauthorised access to or use personal data and the equipment used for processing. These measures are all the more essential as the facial recognition systems are easy to fool.[254] They are organisational and technical, and concern all processing stages, from the collection to transmission and storage.

The GDPR lists examples of appropriate measures, while indicating that security shall be contextually assessed[255] (Article 32). These measures include: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The LED requires that security measures be subject to eleven types of controls: the equipment access control, the data media control, the storage control, the user control, the data access control, the communication control, the input control, the transport control, recovery, reliability and integrity control (Article 29).

[253] CoE, *Guidelines on Facial Recognition*, *op. cit.*, pp. 13-14.

[254] As seen above, n°15.

[255] The measures taken shall take into account "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons", Article 32.

As an example, the Danish DPA has allowed the processing of biometric data in Brøndby stadium for the purpose of uniquely identifying a natural person, using automatic FRT, under specific security conditions:[256]

- The personal data processed by the facial recognition system had to be transported and stored encrypted on the server with up-to-date and widely recognised encryption algorithms;
- The surveillance cameras had to be installed on a separate virtual local area network and not exposed to the Internet;
- Brøndby Stadium had to maintain access control to the facial recognition system.

It involved:

- Employees' authorisation to use the facial recognition software;
- Manual record entries into the system;
- Use of a two-factor approval in the login process.

The technical audit of the systems,[257] although not expressly mandatory, appears thus crucial to ensure security compliance. The CoE recommends enhancing "*a comprehensive risk assessment*" of facial recognition systems, including "*potential for errors, susceptibility to unfair bias, vulnerability to hacking and cyberattacks*".[258] An audit chain's introduction, including a security assessment upstream and downstream of FRT implementations, is recommendation n°7.

III.2.A.3.2 Privacy by design and default

Data-protection principles and, more specifically, appropriate technical and organisational measures shall be implemented:

- *By design*, i.e. "in an effective manner and to integrate the necessary safeguards into the processing," to meet the requirements of European legislation (Article 25.1. GDPR, Article 20.1 LED);
- *By default*, for ensuring that "only personal data which are necessary for each specific purpose of the processing are processed"; (Article 25.2. GDPR, Article 20.2 LED).

As by design and default safeguards, the French DPA recommends for instance in in airports keeping data under the exclusive control of the data subject in two alternative forms:[259]

- Passenger exclusive control over his/her biometric data stored on an individual medium (a secure mobile application on his/her mobile phone, on a badge, card, etc.);

[256] Datatilsynet, *Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion*, 24 May 2019.

[257] On methods for facial recognition technical assessment, see Castelluccia C., Le Métayer D., *Impact Analysis of Facial Recognition: Towards a Rigorous Methodology*, *op cit.*

[258] CoE, *Guidelines on Facial Recognition*, *op. cit* p. 15

[259] CNIL, *Reconnaissance faciale dans les aéroports: quels enjeux et quels grands principes à respecter ?*, 9 October 2020.

- Encrypted biometric database, making it unusable without the passenger involvement (thanks to the possession of an element or a secret allowing its decryption, for instance).

The CoE also set up a list of by design and default technical safeguards to ensure data protection and security. It comprises the automatic deletion of raw data after extracting biometric templates, flexibility to adjust the technical safeguards according to the principles of purpose limitation, data minimisation and limitation of the duration of storage of data, or the implementation of an internal review process designed to identify and mitigate the potential impact.[260] International standards also provide guidance to protect biometric data under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer.[261]

The principles of data protection by design and by default must be considered in public tenders: facial recognition system suppliers will have to guarantee their compliance with data protection laws. To ensure the technical effectiveness of the protection, the CoE recommends the setting up of an "*independent and qualified certification mechanism for facial recognition and data protection*".[262] Such a certification could be implemented "*according to the application of artificial intelligence used by the facial recognition technology: one type of certification to categorise structures (design of algorithm, integration of algorithm, etc) and another to categorise algorithms (computer recognition, intelligent search, etc.)*."[263]

III.2.A.4 Human guaranties

According to the GDPR and the LED, automated processing of sensitive data is prohibited, unless authorised by Union or Member State law which must lay down suitable measures to safeguard the data subject's rights (Article 22 GDPR; Article 11 LED). In the absence of special legislation, this implies that any facial recognition processing must involve human control. An alert generated by an automated facial recognition system cannot lead to an automated arrest: the decision resulting from a match shall only rely on humans.

This interpretation is in line with the CoE guidelines according to which "*entities using FRT should ensure that human operators continue to play a decisive role in the actions taken upon the results of these technologies. Entities using these technologies should take organisational measures to oversee the human operators taking decisions which can have a significant impact on individuals*."[264] The Council

[260] CoE, *Guidelines on Facial Recognition*, *op. cit.*, p.10.
[261] See, for instance, ISO/IEC 24745:2011 that provides "*requirements and guidelines for the secure and privacy-compliant management and processing of biometric information*".
[262] CoE, *Guidelines on Facial Recognition*, *op. cit.*, p.8.
[263] *Ibidem*.
[264] CoE, *Guidelines on Facial Recognition*, *op. cit.*, p. 14.

also considers that "*where the use of facial recognition technologies is intended to enable a decision to be taken solely based on automated processing which would significantly affect the data subject, the latter must, in particular, be entitled not to have such processing carried out without his or her views being taken into account*".[265] This last principle is welcome but raises practical issues which are similar to those raised concerning explicit consent. Therefore, in the absence of specific laws and effective alternatives, automated FRT shall be considered unlawful.

The London Metropolitan Police Service considered this obligation for the rollout of live FRT as officers are "*expected to conduct further checks to confirm their [the matched individual's] identity*" and to make judgments "*on the 'balance of probability' as to the credibility of the match, looking at the two images and deciding whether to accept or discard the match*".[266]

III.2.A.5 Data subject rights guaranties

According to GDPR and LED, the data subject shall have the right of access, to confirm personal data are being processed (Article 15 GDPR; Article 14 LED), the right to rectification and erasure of personal data (or "right to be forgotten"), the restriction of processing and the right to object. In case of false match for instance, data subjects can request rectification to avoid further/repetitive false matches.[267] The controller shall ensure the exercise of these rights. For instance, French law provides that rights of access and rectification for FRT processing at airports (Parafe) are exercised "*with the head of the border police or customs department of the airports, seaports and railway stations concerned either in writing or directly at the registration point.*"[268]

These rights may be limited by law subject to the principles of necessity and proportionality. The exception is particularly broad in the LED, as Member States "*may adopt legislative measures restricting, wholly or partly, the data subject's right of access (…) to protect (c)public or (d) national security*" (Article 15 LED). In such a case, however, the data controller of the facial recognition system shall "*document the factual or legal reasons on which the decision is based*" and inform data subjects of "*the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy*" (Article 15.3 and 15.4 LED).

III.2.B Impact Assessment on biometric data protection

The data personal impact assessment (DPIA) is a tool construed as a processual proof of data process's compliance to the GDPR/LED.

---

[265] CoE, *Guidelines on Facial Recognition*, *op. cit.*, p. 16.

[266] Fussey P. & MurrayD., *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, July 2019, p. 107.

[267] The CoE mentions this hypothesis. CoE, *Guidelines on Facial Recognition*, *op. cit.*, p.12

[268] Article R232-10 du *Code de la sécurité intérieure*.

This processual proof aims to meet two main objectives:

- Define and assess the risks to personal data processed by the controller before deployment of a processing operation. Risk identification in turn helps in mitigating the inherent risks.
- Have a risk assessment management tool. The appropriate measures to be adopted shall be prioritized to prevent any "high risk" to the rights and freedoms.

Given the factual and legal elements already mentioned (sensitivity of the data processed, risks, public concerns), the impact assessment appears to be a critical procedural component to the implementation of safeguards. However, the compulsory nature of DPIA for FRT is debated (III.2.B.1), and its content remains uncertain (III.2.B.2).

III.2.B.1 Uncertainties concerning the obligation of DPIA for facial recognition

Article 35 of the GDPR and Article 27 LED, the data controller(s) shall carry out a DPIA prior the deployment of the data process "[w]*here a 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 natural persons*."

The "*high risk*" nature of the processing is left to the sole interpretation of the controllers.

Article 35 §3(b) of the GDPR provides that "*data protection impact assessment (...) shall in particular be required in the case of (...) processing on a large scale of special categories of data referred to in Article 9(1)*". Subject to the points set out above regarding the definition of biometric data,[269] carrying out a DPIA is mandatory for facial recognition processing under the GDPR.

In addition, according to EDPB,[270] the DPIA is mandatory under the GDPR for certain types of data processing. The EDPB bases its analysis on nine criteria[271]: (1) evaluation or rating, (2) automatic decision-making, (3) systematic surveillance, (4) processing of sensitive data or data of a highly personal nature, (5) large-scale data, (6) cross-referencing or combining data sets, (7) data concerning vulnerable persons, (8) innovative use or application of new organizational solutions, and (9) processing that prevents [data subjects] from benefiting from a service or

[269] See above n°75.

[270] The Article 29's Data protection impact assessment Guidelines on Data Protection Impact Assessment to determine whether the processing is "*likely to result in a high risk*" for the purposes of Regulation 2016/679 (hereinafter referred to as "WP248") were endorsed by the EDPB on the 25th May 2018.

[271] The EDPB assesses these "regulatory situations" according to five distinct criteria, to which are added four new alternative criteria. These criteria are cumulative with those proposed by DPAs based on paragraphs 4 to 6 of Article 35 of the GDPR.

contract. Any two criteria can trigger the performance of a DPIA. Most of the aforementioned criteria occur with facial recognition systems.

Article 27 of LED is less exhaustive. Only recital 51 states that "[*t]he risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from situation (...) where genetic data or biometric data are processed in order to uniquely identify a person*". The same reservations regarding the definition of biometric data may apply. Despite the less assertive provisions, the meaning of the law seems to be the same.

Even though no legislation explicitly requires a DPIA before deploying a facial recognition system, this obligation clearly follows from the law and EDPB guidelines.

Regrettably, this interpretation is not uniformly applied in practice. The mandatory nature of DPIAs for FRT is clear to the Belgian,[272] French,[273] Spanish,[274] and British[275] DPAs. Two DPAs have adopted sanctions in the absence of its implementation: the Swedish DPA against a public school[276] and the Belgian Police Information Control Board against a FRT project at Brussels National Airport.[277] In the Ed Bridges case, the Court of Appeal even ruled that the DPIA carried out by the South Wales Police was not sufficient and "*failed properly to assess the risks to the rights and freedoms of data subjects*" and "*address the measures envisaged to address the risks*".[278] In Greece, however, the implementation of DPIA raises questions. The Hellenic Police has not confirmed that a prior DPIA was conducted, nor the Hellenic DPA consulted.[279]

Two factors contribute to a lack of clarity. On the one hand, the publication of the DPIA is not mandatory despite the WP248 recommendations,[280] as the EPDS' report reveals. As mentioned above, stakeholders are often reluctant to share trade secrets and there is no common position on the subject. Some European courts have sanctioned the data controller for lack of publication, whereas other DPAs and courts ignore the issue or opine on the deficiency of the DPIA without requiring public authorities to disclose it. Given the resulting lack of clarity, DPIAs for FRT, as well as their publication or at least their summary, should be expressly made mandatory (recommendation n°6). On the other hand, the sole controller

[272] Secrétariat Général de L'ADP, *Adoption de la liste des catégories de traitement devant faire l'objet d'une analyse d'impact relative à la protection des données conformément à l'article 35.4 du Règlement Général sur la Protection des données (CO-A-2018-001), n°01/2019*, 16 January 2019.

[273] CNIL, *Analyse d'impact relative à la protection des données: publication d'une liste des traitements pour lesquels une analyse est requise*.

[274] AEPD, *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*.

[275] ICO, Examples of processing likely to result in high risk.

[276] Datainspektionen, *Lagändring krävs för att polisen ska kunna utföra testverksamhet av ansiktsverifiering på flygplats*, 16 December 2019.

[277] B. Schmitz, Le RWDM comme laboratoire pour une technologie de reconnaissance faciale , *RTBF*, 5 September 2018.

[278] [2020] EWCA Civ 1058 §153.

[279] See above n°62.

[280] Guidelines invite the data processor to publish it to inform the public.

decides whether or not to carry out a DPIA, and if so, what means to use.[281] As the EPDS points out, this is a loophole: in their assessment, controllers do not hesitate to deliberately and knowingly put aside certain risks to avoid its completion.[282] DPAs should be involved in assessing the appropriateness of a DPIA (co-regulation model, recommendation n°5).

III.2.B.2 The content of the DPIA on facial recognition deployment

The GPDR and the EDPB both opted for methodology neutrality. The lack of a standard methodology[283] for DPIA raises further difficulties in the impact assessment of FRT.

First, there is a question regarding the scope of "rights and freedoms". Even if Recital 85 of the GDPR provides a long list of examples, certain experts claim that those examples transform the DPIA into a "*Privacy Impact Assessment*" (PIA).[284] Beyond the differences in terminology, DPIA and PIA are tools with different aims.[285] The methodology neutrality of the EPDB also emphasizes the difference of "values" between the DPAs. While some focus on cybersecurity concerns, others prioritize the assessment of "rights and freedoms"[286] or compliance with the procedure. This can also lead to disparities in methods and requirements between DPAs, and consequently, to unequal protection levels.

[281] It should be noted, however, that whichever the purpose and its legal basis, a DPIA may be requested to the data controller. See WP248 p. 9.

[282] EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (case 2020-0066), 6 July 2020.

[283] Which the literature, especially the legal doctrine, struggles to remedy as shown by the relative paucity of information on DPIA. See C. Levallois-Barth (dir), J. Keller, « Analyse d'impact pour la protection des données dans les voitures connectées », *Rapport de recherche Chaire Connected Cars and Cyber Security*, 2021, to be published.

[284] R. Clarke, The Distinction between a PIA and a Data Protection Impact Assessment (DPIA) under the EU GDPR, for a Panel at CPDP, Brussels, 27 January 2017.

[285] *Ibidem*.

[286] On this subject, see C. Levallois-Barth (dir), J. Keller, L'*Analyse d'impact pour la protection des données (AIPD) dans les voitures connectées;* la Chaire C3S (*Connected Cars and Cyber Security*) de Télécom Paris, to be published May 2021.

Box 7: Key areas of FRT DPIA from DPA's perspective

Key areas of FRT DPIA from DPA's perspective

Regarding the cases studied, the DPAs and courts have focused on four key areas when looking at FRT cases:

- Transparency: clear notices must be made available to the data subjects concerning facial recognition processing to collect and process their personal data. In the South Wales police case, a three-tiered approach (notice on social media, notices displayed on police vehicles, and cards handed out to public members) was deemed insufficient by the Court of Appeals.[287]

- Proportionality: given the technology's invasive nature, its use must be proportionate to the objective pursued. Thus, a French administrative tribunal[288] and the Swedish DPA[289] considered FRT in schools to be disproportionate. According to the French DPA, the objectives of securing and easing school access can be achieved by less intrusive means for privacy and individual freedoms, such as badge control.[290]

- Data minimisation: personal data that are not necessary should not be stored and must be deleted at the earliest opportunity. In South Wales police cases and the Danish DPA's decision concerning Brøndby stadium,[291] the immediate deletion of images relating to data subjects, who were not on the 'wanted list, was a decisive element to approve FRT experiments.

- Security: biometric data processing requires strengthening security through measures like encryption, two-factor authentication, or no Internet access to the data. In the Clearview case, the Swedish DPA concluded that "*the Police has not fulfilled its obligations as a data controller on a number of accounts with regards to the use of Clearview AI*" as they have "*failed to implement sufficient organisational measures*",[292] including security measures

The absence of metrics (key performance indicators) of the risks, combined with the data controller's sole arbitration, invites the latter to minimize or discard some high risks for the "rights and freedom". This flaw is reinforced by the absence of a clear duty on behalf of the data controller to submit its DPIA to the DPA.

Moreover, applying the distinction between DPIA and PIA mentioned, the assessment subject varies substantially. Whereas the DPIA will question the

[287] [2020] EWCA Civ 1058 §20.

[288] TA Marseille, 27 February 2020, n°1901249.

[289] Datainspektionen, *Lagändring krävs för att polisen ska kunna utföra testverksamhet av ansiktsverifiering på flygplats*, 16 December 2019.

[290] CNIL, *Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position*, October 2019.

[291] Datatilsynet, *Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion*, 24 May 2019.

[292] Integritetsskyddsmyndigheten, *Beslut efter tillsyn enligt brottsdatalagen – Polismyndighetens användning av Clearview AI, DI-2020-2719*, 10 February 2021.

process and the effectiveness of the data rights subject whose biometric data is captured (aka the procedure aspects), the PIA will review the global purpose of facial data collection from both the point of view of the data subject and the collective. Even if the EPDB supports this vision, fostered by the DPA, the tools to appreciate such points are either completely missing or consciously discarded.

This last issue raises another. FRT must have a legal basis, supposedly resulting from a European or State Member law). Therefore, onboarding data subjects' collectives to assess such a process's opportunity is deemed useless, and second scrutiny may question the Rule of Law. DPIA, in such context, will not be used to examine the *legal* but the *technical* compliance to the GDPR. The data controller will use the DPIA as a way to ensure the legality of the process by taking into consideration the privacy by design and default obligation as explained by the EDPB's guidelines.[293]
To be effective, all stakeholders' views[294] must be heard. However, private compliance does not invite democratic participation, as the law contemplates in spirit if not in letter.[295]

These findings call for a twofold recommendation:

- A standard methodology,[296] with a specific set of expectations, should be established for FRT use through audit chain's introduction (recommendation n°7);
- The black box system is not compatible with a democratic transparency regime, and stakeholder's participation in the process should be clarified (recommendation n°8).

[293] Guidelines 04/2019 on Article 25 DPDD, April 2019.
[294] EDPS, Report: EU Institutions' use of Data Protection Impact Assessments, 6 July 2020.
[295] It is worth noting that some European researchers are trying to provide solutions to those issues with software development kits or models DPIA. See H2020 Privacy and data protection 4 engineering (PDP4E).
[296] For a proposition, see: Castelluccia C., Le Métayer D., *Impact Analysis of Facial Recognition: Towards a Rigorous Methodology*, *op. cit.*

III.3 Specific provisions on security and border control

Various European texts provide for specific provisions on the use of FRT for identification purposes, especially in matters of security and border control.

The Entry-Exit System (EES) Regulation of 30 November 2017[297] enabled the widespread use of FRT for identification within the European Union. This regulation paves the way for the development of recognition systems thanks to standardized use of facial images for identity verification, visa and asylum applications, and, more broadly, border crossings of short-stay Third Country Nationals (TCN).

The regulation will be applied in combination with the European Passenger Name Record (PNR) Directive. The processing of biometric data is supposed to enhance the effectiveness of controls. The EES will be effective in February 2022 but is already available,[298] The EES will be effective in February 2022, but is already available[299] allowing each Member State to complete functional and compliance testing allowing each Member State to complete functional and compliance testing.

The Regulation of 28 December 2018 on the use of the Schengen Information System[300] for border checks lays down specific requirements for facial image collection and use and the enforcement of data subjects' rights. Recital 22 states that "[*t]his Regulation should set out the conditions for use of (…) photographs and facial images for identification and verification purposes. Facial images and photographs should, for identification purposes, initially be used only in the context of regular border crossing points. Such use should be subject to a report by the Commission confirming the availability, reliability and readiness of the technology*".

FRT in border control is also considered under the revision of the Prüm Treaty.[301] This Treaty, established in 2008,[302] aims at enhancing cross-border cooperation, particularly in the fight against terrorism and cross-border crime. It has already facilitated the automated exchange of specific personal data (DNA, dactyloscopic and registration data) between the Members States. Following the draft council

[297] Regulation (EU) 2017/2225 of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System, 30 November 2017; Regulation (EU) 2017/2226 establishing an Entry/Exit System (EES) to register the data of non-EU nationals crossing the EU's external borders.

[298] Migration and Home Affairs, Entry/Exit System, European Commission.; Frontex, Entry-Exit System pilot project at land borders, 5 August 2020; Idemia, Five key recommendations to support Member States in implementing the European Entry/Exit System, 11 May 2020.

[299] Migration and Home Affairs, Entry/Exit System, European Commission. See above.

[300] Regulation (EU) 2018/1861 of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, 28 November 2018.

[301] Burt C., EU police face biometrics system debated by lawmakers, experts concerned about false positives, *Biometric Updates*, 23 September 2020.

[302] By Council Decision 2008/615/JHA JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, 23 June 2008.

conclusions,[303] the European Commission is due to produce a feasibility report[304] that could broaden the scope of shared biometric data.

Finally, it should be noted that the regulatory movement has resulted in the funding of European projects encouraging the use of new technology at borders. For instance, the EU Horizon 2020 program funded the program "*Secure societies – Protecting freedom and security of Europe and its citizens*", that aims at "*enhancing the quality and efficiency of identity verification at border crossings in all modalities: land, air and sea by providing faster and more secure border control solutions*".[305]

[303] General Secretariat of the Council, Draft Council Conclusions on the implementation of the "PRÜM DECISIONS" ten years after their adoption, 5 July 2018.

[304] Burt C., EU police face biometrics system debated by lawmakers, experts concerned about false positives, *op.cit.,* [300].

[305] D4FLY, *Detecting Document Fraud and Identity on the Fly*, 2020.

IV. Recommendations

This study has shown the increasing deployment of FRTs in public spaces. It reflects cities and law enforcement agencies' appetite for these technologies in the current security context, that the Covid-19 crisis has not stopped. The study also highlighted risks raised by their deployment. Various technical vulnerabilities, threats to fundamental rights, and the mass surveillance spectrum are proper concerns.

The study has also shown that the European legal framework lays the ground to set-up a trustworthy ecosystem for FRT rollouts. However, European laws, which are not specific to FRT or even to surveillance technologies, suffer from weaknesses. They are not sufficient and require consideration of the specific uses and risks of the technology.

Taking into account these findings, the recommendations below can be put forward. They consist of amending the biometric data legal definition (IV.1), adopting a specific framework and clarifying biometric prohibition exemption (IV.2), enhancing the DPIA and its effectiveness (IV.3).

IV.1 Amend the biometric data legal definition

The study has shown that raw data and data not processed for identification or authentication of a natural person are excluded from the legal definition of biometric data. Thus, collected data such as facial images collected in large publicly available databases of facial image fall out of the definition if they are not processed. Such a distinction entails risks, like building up biometric databases that might be used later without noticing the individuals concerned or to the public.

In response to this loophole, the study recommends amending the biometric data legal definition. The definition should offer adequate protection to unique human characteristics that fits the various purposes of FRT and restricts the storage of this data in databases. An alternate definition could be: "*all personal data (a) relating directly or indirectly to unique or distinctive biological or behavioural characteristics of human beings and (b) used or fit for use by automated means (c) for purposes of identification, identity verification, or verification of a claim of living natural persons*"[306] (recommendation n°1).

[306] Based on the research work of Kindt E. A First Attempt at Regulating Biometric Data in the European Union, *op.cit.*

IV.2 Adopt a specific framework and clarify biometric prohibition exemption

The analysis of exceptions shows the legal basis's weakness for the deployment of FRT in the public space. The analysis of exceptions shows the legal basis's weakness for FR's deployment in the public space. Of the exceptions allowing biometric data processing, only the legal authorisation appears inappropriate for FRT rollout in public space. National and European laws may authorize the use of FRT for reasons of "substantial public interest" (Article 9g GDPR) where "strictly necessary" (Article 10a LED).

The study has shown that this exception raises twofold concern. First, no specific law has been enacted to date. The lack of specific legislation can itself be considered an infringement of privacy rights and leads to hesitation and divergence among national DPAs. Second, this exception is broad as it leaves the door open to national interpretation, covering a wide range of values relating to the public good. The study warns that having defined the public interest broadly:

- Protection granted is likely significantly to vary from country to country;
- Some jurisdictions may pursue risky projects.

The study also cautioned that even though the exemption concerning biometric data "*manifestly made public*" does not provide a general legal basis for deploying FRT in public spaces, it remains a concern insofar as it allows database development that puts sensitive data at risk.

The study thus recommends:

- For the legislator to adopt a specific framework to guarantee legal certainty and the respect of fundamental and data protection rights (recommendation n°2).
- For the legislator to clarify biometric prohibition and sweeping exceptions. In this respect, compliance with fundamental rights requires some uses to be prohibited (recommendation n°3).
- For the CoE, "the use of facial recognition for the sole purpose of determining a person's skin colour, religious or other beliefs, sex, racial or ethnic origin, age, health condition or social condition should be prohibited unless appropriate safeguards are provided for by law to avoid any risk of discrimination."[307] The study also, and more specifically, recommends prohibiting the deployment of all RF systems implementing mass surveillance, such as the real-time FRT, and the deeply flawed emotional recognition.
- For the European supervisory authority, to issue restrictive interpretative guidelines concerning "made public data." As found by the Canadian DPA, it should be clear that information from sources such as social media or professional profiles, collected from public websites and then used for an

[307] CoE, *Guidelines on Facial Recognition*, *op. cit.*, p. 5

unrelated purpose, does not fall under the publicly available exception (recommendation n°4).

IV.3 Enhance the DPIA and its effectiveness

The study has shown that even though no legislation explicitly requires a DPIA before deploying a facial recognition system, this obligation clearly follows the law and EDPB guidelines. Regrettably, this interpretation is not uniformly applied in practice. Two factors contribute to a lack of clarity. First, the publication of the DPIA is not mandatory, and stakeholders are often reluctant to share trade secrets. Second, the sole controller decides whether or not to carry out a DPIA, leading them to deliberately and knowingly put aside certain risks to avoid its completion.

The study also warned that the lack of a standard methodology for DPIA raises further difficulties in FR's impact assessment. This can lead to disparities in methods and requirements between DPAs, and consequently, to unequal protection levels. The absence of metrics (key performance indicators) of the risks, combined with the data controller's sole arbitration, invites the latter to minimize or discard some high risks for the "rights and freedom." This flaw is reinforced by the absence of a clear duty on behalf of the data controller to submit its DPIA to the DPA. Finally, private compliance does not invite democratic participation, as the law contemplates in spirit if not in letter.

These findings call for the following recommendations:

- DPAs should be involved in assessing the appropriateness of a DPIA (co-regulation model, recommendation n°5).
- DPIAs for FRT, as well as their publication – at least their summary, should be expressly made mandatory (recommendation n°6).
- A standard methodology, with a specific set of expectations, should be established for FRT use through audit chain's introduction (recommendation n°7).
- The black box system is not compatible with a democratic transparency regime, and stakeholder's participation in the process should be clarified (recommendation n°8).

V. References

V.1 National and European DPA decisions & publications

- ADP, *Un choix de société*.
- AEDP, *Orientaciones para centros educativos - Informe sobre la utilización por parte de profesores y alumnos de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas*, 6 March 2018.
- AEPD, *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*.
- AEPD, *Guía sobre el uso de videocámaraspara seguridady otras finalidades*, 29 June 2018, pp. 8-9.
- Autoriteit Persoonsgegevens, *Brief branche normkader digitale billboards*, 25 June 2018.
- *Bundesdatenschutzbeauftragter mahnt Zurückhaltung bei Gesichtserkennung an*, BFDI, 24 January 2019.
- CNIL, *Analyse d'impact relative à la protection des données: publication d'une liste des traitements pour lesquels une analyse est requise*.
- CNIL, *Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position*, October 2019.
- CNIL, *La CNIL appelle à la vigilance sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques*, 17 June 2020.
- CNIL, *Reconnaissance Faciale: pour un débat à la hauteur des enjeux*, 15 November 2019, p.4.
- CNIL, *Reconnaissance faciale dans les aéroports: quels enjeux et quels grands principes à respecter ?*, 9 October 2020.
- CNIL, *Reconnaissance faciale et interdiction commerciale de stade: la CNIL adresse un avertissement à un club sportif*, 18 February 2021.
- BfDI, *Activity Report 2019,* 28th Activity Report on Data Protection, p. 47-48.
- BfDI, *Extracts from the 2017/2018 Activity Report of the Federal Commissioner for Data Protection and Freedom of Information*, 27th Activity Report, p.42-43.
- Datainspektionen, *Polisen får använda ansiktsigenkänning för att utreda brott*, 24 October 2019
- Datainspektionen, *Lagändring krävs för att polisen ska kunna utföra testverksamhet av ansiktsverifiering på flygplats*, 16 December 2019.
- Datatilsynet, *Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion*, 24 May 2019.
- *Fuite de 2000 empreintes digitales: l'Autorité de protection des données suit l'affaire Adecco de près*, ADP, 21 August 2019.

- Garente per la Pootezione dei Dati Peronali, *Verifica preliminare. Sistema di rilevazione delle immagini dotato di un software che permette il riconoscimento della persona (morfologia del volto)*, n°8789277, 15 March 2018.
- EPDB Guidelines on connected cars, January 2020, p.12.
- EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (case 2020-0066), 6 July 2020.
- ICO, *AI blog human biais and discrimination*.
- *Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places*, 31 October 2019, p. 5.
- Integritetsskyddsmyndigheten, *Beslut efter tillsyn enligt brottsdatalagen – Polismyndighetens användning av Clearview AI, DI-2020-2719*, 10 February 2021.
- *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*, 2 February 2021.
- Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta, *PIPEDA Report of Findings #2021-001*, 2 February 2021.
- Police unlawfully used facial recognition app, *IMY*, 11 February 2021.
- Secrétariat Général de L'ADP, *Adoption de la liste des catégories de traitement devant faire l'objet d'une analyse d'impact relative à la protection des données conformément à l'article 35.4 du Règlement Général sur la Protection des données (CO-A-2018-001), n°01/2019*, 16 January 2019.
- The Office of the Australian Information Commissioner and the UK's Information Commissioner's Office open joint investigation into Clearview AI Inc, ICO, 9 July 2020.
- Urzędu Ochrony Danych Osobowych, DKN.5131.6.2020, Warszawa, dnia 05 stycznia 2021.

V.2 Court decisions

- CJEU, case C-623/17, *Privacy International*, 6 October 2020.
- CJEU, case C-345/17, *Buivids*, 14 February 2019.
- CJEU, *Joined cases C-203/15 and C-698/15*, *Tele2 Sverige* 21 December 2016.
- CJEU, case C-212/13, *Frantiscaronek Rynescaron; c/ Úrad pro ochranu osobních údaju*, 11 December. 2014;
- ECHR, *Gaughran v. The United Kingdom*, 13 February 2020.
- [2008] ECtHR 1581, *S. and Marper v United Kingdom*, 4 December 2008.
- [2013] ECtHR, *M.K. v France*, 18 April 2013.

- [2019] EWHC 2341 *Cardiff, R (Bridges) v. Chief Constable of the South Wales Police*.
- [2020] EWCA Civ 1058, *Bridges R. v Chief Constable of South Wales Police*.
- Superior Court Of New Jersey Law Division, Nijer Parks Lawsuit, 25 November 2020.
- CE, Ass., Ville de Castelnaudary, 17 June 1937.
- TA Marseille, *La Quadrature du Net,* n° 1901249, 27 February 2020.

V.3 Institutional report and White Paper

- COM(2020)65, *White Paper on Artificial Intelligence - A European approach to excellence and trust*, 2020, p. 21.
- CoE, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data*, recommendation 7, 2005.
- FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27 November 2019.
- French Sénat, Rapport d'information n° 621 (2019-2020), 9 July 2020.
- Nice, *Facial Recognition Experiment*, 2019.
- Nist, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, Washington DC: US Department of Commerce, 2019.
- Nist, *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, Washington DC: US Department of Commerce, 2018, p.7.
- OHCHR, *Rights to freedom of peaceful assembly and of association - Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, 17 May 2019, A/HRC/41/41.
- OHCHR, *Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 28 May 2019, A/HRC/41/35.
- UN Human Rights Commissioner, *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, Report of the United Nations High Commissioner for Human Rights*, 24 June 2020, A/HRC/44/24.
- French Sénat, Rapport d'information n° 621 (2019-2020), 9 July 2020.

V.4 NGO reports

- Ada Lovelace Institute, *Beyond face value: public attitudes to facial recognition technology,* September 2019.
- Aclu, Community control over police surveillance ccops model Bill.
- Amnesty International, *Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance*, 11 June 2020.

- Amnesty International, *Out of control: Failing EU Laws for Digital Surveillance Export*, 2020.
- Chiusi F., In Italy, an appetite for face recognition in football stadiums, *Algorithm Watch*, 2020.
- International Network of Civil Liberties Organizations (INCLO), Facial Recognition Tech Stories and Rights Harms from around the World, January 2021, pp. 5-8; pp 13-17.

V.5 Doctrinal work

- Angwin J., Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance, Times Books, 2014.
- Alparslan Y. et al., Adversarial Attacks on Convolutional Neural Networks in Facial Recognition Domain, 2021.
- Bose A. J., Aarabi P., Adversarial Attacks on Face Detectors using Neural Net based Constrained Optimization, 2018.
- Castelluccia C., Le Métayer D., Impact Analysis of Facial Recognition: Towards a Rigorous Methodology, Inria, 2020, hal-02480647f.
- Castets-Renard C., Besse P., Loubes J.-M. et Perrussel L., Encadrement des risques techniques et juridiques des activités de police prédictive, Rapport 2019 CHEMI, ministère de l'Intérieur, 12 July 2019, p.13.
- Castets-Renard C., Guiraud E. et Avril-Gagnon J., *Cadre juridique applicable à l'utilisation de la reconnaissance faciale par les forces de police dans l'espace public au Québec et au Canada Éléments de comparaison avec les États-Unis et l'Europe*, Rapport de recherche Obvia, September 2020.
- Charpenet J., Lequesne Roth C., Discrimination et biais genrés, Les lacunes juridiques de l'audit algorithmique, Dalloz, 2019, p. 1852.
- Clarke R., *The Distinction between a PIA and a Data Protection Impact Assessment (DPIA) under the EU GDPR, for a Panel at CPDP*, Brussels, 27 January 2017.
- Dove E.S., Chen J., *What does it mean for a data subject to make their personal data "manifestly public"? An analysis of GDPR Article 9(2)(e)*, University of Edinburgh School of Law Working Paper No 2020/18.
- Evtimov I. et al., What if a facial recognition system is too easy to fool? Is Tricking a Robot Hacking? Berkeley Technology Law Journal 34, 2019.
- Feldman Barrett L. et al., Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, Psychological Science in the Public Interest 20, 2020, no.1: 1–68.
- Fussey P. & Murray D., Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, July 2019, p. 107.
- Gaudin H., Les droits fondamentaux constituent-ils un frein ou un moteur de l'intégration européenne ? in Andriantsimbazovina J. (dir.) Droits

Fondamentaux Et Intégration Européenne: Bilan Et Perspective De L'union Européenne, éd. Mare et Martin, 2020.
- Gonzàlez Fuster G., *Artificial Intelligence and Law Enforcement, Impact on Fundamental Rights*, for the European Parliament, July 2020.
- Khan J. K. and Upadhyay D., Security issues in face recognition, 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence), Noida, India, 2014, pp. 719-725.
- Lequesne-Roth C., La Reconnaissance Faciale dans l'Espace Public – Une cartographie juridique européenne, Rapport Fablex, 2020.
- Levallois-Barth C. (dir), Keller J., L'Analyse d'impact pour la protection des données (AIPD) dans les voitures connectées; la Chaire C3S (Connected Cars and Cyber Security) de Télécom Paris, to be published May 2021.
- Mundial I.Q. et al, Towards Facial Recognition Problem in COVID-19 Pandemic,", 4rd International Conference on Electrical, Telecommunication and Computer Engineering (ELTICOM), Medan, Indonesia, 2020, pp. 210-214.
- Policing Project, *The Growing World of Face Recognition Legislation: A Guide to Enacted and Proposed Legislation*, NYU School of Law, September 2019, pp. 4-5.
- Rossi S. L., "Droits fondamentaux, primauté et autonomie: la mise en balance entre les principes "constitutionnels" de l'Union européenne", RTDE, 2019.
- Sudeep S.V.N.V.S., et al, An Overview of Biometrics and Face Spoofing Detection, In: Kumar A., Mozar S. (eds) ICCCE 2020. Lecture Notes in Electrical Engineering, vol 698. Springer, Singapore, 2021.
- Tamir I., *Facial Recognition at a Crossroads: Transformation at our Borders and Beyond*, 30 September 2020.
- University of Essex, London Metropolitan Police & Trial of Facial Recognition, Report, p.116.

V.6 Miscellaneous

- 27 pays ont testé l'application de reconnaissance faciale de Clearview, *Nextinpact*, 28 February 2020.
- A Cannes, des tests pour détecter automatiquement par caméras le port du masque, *Le Monde*, 28 April 2020.
- Asenjo A., Un instituto catalán está usando reconocimiento facial para controlar la asistencia a clase, algo por lo que ha sido multado con 19.000 euros un colegio sueco », *Business Insider*, 19 September 2019.
- Aéroport de Bruxelles : reconnaissance faciale et Dashboard, *Air Journal,* 11 July 2019.
- Amazon, *We are implementing a one-year moratorium on police use of Rekognition*, 10 June 2020.

- Anyvision Interactive Technology, Adaptive Positioning of Drones for Enhanced Face Recognition, *United States Patent & Trademark Office,* 4 February 2021.
- Arroyo V., Leufer D., Facial recognition on trial: emotion and gender "detection" under scrutiny in a court case in Brazil, *Access now*, 29 June 2020.
- Schmitz B., Le RWDM comme laboratoire pour une technologie de reconnaissance faciale , *RTBF*, 5 September 2018.
- Bates Ramirez V., Facial Recognition Drones Will Use AI to Take the Perfect Picture of You, *Singularity Hub*, 23 February 2021.
- Big brother in Berlin: Face recognition technology gets tested, *Deutsche Welle*, 31 July 2017.
- Buolamwini J., Response: Racial and Gender bias in Amazon Rekognition — Commercial AI System for Analyzing Faces', *Medium*, 25 January 2019.
- Burt C., EU police face biometrics system debated by lawmakers, experts concerned about false positives, *Biometric Updates*, 23 September 2020.
- Capriel J., Drones that recognize you? Amazon has a patent for that, *Biz journals*, 21 August 2019.
- Chenarchive A., Computers can't tell if you're happy when you smile, *MIT Technology Review*, 26 July 2019.
- Clearview AI Data Processing Violates GDPR, German Regulator Says, *Bloomberg*, 29 January 2021.
- Clearview AI to stop selling controversial facial recognition app to private companies, *The Verge*, 7 May 2020.
- D4FLY, *Detecting Document Fraud and Identity on the Fly*, 2020.
- Dechaux D., La vérité sur les failles de la biométrie faciale', *Challenges*, 23 January 2021.
- Draft ministry bill allows facial recognition at sports stadiums, *Radio Prague International,* 16 February 2020.
- Ds Avond, Federale politie moet gezichtsherkenning stopzetten , *De Standaard*, September 2019.
- Faces Fourth Lawsuit Alleging Biometric Privacy Violations, *Expert Institute*, 25 June 2020.
- Face-scanning at pubs could offer key to vaccine passports, *The Times*, 27 March 2021.
- Fears for children's privacy as Delhi schools install facial recognition', *Reuter*, 2 March 2021.
- German police seek volunteers for facial recognition surveillance, *Deutsche Welle*, 19 June 2017.
- Germany and facial recognition tech: a love affair, *Fairplanet*, 11 January 2019.
- Germany's plans for automatic facial recognition meet fierce criticism, Euractiv.de, 10 January 2020.
- Hamilton F., Police facial recognition robot identifies anger and distress, *The Times*, 15 August 2020.

- Harris M., An Eye-Scanning Lie Detector Is Forging a Dystopian Future, *Wired,* 12 April 2019.
- Hartmann M., Fundamental rights implications of recent trends in digital forensics, Bonn's staatsanwaltschaft, *CPDP 2021*.
- Harwell D., A face-scanning algorithm increasingly decides whether you deserve the job, *The Washington Post*, 6 November 2019.
- *Homo Digitalis' request for opinion to the Hellenic DPA* (only in Greek), 19 March 2020.
- In fight against coronavirus, governments embrace surveillance, *Politico*, 24 March 2020.
- Jumbo Privacy brings a formal GDPR complaint against Clearview, *Jumbo Privacy*, 14 July 2020.
- Kindt E. A First Attempt at Regulating Biometric Data in the European Union, AI Now, Regulating Biometrics: Global Approaches and Urgent Questions, 2020, p.66.
- Komkov S., Petiushko A., *AdvHat: Real-world adversarial attack on ArcFace Face ID system*, 2019.
- La RATP va tester des caméras « intelligentes » pour mesurer le taux de port du masque dans la station Châtelet, *Le Monde*, 7 May 2020.
- Law on collection of facial recognition data to be proposed at two sessions', *Global Times,* 2 March 2021.
- *Letter from IBM to the US Congress,* IBM, 8 June 2020.
- Libert M., Reconnaissance faciale: Les caméras de vidéosurveillance offertes à Valenciennes par Huawei posent question, *20 minutes*, 29 January 2020.
- Maass D., Guariglia M., Video Analytics User Manuals Are a Guide to Dystopia, *EFF*, 19 November 2020.
- Microsoft bans police from using its facial-recognition, *Washington Post,* 11 June 2020.
- Miller K., *Facial Recognition: Current Uses, Concerns, and State Action*, 19 February 2020.
- Monroy M., German authorities improve face recognition, *Digit,* 31 January 2020.
- N. B. López-Molina, Spain's largest bus terminal deployed live face recognition four years ago, but few noticed, *Algorithm Watch*, 11 August 2020.
- Panasonic, *Case study*, 2018.
- Peng K., Facial recognition datasets are being widely used despite being taken down due to ethical concerns. Here's how, *Freedom to tinker*, 21 October 2020.
- *Press Release of Hellenic Police* (only in Greek), 14 December 2019.
- Privacy International, How facial recognition is spreading in Italy: the case of Como, 17 September 2020.
- Protección de Datos investiga el sistema de reconocimiento facial de Mercadona, *El Diario,* 6 July 2020.

- Rodriguez K., Activists Worldwide Face Off Against Face Recognition: 2019 Year in Review, *EFF*, 30 December 2019.
- Scammell R., Suprema downplays biometric data leak of 'one million fingerprints, *Verdict*, 20 August 2019.
- Seehofer verzichtet auf Software zur Gesichtserkennung, *Der Spiegel,* 24 January 2020.
- Shankland S., Tokyo 2020 Olympics using Facial Recognition system from NEC, Intel, *CNET*, 1 October 2019.
- *Statement on the High Court judgment on the use of Automatic FRT by South Wales police*, 11 September 2019.
- STUPP C., German Prosecutors Are Building AI In-House, *Wall Street Journal*, 26 February 2021.
- Tariq S., Jeon S., WOO S. S., *Am I a Real or Fake Celebrity? Measuring Commercial Face Recognition Web APIs under Deepfake Impersonation Attack*, 2 March 2021.
- The Facial Recognition Company That Scraped Facebook And Instagram Photos Is Developing Surveillance Cameras, *Buzzfeednews*, 2 March 2020.
- *The technical specifications of the smart policing contract* (only in Greek), 12 April 2018.
- Un logiciel pour décoder les émotions des usagers du tramway de Nice, *France Bleu*, 4 January 2019.
- Untersinger M., Reconnaissance faciale: la CNIL tique sur le bilan de l'expérience niçoise, *Le Monde*, August 2019.
- Report: Data Breach in Biometric Security Platform Affecting Millions of Users reported in 'Major breach found in biometrics system used by banks, UK police and defence firms', *The Guardian*, 14 August 2019.
- Whittaker Z., Security lapse exposed Clearview AI source code, *TechCrunch*, 16 April 2020.
- World Economic Forum, EU push for human-centered AI regulatory framework to build trust, *Biometric update*, 20 July 2020.

VI. Annex

VI.1 List of interviewees

- Representative of the Métropole Nice Côte d'Azur, 3 February 2021.
- Representative 1 of the European Forum for Urban Security (EFUS), 24 February 2021.
- Representative 2 of the European Forum for Urban Security (EFUS), 24 February 2021.
- Representative of DG CONNECT, European Commission, 25 February 2021.
- Representative of DG HOME, European Commission, 26 February 2021.
- Representative of the European Union Agency for Fundamental Rights (FRA), 26 February 2021.

The report was also discussed and commented on during its presentation to the AI Expert group VTC, hosted by the European Commission on 11 March 2021.

VI.2 List of position statements by country

Belgium

- Commission de la protection de la vie privée, avis d'initiative n°17/2008, relatif aux traitements de données biométriques dans le cadre de l'authentification des personnes,9 April 2008.
- APD, Un choix de société.
- Secrétariat général de l'APD, Adoption de la liste des catégories de traitement devant faire l'objet d'une analyse d'impact relative à la protection des données conformément à l'article 35.4 du Règlement général sur la Protection des données (CO-A-2018-001), n°01/2019, 16 January 2019.

Czech Republic

- Úřad pro ochranu osobních údajů, ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech, 16 August 2019.
- Úřad pro ochranu osobních údajů, Kontrola používání technologie FaceID (společnost Metrostav a.s.), 2019.

Denmark

- Datatilsynet, Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion, 24 May 2019.

France

- CNIL, Délibération n° 2016-012 portant avis sur un projet de décret portant modification d'un traitement automatisé de données à caractère personnel dénommé PARAFE, 28 January 2016.

- CNIL, Plenary Session, Expérimentation de la reconnaissance faciale dans deux lycées, la Cnil précise sa position, 17 October 2019.
- CNIL, Rapport Reconnaissance faciale: pour un débat à la hauteur des enjeux.
- CNIL, La reconnaissance faciale dans les aéroports, quels enjeux et quels grands principes à respecter, November 2019.
- CNIL, Reconnaissance faciale et interdiction de stade, la CNIL adresse un avertissement à un club, 18 February 2021.

Germany

- BfDI, Bundesdatenschutzbeauftragter mahnt Zurückhaltung bei Gesichtserkennung an, 24 January 2019.
- Daten Ethik Kommission, Opinion of the Data Ethics Commission, 19 October 2019.

Italy

- GDPD, Personali, Sistema automatico di ricerca dell'identità di un volto, n°904025, 26 July 2018.
- GDPD, Decision n°9040256, 6 August 2018.

Netherlands

- College bescherming persoonsgegevens, Beleidsregels cameratoezicht.
- Authoriteit persoons gegevens, Algemene verordening gegevensbescherming, 2016.

Portugal

- CNPD, decision 292/2020.

Spain

- AEPD, Orientaciones para centros educativos - Informe sobre la utilización por parte de profesores y alumnos de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas, 6 March 2018.

Sweden

- Datainspektionen: Inom skolområdet är det tydligt att elva står i beroendeställning till skolan vad klassificering, studiemedel, utbildning och därmed möjlighet till framtida arbete eller fortatta studier, 18 August 2019.
- Datainspektionen: Tillsyn enligt EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever, 20 August 2019.
- Datainspektionen, Datainspektionen anser att Polismyndigheten har ett berättigat intresse av att behandla personuppgifter på det sätt man föreslagit., 23 October 2019.
- Datainspektionen, Polisen får använda ansiktsigenkänning för att utreda brott, 24 October 2019.

- Datainspektionen, regarding the Skavsta airport experiment « Under fas två kommer uppgifterna hanteras avgränskontrollanter vid Skavsta flygplats som ett beslutsstöd för kontroll motden resehandling som uppvisas », 16 December 2019.
- Datainspektionen, Lagändring krävs för att polisen ska kunna utföra testverksamhet av ansiktsverifiering på flygplats, 16 December 2019.

United Kingdom

- ICO, Human bias and discrimination in AI systems, 25 June 2019.
- Biometrics Commissioner, Biometrics Commissioner response to court judgment on South Wales Police's use of automated facial recognition technology, 10 September 2019.
- ICO, ICO statement in response to an announcement made by the Metropolitan Police Service on the use of live facial recognition, 24 January 2020.