Facial Recognition for Preventive Purposes: the Human Rights Implications of Detecting Emotions in Public Spaces

# Facial Recognition for Preventive Purposes: The Human Rights Implications of Detecting Emotions in Public Spaces

**Isadora Neroni Rezende**

**Abstract** Police departments are increasingly relying on surveillance technologies to tackle public security issues in smart cities. Automated facial recognition is deployed in public spaces for real-time identification of suspects and warranted individuals. In some cases, law enforcement is going even further by exploiting also emotion recognition technologies. In preventive operations indeed, emotion facial recognition (EFR) is being used to infer individuals' inner affective states from traits like facial muscle movements. In this way, law enforcement aims to obtain insightful hints on unknown persons acting suspiciously in public or strategic venues (e.g. train stations, airports). While the employment of such tools still seems to be relegated to dystopian scenarios, it is already a reality in some parts of the world. Hence, there emerges a need to explore their compatibility with the European human rights framework. The Chapter undertakes this task and examines whether and how EFR can be considered compliant with the rights to privacy and data protection, the freedom of thought and the presumption of innocence.

Isadora Neroni Rezende is a PhD Candidate in Law, Science and Technology – Rights of the Internet of Everything.

I. Neroni Rezende (✉)

Department of Legal Studies, University of Bologna, Bologna, Italy
e-mail: isadora.neroni2@unibo.it

## 1 Introduction

Cities worldwide are undergoing a radical shift towards digitization, a process that is often reconnected to the adoption of smart city strategies. At its core, indeed, the smart city paradigm – often described as fuzzy and elusive – implies the integration of digital technologies in urban infrastructure to achieve a more efficient and sustainable exploitation of available resources.[1] Unsurprisingly, one of the most crucial domains of implementation of digital technologies in smart cities is public security: in some parts of the world, being "smart" for a city basically equates to being "safe".[2] Against this background, private companies' efforts in marketing security technologies seem to have conveniently met the demands of law enforcement agencies, always in search of "smarter" strategies for crime prevention and early detection.[3]

Among these instruments, Automated Facial Recognition (AFR) certainly plays a decisive role, in both preventive and investigative activities. As well known, AFR involves the automated processing of digital facial images for the purposes of identifying, authenticating and classifying individuals[4]. Despite their invasiveness from a privacy and data protection standpoint,[5] in the last few years facial recognition technologies have gained big traction in both law enforcement and commercial domains.

On the one hand, indeed, different smartphone applications and banking services now rely on facial recognition to authenticate their users and unlock access to their services.

On the other, law enforcement is increasingly deploying facial recognition in public places and strategic venues (e.g. airports, train stations) to identify known or warranted individuals, specifically inserted in prepopulated watchlists.[6] Even in this context, however, the uses of AFR technologies widely differ around the world. China, for instance, is often mentioned as a worrying example of the unfettered use of facial recognition, which is often relied upon to catch jaywalkers and petty crime offenders.[7] In the United States, facial recognition has sparked an intense public and regulatory debate. In the wake of protests against police brutality and racism, big corporations such as Amazon, IBM and Microsoft have also set out a temporary moratorium on software sales to law enforcement;[8] nonetheless, tech start-ups – like the infamous Clearview AI – keep on providing their services to hundreds of local police departments across the country.[9] In Europe, finally, the advent of facial recognition in the security domain seems to advance at a slower pace, as when compared to Asia and North America. Instances of law enforcement agencies in the European Union using the technology are sporadic, but steadily growing.[10] Often cited examples of pilot projects comprise the ones conducted by the Hamburg and Berlin Police,[11] or that at the Zaventem airport in Brussels.[12]

As if AFR was not worrying privacy activists enough, law enforcement agencies worldwide are starting to go even further, coupling its deployment with emotion recognition technologies. Specifically, the latter build on affective computing[13] and AI to sense and acquire information about human emotional life.[14] A wide range of physiological inputs

[1] Albino et al (2015), p. 2 ff.; Kummitha, Crutzen (2017), pp. 43, 45.
[2] Marat, Sutton (2021), p. 248.
[3] On the potentialities of AI applications in law enforcement and criminal justice, see Lasagni, in this volume; Caianiello (2021).
[4] Adapted from Article 29 Data Protection Working Party (2012), p. 2. For an overview of face recognition technologies, their functioning, issues and implications see Berle (2020), pp. 1-17.
[5] Facial recognition technologies indeed process biometric data, a special category of personal data. On the notion of biometric data, see generally Kindt (2018).
[6] See, e.g., BBC News (2018).
[7] Notably, in China AFR is used to catch jaywalkers. See Liao (2018).
[8] Heilweil (2020).
[9] Clearview AI is an US-based tech company which provides facial recognition services. Notably, the app developed by Clearview runs its software not only on government-held images, but also on people's pictures scraped by social media network. On the matter see Neroni Rezende (2020).
[10] O'Flaherty (2020), p. 170.
[11] See, e.g., Raab (2019).
[12] Peeters (2020).
[13] Affective computing comprises both "the creation of and interaction with machine systems that sense, recognize, respond to, and influence emotions". See Daily et al (2017), p. 213.
[14] Mc Stay (2020), p. 1.

– such as facial movements, vocal tone, gait, respiration, heart rate, gaze direction – can be processed by machine learning algorithms to infer people's affective inner states.[15] When these tools are combined with facial recognition software, the system is designed to deduce the individual's emotional condition primarily from her facial muscle movements.

At the moment, the applications of Emotion Facial Recognition (EFR) are varied in the security context.[16] Within criminal proceedings, EFR is being tested to detect liars during police interrogations: Often marketed as more refined descendants of polygraph machines,[17] software like CM Cross, EmoKit, Miaodong and Sage Data rely on facial expression images, vocal tone, heart rate and similar datapoints to determine interviewees' emotions during police questionings.[18]

On the other hand, "early warning" systems are leveraged by the police in preventive activities to spot suspicious individuals in public venues. One famous example is the US Transportation Security Authority's 2003 Screening Passengers by Observation Techniques (SPOT) program, which in the aftermath of 9/11 aimed to find terrorists by scrutinizing airline passengers displaying fear or stress.[19] In China, instead, a research paper published by the Hubei Police Academy examines the value of facial expression to identify "dangerous people" and "high-risk groups" who do not have prior criminal records. The author of this research proposes to build a database of video images of offenders before and after they have committed crimes, in order to train an algorithm to pick up individuals involved in illicit undertakings.[20] In this kind of situations indeed, the claim is that offenders suffer high psychological pressure and cannot really hide their true inner states.[21] The reasoning behind preventive EFR systems already finds application in different software like Alpha Hawkeye, CM Cross, Joyware and Shenzhen Anshibao, which specifically detects light vibrations on faces and bodies to infer mental – and especially aggressive – states.[22] While it is evident that Chinese-based companies are heavily betting on the success of these tools, it should be highlighted that European law enforcement authorities are not immune to the charm of EFR. For instance, it is noteworthy to mention the Horizon 2020-funded iBorderCrtl program shortly trialed in Hungary, Latvia, and Greece.[23] With the aim of ensuring faster and more efficient border controls, AI-equipped cameras scanned travelers' faces for signs of deception while they responded to border-security agents'.[24]

In light of such growing interest towards these technologies in the security context and beyond, this contribution proposes a wide-ranging assessment of the use of EFR in public places for the purposes of law enforcement. This analysis is very topical, considering the recent publication of the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act).[25] That is why, before setting the terms of the investigation, an overall picture of the rules that have been put forward in this prospective piece of legislation, in relation to both AFR and emotion recognition technologies, will be presented.

## 2 Facial and Emotion Recognition Technologies in the EU Proposed AI Regulation

Recital 38 of the newly proposed Artificial Intelligence Act (hereinafter "the Proposal") highlights the significant degree of intrusion on fundamental rights – such as privacy and data protection, effective remedy and fair trial rights – caused by the use of AI systems in the law enforcement context. Because of the power imbalance that exists between

[15] Article 19 (2021), p. 15.
[16] On different applications beyond the security domain, see Mc Stay (2020).
[17] On lie detectors and their implications in criminal proceedings, see Lasagni (2021).
[18] Article 19 (2021), p. 21.
[19] Crawford (2021).
[20] Article 19 (2021), 19.
[21] *Id.*
[22] *Id.*
[23] iBorderCrtl (2016). Critically assessed by Sánchez-Monedero, Dencik (2020).
[24] Article 19 (2021), p. 19. See also Gallagher, Jona (2019).
[25] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final. Critically assessed by Vaele, Borgesius (2021); Papakostantinou, De Hert (2021).

public authorities and individuals that could be subject to surveillance,[26] the Proposal classifies these systems as "high-risk" when employed in this domain, thereby submitting them to a "stricter" regime in terms of obligations impending on the users. Although the list should not be considered as comprehensive, the Recital enumerates different kinds of technologies that could fall within this discipline, including individual risk assessments software, lie detectors and 'deep fakes' tools.

While emotion *facial* recognition in itself is not specifically tackled in the Proposal, two of its building technologies (AFR and emotion recognition technologies) are.[27] AFR is defined by the Proposal as "remote biometric identification", a notion that, according to the proposal, should be interpreted functionally so as to refer to "an AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used".[28] A distinction is made between real-time and post biometric identification, where the former identifies systems involving the use of "live" or "near-live" materials, such as CCTV footage. This kind of application is regulated at Article 5 of the Proposal, which lists (tendentially) prohibited AI practices. Using a negative formulation, the provision bans the use of AFR in publicly accessible[29] places for law enforcement purposes, unless specific conditions apply.

While observing the principle of strict necessity, AFR should be deployed only for the following grounds: (i) the targeted search for specific potential victims of crime, including missing children; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; (iii) the detection, investigation and prosecution of a serious criminal offence for which the European Arrest Warrant does not demand the so-called dual criminality requirement".[30] In addition, the provision lays down further parameters – inspired by a risk-based approach informing the whole Proposal – that should guide a case-by-case assessment on the opportunity of the deploying live facial recognition. These are: (a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system; (b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

Importantly, Article 5(2) of the Proposal also recalls the applicability of the proportionality principle, with specific regard to temporal, geographic and personal limitations in the use of the technology. In any case, implementation of the AFR in publicly accessible places for law enforcement purposes should be subject to the prior authorization of a judicial or independent administrative authority, on the basis of a "reasoned request" including objective evidence or clear indications so as to the necessity and proportionality of its deployment.

For situations of urgency, the use of the system may be commenced without a prior authorization, and a subsequent intervention of an independent authority is allowed only during or after the use. Finally, the Proposal leaves a space for national regulation on the matter by Member States, which are called on to provide for detailed national rules for the

[26] Malgieri and Ienca note indeed that the scheme of classification of high-risk AI system seems to revolve around three main criteria: (i) the type of AI system; (ii) its domain of application and (iii) its human target. This implies that if AI systems featuring limited risks are employed in very sensitive contexts and used for practices falling under the unbearable risk list they would be prohibited. This mechanism emerges clearly in the case of EFR that is labeled as low-risk when employed, for instance, in the commercial context, and as high-risk when used in law enforcement or education. See Malgieri, Ienca (2021). The Consultative Committee on the 108+ Convention has also highlighted the sensitivity of the law enforcement context, also in light of the power asymmetries between public authorities and data subjects. See Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (2021).

[27] It should be noted that biometric *identification* systems should not be conflated with biometric *classification* ones. Generally speaking, facial recognition technologies may have three different purposes: (i) verification/authentication; (ii) identification; (iii) classification/categorization. For an overview, see Castelvecchi (2020).

[28] Recital 8 of the Proposal.

[29] See Recital 9 of the Proposal for a notion of "publicly accessible place".

[30] See Art. 2(2) of the Framework Decision 2002/584/JHA: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision, OJ L 190, 18.7.2002, p. 1–20.

request, issuance and exercise of necessary authorizations, the criminal offences legitimizing the use of the technology and the authorities that could use such systems.[31]

Furthermore, emotion recognition technologies are explicitly comprised into the scope of the Regulation under Article 1(c) of the Proposal. They are defined as an "AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data".[32] Differently from live AFR, (biometric) emotion recognition *per se* is not targeted by many provisions in the Proposal. Depending on the functionalities concretely embedded in the system, EFR applications may be subject to different layers of rules in the framework of the Regulation. The Proposal only regulates a specific instance of facial recognition technologies in the law enforcement domain, namely those that perform strict identification operations by comparing biometric inputs with templates pre-stored in dedicated watchlist databases (i.e. the so-called "one to many" comparison). Software processing facial images data may then fall within this regime only if it integrates this kind of functionality, and this applies also to EFR systems. As known, however, EFR and more broadly biometric categorization systems do not always involve identification of targeted individual.[33]

When these applications are often leveraged in the commercial context, for instance, individuals' singling out is not always foreseen.[34] At the same time, implementation in the law enforcement domain cannot be excluded a priori. Here identification becomes key to many – if not all – activities of public authorities.[35] In EFR policing uses, one-to-many identification may not a direct function of the software, but it is certainly an objective pursued by law enforcement agencies employing such systems – and it may be performed "manually" at a subsequent moment. That is, identification may be carried out first-hand by human police officers having stopped the individual targeted by the software. In this latter case, EFR would not strictly fall within the scope of the rules laid down at Article 5 of the Regulation. Nonetheless, as it will be also argued later on, where identification objectives are still pursued, it would still be appropriate to apply this regime.[36]

Emotion recognition is lastly mentioned at Article 52 of the Proposal, which foresees transparency obligations for certain AI systems. Because of the specific nature of law enforcement activities, the provision excludes that technology providers should design the systems in such a way that individuals may be aware that they are interacting with an artificial agent, unless when these tools are available for the public to report a criminal offence.[37]

In conclusion, it is noteworthy to mention that Article 2(4) of the Proposal foresees a significant limitation to the scope of the Regulation in specific law enforcement scenarios. In derogation to the rules laid down in Article 2(1)(c) of the Proposal, Article 2(4) exempts public authorities in a third country or international organizations from complying with the standards set out in the Regulation, provided that these entities use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or more Member States.

Regrettably, this provision seems to ignore the hierarchy of the sources of the law within the EU system.[38] While international agreements concluded by the Union need to respect EU Treaties but not secondary law, those autonomously concluded by Member States are entirely subject to the principle of the primacy of EU law. Hence, it seems difficult to understand how a Regulation could exempt public authorities from respecting European human rights standards (enshrined in EU primary law) in extraterritorial operations carried out in the framework of international agreements to

[31] Cf. Article 10 the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131 (the Police Directive).
[32] Art. 3(34) of the Proposal.
[33] See note 30 for an overview of different facial recognition systems.
[34] In this case emotion facial recognition technologies are also referred to as "soft biometrics". See McStay (2020), p. 4. Examples of this kind of applications involve EFR embedded in billboards and shopping malls cameras to register people's emotional reactions to adverts displayed in public venues.
[35] Kotsoglou, Oswald (2020), p. 87; Neroni Rezende (2020), pp. 382-383.
[36] Below, Sect. 5.
[37] Art 52(1) of the Proposal. Under Art. 52(2), this applies also to biometric classification.
[38] On the position of the international agreements concluded by the Union within the hierarchy of the sources of EU law, see Tizzano (2014), pp 149-156.

which the Union is not a party. A reversal of the hierarchy of EU legal sources appears here to be at play, and this dangerously creates a hole in the application of human rights safeguards in these extraterritorial scenarios.

## 3 Which Room for Emotion Facial Recognition in Europe?

Given that the use of EFR technologies is increasing worldwide, and instances of its application have also been witnessed in Europe,[39] it seems appropriate to engage in a legal assessment of the technology against the European human rights framework, comprising both the Charter of Fundamental Rights of the EU (CFREU) and the European Convention of Human Rights (ECHR).[40] Our analysis will be articulated in two steps. First, the question of whether EFR can at all be deemed to be compatible with the CFREU and the ECHR will be addressed. This Section will examine the first conditions set out by Article 52(1) CFREU to justify the interferences on CFREU rights, and will mainly revolve around the "essence of the right" criterion. The second Section will then shift the focus to the proportionality test only, to see whether, regardless of the outcome of the first evaluation, EFR can be considered compliant with these further requirements of Article 52 CFREU.

The analysis will mainly take preventive activities of law enforcement in public urban spaces as a reference setting. As suggested, normative benchmarks for this assessment will leverage the rights to privacy and data protection, given the strict inapplicability of other fair trial rights in the preventive phase.[41] This choice presents several advantages. Firstly, both rights apply to data-driven preventive activities of security agencies by explicit legislative provision, as provided by Article 1(1) of the Directive 2016/680/EU (the Police Directive).[42] Secondly, privacy and data protection present strong conceptual links with other fundamental rights – even in the criminal context – as the former are often framed as instrumental rights.[43] This is true for instance with regard to the freedom of thought that, as we will see, is also called into question by emotion recognition technologies. The freedom of thought and the right to privacy seem to revolve specifically around the protection of *thoughts* when it comes to preserving the inner self of the individual. Certainly, the association of these entitlements to mere (involuntary) emotions may not seem totally fitting. As a premise for the assessment, however, it can be argued that emotions are actually very like thoughts. The link between emotions and thoughts has indeed been explored from both a philosophical and cognitive perspective.[44] Given the similarities between thoughts and emotions, it is reasonable to assess the impact of EFR against the abovementioned rights, whose span of protection should equally cover thoughts and emotions alike.

Finally, the rights to privacy and data protection share a "common concern" with the presumption of innocence, that is the protection of the individual against undue stigmatization. While this fair trial right is not specifically designed for the preventive phase, a strong upholding of these other "kindred rights" may achieve an anticipated application or coverage in this domain as well. From this perspective, one last Section will explore the possible tensions between the use of EFR technologies and the rationale behind the presumption of innocence.

## 4 Lawfulness, General Interest and the Interest of the Rights at Stake

### *4.1 Lawfulness and General Interest*

[39] See, e.g., European Parliament (2021).
[40] The European framework has been rightly described as a multilevel system of protection of fundamental rights. See Kostoris (2018), p. 68 ff.
[41] Cf. Neroni Rezende (2021), p. 375, note 63. On the qualification of data stemming from EFR processing as personal data and thus the applicability of the EU data protection framework, see Ienca, Malgieri (2021).
[42] See, e.g., Art. 1(1) of the Police Directive.
[43] Rouvroy, Poullet (2009), p. 50; Hildebrandt (2010), pp. 36-37.
[44] In philosophy, see Nussbaum (2001), p. 33. In cognitive research, see Feldman Barrett (2017), pp. 1–23; Science Daily (2017).

First of all, when assessing the legitimacy of a measure limiting fundamental rights, the existence of a legal basis should be verified. Indeed, the need for a legal basis grounding (and framing) the encroachments upon the rights protected emerges clearly both at the level of primary and secondary legislation in the EU. This is echoed at Article 8(2) of the Convention, which should be taken into consideration in consideration of the so-called "equivalence clause". At the level of secondary law, the lawfulness requirement is one of the foundational principles of the EU legislation on data protection, and it is indeed recalled by Article 4(1)(a) of the Police Directive. The use of EFR technologies should then be explicitly foreseen in a further legal basis of national or EU law.[45] This text should in particular determine the grounds and purposes of the implied data processing operations, pursuant to the purpose limitation principle, another tenet of EU data protection law.[46]

Interpreting the lawfulness principle in compliance with the jurisprudence of the ECtHR, the "quality of the law" doctrine should also be taken into consideration. In order for this requirement to be satisfied, the Court demands that the legal basis in question is at once "foreseeable" and "accessible".[47] The quality of the law requirement has also been examined within the specific context of preventive and covert surveillance measures.[48] The ECtHR has specified that here the meaning of foreseeability is not the same here as in other domains. Specifically, "foreseeability" means here that the law should simply be clear enough to inform citizens of the *circumstances* in and the *conditions* on which public authorities are empowered to resort to these measures.[49] In particular, the legal basis for surveillance should precisely frame the margin of discretion afforded to public authorities in resorting to these tools, as safeguard to potential abuses.

A second requirement to be met refers to the general objectives pursued with the use of the surveillance tool. This criterion has never posed significant challenges in the law enforcement context, and the same goes for EFR technologies. On the one hand indeed, Article 8(2) of the ECHR explicitly mentions national security, public safety and prevention and prosecution of crimes as legitimate aims justifying encroachments upon the right to private life. On the other, the CJEU has recognized the prevention, investigation and prosecution of criminal offences and the protection of national security as objectives of general interests under the Charter.[50]

### *4.2 Essence of the Right*

If these cumulative criteria are satisfied, the analysis should then turn to the "essence of the right" requirement. Because of its vagueness, this criterion has been subject to significant doctrinal and jurisprudential analysis, both at the EU and national level. For instance, Brkan defines it as "the untouchable core or inner circle of a fundamental right that cannot be diminished, restricted or interfered with".[51] The roots of the concepts are often traced back in the German legal system, where Article 19(2) of the Constitution provides that "[i]n no case may the essence [*Wesensgehalt*] of a basic right be affected".[52] While the notion has made inroads in other Member States' constitutional settings, the CJEU had its first recourse to the essence of the right in the landmarking case *Nold*. There, the Court recognized fundamental rights as being part of Community (now Union) law and underlined that these can be limited only "on condition that the *substance* of these rights is left untouched".[53] In absence of any binding text of primary law, the Court gradually developed this

[45] Noteworthily, Recital 41 of the Proposal for the AI Regulation excludes that the latter can be understood as providing for a legal basis for the use of the technologies and related data processing operations tackled in the text.
[46] Art. 4(1)(b) of the Police Directive.
[47] For a very detailed reconstruction of how the case law of the ECtHR and CJEU evolved in this respect, see De Hert, Malgieri (2020).
[48] See, e.g. ECtHR, *Roman Zakharov v Russia*, judgement of 4 December 2015, Appl. No.47143/06, para. 229; ECtHR, *Big Brother Watch and others v the United Kingdom*, judgement of 13 September 2018, Appl. Nos. 58170/13, 62322/14 and 24960/15, para. 306.
[49] ECtHR, Grand Chamber, *Big Brother Watch and Others v United Kingdom*, judgement of 25 May 2021, Appl. Nos. 58170/13, 62322/14 and 24960/15, para. 333; ECtHR, *Zackarov v Russia*, para. 229; ECtHR, *Malone v the United Kingdom*, judgement of 2 August 1984, Appl. No.8691/79, para. 67; ECtHR, *Huvig v France*, judgement of 24 April 1990, Appl. No.11105/84, para. 29; ECtHR, *Kruslin v France*, judgement of 24 April 1990, Appl. No.11801/85, para. 30; ECtHR, *Rotaru v Romania*, judgement of 4 May 2000, Appl. No. 28341/95 para. 55; ECtHR, *Weber and Saravia v Germany*, judgement of 29 June 2006, Appl. No.54934/00, para. 93;
[50] Cf. CJEU, *Digital Rights Ireland and Others*, judgement of 8 April 2014, Joined Cases C-293/12 and C-594/12, paras. 41-42; CJEU, *La Quadrature du Net and Others*, judgement of 6 October 2020, Joined Cases C-511/18, C-512/18, C-520/18, para. 122.
[51] Brkan (2018), p. 333.
[52] *Id.*, p. 339; Ojanen (2016), p. 324.
[53] CJEU, *Nold v Commission*, judgement of 14 May 1974, Case C-4/73, para. 14 [emphasis added].

autonomous concept[54] while taking inspiration from both national constitutional traditions of Member States[55] and the case law of the ECtHR.[56] As crowning of this jurisprudential path, the "substance" of rights was then translated into the Charter with a different wording, becoming the "essence".

Despite this final acknowledgement in EU primary law, the "essence of the right" criterion has long been subject to diverging interpretations. In particular, two doctrines have been counterposed: the relative (or exclusionary) theory and the absolute (or integrative) one. The divergence between the two revolves around the relationship of the "essence of the right" with the proportionality assessment. On the one hand, the proponents of the absolute theory conceive the essence of the right as being completely independent from the proportionality principle. The starting point is that fundamental rights are conceptualized as being composed of a nucleus and a peripheral part which can be restricted exclusively under certain conditions.[57] The proportionality test would thus apply only to peripherical limitations to fundamental rights, being the core of the right absolutely immune from such restrictions, even in presence of powerful overriding reasons.[58] On the other hand, the relative theory tends to merge the "essence of the right" criterion and proportionality assessments. Essence has only a declarative value because the legitimacy of *any* interference can be assessed through the lens of proportionality. In the EU legal framework, a literal interpretation of Article 52 CFREU suggests that an absolutist approach is preferred.[59] From the *Digital Rights Ireland* judgement onwards, indeed, the case law of the CJEU has made increasing references to this criterion and confirmed the latter interpretative perspective.[60]

While seemingly of a pure doctrinal nature, this discussion has undeniable practical consequences in the case at hand. The implications of an absolutist conception of the "essence of the right" parameter have first become tangible in the *Schrems* case. Here the CJEU annulled the Safe Habour scheme only based on a finding of violation of the essence of the rights to privacy and judicial protection.[61] As a result, the CJEU esteemed that it was not necessary to perform a proportionality test, thus reinforcing the independent conception of the essence of the right in its relationship with proportionality.

Despite the importance attributed to this criterion, the Court has never determined – on a pure theoretical level – *what* the essence of a right actually is. However, there is consensus in the legal doctrine that this is the result of an intentional choice of the CJEU. Even with few opportunities to examine the respect of the rights' essence, the Court seems to suggest that this is necessarily a *contextual* concept and that it can only be determined on a case-by-case basis, in consideration of the factual circumstances of the case.[62] When thinking about the impact of emerging technologies, this vague approach certainly presents its advantages, being able to simply unfold its potential in ever-new factual and legal situations. In the case of EFR indeed, there are strong reasons to believe that these tools impinge upon the very essence of the rights to privacy, data protection and the freedom of thought, with no further need for performing a proportionality assessment, as it will be shown next.

#### 4.3.1 Privacy and Freedom of Thought

With respect to privacy, for instance, it is well acknowledged that one of the constitutive elements of the right is the protection of one's thoughts and inner states (i.e. so-called mental privacy), which also comprises the freedom *not* to manifest one's thoughts[63]. The protection of the mind and the individual's self-determination serves indeed as the common rationale for privacy and the freedom of thought, which are even jointly conceptualized in some constitutional frameworks[64].

---

[54] Brkan (2018), p. 347.
[55] *Id.*, pp. 341-344.
[56] *Id.*, pp. 348-349 (discussing the inconsistency of the interpretation and application of the notion in the ECtHR's jurisprudence).
[57] *Id.*, p. 336.
[58] *Id.*
[59] Brkan (2018), p. 360. As for the ECHR, a similar stance is proposed by Rivers (2006), pp. 184-185.
[60] *Compare* CJEU, *Digital Rights*, paras. 39-40; CJEU, *Tele2 Sverige and Watson and Others*, judgement of 21 December 2016, Joined Cases C-203/15 and C-698/15, para. 101; CJEU, *Opinion 1/15*, Opinion of the Court (Grand Chamber) of 26 July 2017, para 150.
[61] CJEU, *Maximillian Schrems v Data Protection Commissioner*, judgement of 6 October 2015, Case C-362/14, paras. 94-95. For a thorough analysis, see Ojanen (2016).
[62] Ojanen (2016), p. 326. Christofi, Verdoodt (2019). Tzanou (2017), p. 43. See also Brkan (2018), p. 363 ff.
[63] Koops et al (2017), pp. 531-532; Mantovani (2013), p. 588, note 6.
[64] Koops et al (2017), p. 531.

Also, in the structure of the freedom of thought, people's inner mental space is covered by an absolute protection in Article 9 of the Convention, being only external manifestations subject to possible restrictions[65]. By pretending to capture into datapoints the most intimate aspects of one's life, in absence of any will of the individual to share them, it is possible to argue that EFR technologies engage the very substance of the right to mental privacy and the freedom of thought. Importantly, the outcomes of the processing do not need to be accurate to engender an interference on the rights at stake[66]. Especially with regards to privacy, but the argument could be extended to the freedom of thought as well, the right may be considered to be violated even if the invasion entails falsely attributing to a person some opinion.[67] In EFR, the contents of the mind are reified and used as basis for decision-making, unbeknownst or against the will of the subject. Being unaware of where this kind of invasive processing may intervene, individuals are also exposed to the chilling effects of surveillance and can be subtly manipulated into avoiding unordinary behavior. Therefore, they may also be restricted in their freedom of self-determination, freedom of expression and assembly in any public place, in such a way that no overriding interest could justify.

Besides, it has also been submitted that the essence of fundamental rights is essentially connected to human dignity, which may even work as a grounding basis for an independent conceptualization of the essence.[68] The Explanations to the Charter, indeed, seem to equate the need for respecting human dignity with the core essence of the rights protected.[69] Generally, in the case of AFR, it has been purported that the fact of transforming the human face into an item for objectivization and measurement touches upon the very dignity of the individual.[70] When this biometric processing reaches out to emotions – the most private element of our personal life – it can be argued that individuals are susceptible of being deprived of their own dignity, provided that this kind of "emotion reading" carried out by the machine is non-consensual or covert.[71]

#### 4.3.2 Data Protection

With regard to the right to data protection, it may be useful to make reference to the *Schrems* case once again. In this decision, the Court considered that the right to judicial protection was compromised in the Safe Harbour regime because any effective remedy to access, erase or review individuals' data was lacking. The existence of legal remedies to injustices is the logical premise to the effectivity of any fundamental right, and this need is explicitly recalled in the Charter with special regard to the right to data protection. Article 8(3) provides indeed that compliance with data protection rules should always be subject to the control of an independent authority. Because of the specific features of EFR technologies, it is safe to argue that an effective review of this kind of biometric processing would be impossible or very difficult, thereby making the safeguard of Article 8(3) of the Charter practically ineffective.

The difficulties in challenging the decisions of EFR systems stem from doubts concerning the science underlying emotion recognition technologies. From a psychological perspective, these find their roots in the work of Paul Ekmann, who in the 1960' developed a theory according to which all human emotions can be reduced to small number of "micro-expressions".[72] Today, the mistrust towards the scientific foundations of this approach has significantly increased, to the point that emotional AI – and consequently EFR – has often been labelled as a "pseudoscience".[73] Among the most critical arguments against Ekman's work there is the supposedly discriminatory nature of his findings, which would be blatantly

[65] Schabas (2017), p. 420.
[66] The scientific community is quite divided on whether EFR technologies are accurate and can actually "read our minds". As reported by Murgia (2021), the EFR company 4LittleTrees claims around 85% of accuracy, while Affectiva more than 90%, as indicated by Heaven (2020), p. 504. Nonetheless, these results should be taken with a grain of salt. Indeed, one of the major underlying issues concerning the accuracy of these technologies seems to be data annotation. Before the EFR system is trained, datasets need to be labelled by humans choosing whether a given individual in a picture is expressing feelings of fear, happiness etc., often without any context. Even in this case, experts disagree about whether humans are always able to correctly read other's facial expressions. In this sense, a panel of experts led by psychologist Lisa Feldmann Barrett has recently reviewed more than 1000 contributions on the matter, concluding that there is little to no evidence that people can reliably infer someone else's emotional state from a set of facial movements. See Heaven (2020), p. 503. Cf. also Chen et al (2018).
[67] Prosser (1984, original work published in 1960), p. 107; Schoeman (1984), p. 16.
[68] Brkan (2018), p. 365.
[69] See Explanation on Article 1. Explanations relating to the Charter of Fundamental Rights OJ C 303, 14.12.2007, p. 17–35.
[70] McStay (2020), p. 3 (citing Wiewieorowski (2019)).
[71] Different might be the case in which the user voluntarily decides to interact with emotional AI, see McStay (2018).
[72] See Crawford (2021); Thomas (2018); Kelion (2019).
[73] Article 19 (2021), p. 6; Mc Stay (2020), p. 2.

ignorant of social, cultural and contextual factors impacting on the display of emotions.[74] Against this background, it could be asked whether any effective remedy against a supposedly arbitrary or highly mistaken profiling of the data subject – possibly involving racial discrimination – is imaginable.

Where the very scientific foundations of the technology are unclear or highly questioned, which criteria should be employed to perform a sound review the data processing? Would it ever be possible to achieve a reasonable outcome in such processing? According to which scientific standards should it be determined? In other words, the idea that it would be possible to ensure an effective review of data processing operations carried out by EFR technologies seems to be highly questionable.

As highlighted by Tzanou, the "hard core" of the right to data protection – but the argument could be extended to the right to privacy and the freedom of thought – would be "what needs to be protected", i.e. the final values that are protected by such rights: dignity, informational self-determination and individual autonomy. In light of what mentioned above, these values may be irreparably jeopardized by the use of EFR technologies in (urban) public spaces. In other words, there is an *a priori* incompatibility between these tools and the European human rights framework.

As it has been noted, when a shortcoming is detected in assessing one of these first compatibility requirements, there is no need to perform a proportionality test. In the case of EFR, it can be argued here that such technologies should be banned because their use is simply incompatible with the essence of the right to privacy, the freedom of thought and the right to data protection. Nonetheless, it may still be useful to engage in a proportionality assessment of EFR. Considering the significant economic interests behind the development of the emotional biometrics industry and its implicit acknowledgement in the Proposal for the AI Regulation, limiting ourselves to proposing a ban of the technology would not probably bring a great practical contribution to the ongoing debate. Also, if end-users of the technology (e.g. law enforcement agencies) did not consider the essence of the rights at stake to be interfered upon, these would still need to carry out a proportionality assessment of the technology at hand. To this end, the next Section will engage with such test. This analysis will reveal that, even if the use of EFR in law enforcement were compatible with EU human rights standards, its acceptable deployments in real case scenarios would be very limited.

## 5 Proportionality: Applying AFR Requirements to EFR

### *5.1 Suitability and Necessity*

The proportionality principle is the last requirement listed in Article 52(1) of the Charter. Notably, the CJEU was heavily inspired by the German Federal Constitutional Court in developing the procedural steps of its proportionality test, which first comprises an assessment of the suitability and necessity of the measure. In the specific context of data-driven technologies, the European Data Protection Supervisor has also clarified that the necessity test calls for an "assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal".[75] Thus, the assessment of the strict necessity – but also of the suitability of the technologies – requires a factual evidence basis.

Against this background, it is useful to recall an often-cited initiative, the US Transportation Security Authority's 2003 Screening Passengers by Observation Techniques (SPOT) program. The employed software was directly built on a system set up by Ekman, which could automatically detect the six fundamental micro-expressions studied by the psychologist at a large scale. Ekman's method was then further leveraged to train "behaviour detection officers". During the implementation phase, the program was highly criticized not only for its supposedly embedded racial biases, but also for its lack of effectiveness and credibility.[76] Specifically, involved officers reported that passengers were flagged and interviewed more or less randomly, and the scarce number of arrests made was totally unrelated to terrorist offences,

[74] Crawford (2020); Article 19 (2021), pp. 15-16; Sedenberg, Chuang (2017), p. 2; Korte (2020). For empirical evidence, see Chen et al (2018).
[75] EDPS (2017), p. 5.
[76] Schwartz (2019).

which were the main targets of the initiative.[77] Even more worryingly, it was claimed that the program itself was leveraged to cover racial profiling practices.[78] Eventually, the US Transportation Security Authority decided for the future to limit funding for behaviour detection activities, claiming that no evidence could support the suitability and effectiveness of the system which had costed the government 900 million US dollars.[79]

Moreover, the suitability of policing initiatives leveraging EFR could also be called into question from another perspective. When deployed in public spaces, especially those passed through by a significant number of people, AI cameras would presumably collect many different inputs. To review them, police departments in charge would need to allocate a considerable amount of trained personnel in dedicated control rooms. This would be a necessity imposed from both practical and legal requirements. On the one hand, indeed, human review would be essential to exclude from further scrutiny people that have been targeted due to an obvious error of the machine. On the other, Article 11 of the Police Directive would require in any case a human in the loop before any negative decision – like being subject to a search – is taken with regard to the individual. Thus, regardless of the level of accuracy reached by the machine, any effective EFR initiative would have to be supported also by human resources, which are often lacking in underbudgeted law enforcement agencies. Hence, one could wonder if deploying EFR in urban policing would be more financially burdensome than directly sending patrolling officers looking in strategic venues. Decisions on the deployment of EFR should consider the financial affordability and sustainability of such programs when compared to traditional stop and frisk practices. In such assessments, it should also be taken under consideration that CCTV cameras in uncontrolled environments may provide lower quality images, which in turn may affect the accuracy (and thus the effectiveness) of the processing.[80]

## *5.2 Proportionality* Stricto Sensu

The last argumentative passage of the CJEU's test is the proportionality *principle in its strictest application*. Almost indulging on a political task, the Court balances the impinged rights and the pursued values, questioning whether the legislator has made a correct use of its margin of appreciation. When the limitation imposed on the right is considerably serious, it tends to apply a stricter approach,[81] thereby requiring foreseen restrictions to be outbalanced by strong safeguarding countermeasures.

### 5.2.1 The Need for a Stricter Scrutiny

In the case of EFR use in public spaces, it should be preliminarily highlighted that a very strict proportionality assessment should be performed in light of the seriousness of the interference at stake. Three elements push us towards this direction: (i) the kind of data and processing involved; (ii) the scope and context of the surveillance measure; (iii) the absence of notification mechanisms for individuals interacting with EFR systems. First of all, EFR technologies imply the automated processing of biometric data. Here, sensitivity invests both the kind of data and means of processing employed, and major safeguards against abuse by public authorities are required.[82]

Secondly, the scope of the envisaged interference should be taken under consideration. The use of EFR in uncontrolled environments can indeed capture the data of any individual passing within the range of the camera indiscriminately.[83] This kind of scheme thus involves the collection of biometric data on a large scale, and the significance of such

[77] *Id.*
[78] Ackerman (2017).
[79] US Government Accountability Office (2013). However, the US government has not completely given up emotional biometrics initiatives in the aviation security field, see Hogdson (2019).
[80] European Union Agency for Fundamental Rights (2019), p. 3.
[81] Cf. CJEU, *Digital Rights*, para. 48. Within the ECtHR's case law see ECtHR, *Segerstedt-Wiberg and Others v Sweden*, judgement of 6 June 2006, Appl. No. 62332/00, para. 88.
[82] *Id.* para. 54. See also Ienca, Malgieri (2021), pp. 9-10.
[83] The notion of uncontrolled environments covers "places freely accessible to individuals, where they can also pass through, including public and quasi-public spaces such as shopping malls, hospitals, or schools". Consultative Committee (2021), p. 5.

interference is magnified in public urban spaces where individuals do not often have the chance to opt-out neither control over the processing.[84]

Thirdly and finally, the lack of notification obligations for public authorities has been identified in the CJEU's case law as a criterion by which the seriousness of the interference can be assessed. That is because the absence of notification is "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance".[85] Such danger is very much present for EFR implementations in the security domain. Article 52(2) of the Proposal exempts users of biometric categorization systems from notifying targeted individuals of their *interaction* with an AI system when the technology is used for the detecting, preventing and investigating criminal offences.

While this derogation from the general transparency regime seems coherent with the latest ECtHR's approach to bulk surveillance systems,[86] its compatibility with the CJEU's view is less clear. In *Tele2/Watson* indeed, the Court has considered that when access to retained data was granted to law enforcement, targeted individuals should be notified of such processing and of the right to effective remedy, once such notification is no longer liable to jeopardize the investigations.[87] Translating this condition in the EFR context may not require law enforcement authorities to notify *every* individual of their exposure to an EFR system, but it may impose notification to every subject that has been labelled as dangerous by the technology once this can no longer affect the efficacy of investigations. In absence of any clear indication on this point, however, the absence of notification can certainly be taken into consideration as a factor demanding the application of a stricter proportionality assessment of EFR security deployments.

The need for a close scrutiny of EFR can also be argued from the angle of its fundamental difference with AFR identification. What strikes the most, indeed, is the lack of personal criteria of scope limitation in EFR applications. In these scenarios, law enforcement agencies are not looking for someone that is already known or warranted by the police, and inserted in pre-populated watchlists; they are pursuing the "unknown unknowns", scrutinizing anyone that displays suspicious behavior compatible with her being involved in criminal undertakings. This parameter of "scope-limitation" is thus excluded from the proportionality assessment. Instances of preventive EFR could then be associated with a *hybrid* form of surveillance featuring characteristics of both targeted and unfettered surveillance systems. On the one hand, the EFR surveillance initiatives are susceptible of being circumscribed from a temporal and especially geographical perspective, being deployable in restricted chosen venues for limited periods of time; on the other, EFR cameras can capture anyone within their visual range, even though the people pinpointed may not have any connection whatsoever with the commission of criminal offences.[88]

Overall, two main elements support the application of a very strict proportionality assessment. First, the greater intrusiveness of EFR technologies in the law enforcement domain. Second, in comparison with AFR, the inapplicability of personal limitations to the technology deployments. To exemplify the repercussions of adopting a stricter approach with EFR, it could be useful to look at the proportionality requirements already set out for remote biometric identification in public spaces by the Proposal for the AI Regulation. At the moment of writing, the Proposal is undergoing an ordinary legislative procedure before the competent EU institutions.[89] Being the outcomes of this process unknown at present, the analysis certainly bears some degree of speculative character.[90] This is all the more uncertain considering the recent joint Opinion of the European Data Protection Board (EDPB) and the EDPS, rejecting the regime laid down at Article 5 of the Proposal and calling for a ban of the AFR technology altogether. With regard to EFR specifically, the EDPB and EDPS

[84] Information Commissioner's Office (ICO) (2021), p. 9; see Consultive Committee (2021), p. 6 (discussing the role of consent in the use of AFR by public authorities).
[85] CJEU, *Digital Rights*, para. 37.
[86] While the ECtHR has acknowledged that subsequent notification is a relevant factor when assessing the effectiveness of remedies (see ECtHR, *Roman Zakharov*, para. 234; see also ECtHR, *Klass and Others v Germany*, judgement of 6 September 1978, Appl. No.5029/71, paras. 68-71; ECtHR, *Weber and Saravia*, para. 135), it has also considered that in bulk interception systems remedies that do not depend from previous individual notification may even provide better guarantees (see ECtHR, *Big Brother Watch*, para. 358). On notification in the ECtHR's surveillance case law, see De Hert, Malgieri (2020), pp. 26-29.
[87] CJEU, *Tele2/Watson*, para. 121.
[88] The same happens when social media databases are integrated in AFR software, enabling the identification of people that have not been inserted in watchlists. See Neroni Rezende (2020), p. 385.
[89] 2021/0106(COD) Artificial Intelligence Act, Legislative Observatory.
[90] EDPB-EDPS (2021), p. 3.

have also indicated that "the use of AI to infer emotions of a natural person is *highly undesirable* and should be prohibited".[91]

Regardless of the outcome of the legislative procedure undergone by the Proposal, this analysis may hopefully bring some theoretical and practical contribution to the debate on the regulation of EFR technologies.[92] Indeed, the rules set out in the proposed Article 5 embed certain criteria elaborated, in the last few years, by the European national and supranational Courts in surveillance case law. It has been underlined that *not all* EFR applications could automatically fall within the purview of the regime of Article 5 of the Proposal.[93] That is because some of these tools may not be designed to directly perform identification operations, specifically by matching the images of the people labeled as suspicious with a database of pre-stored templates. However, given the specificities of the law enforcement context, it seems pertinent to apply these criteria to EFR tools. Here, as said, public authorities always need to perform identification activities to pursue their primary objectives of preventing, and especially investigating and prosecuting criminal offences. Practically, emotional AI capabilities may be embedded in facial recognition software already designed for the identification of individuals. When such features are not available in the system, identification operations will probably be carried out subsequently by police officers themselves.

### 5.2.2. Guidelines from the European Surveillance Case Law

Different aspects should be taken into account when assessing fair and balanced implementations of EFR technologies in law enforcement: (i) grounds for authorization; (ii) scope-delimitation criteria; (iii) data storage requirements; (iv) *ex ante* and *ex post* supervision. To begin with the grounds that could legitimize EFR in public places, not all the criminal offences that authorize the use of facial recognition could probably serve the same purpose in this context. For instance, Article 5(1)(d)(iii) of the Proposal refers to the crimes listed at Article 2(2) of Council Framework Decision 2002/584/JHA and "punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State". Although these criminal offences are identified within the EU framework as falling within the category of serious crime,[94] they may not always reach such a level of gravity to justify the deployment of EFR, which implies the setup of an indiscriminate surveillance system (even though in specific locations). EFR, if suitable and effective, could be used only to address the most serious forms of crime which also fall within the State needs of protecting its national security. For example, that would be the case of terrorism, a domain where the overlap between intelligence and law enforcement activities is evident.[95] This argument finds corroboration also in the position recently adopted by the CJEU in *La Quadrature du net*. Here the Court found that only the objectives of safeguarding national security – from terrorist offences included – can justify more serious interference with fundamental rights.[96] Considering that the "mental data processing"[97] performed by EFR poses greater dangers than mere AFR identification, this kind of surveillance could be implemented only on the basis of objective evidence establishing a risk of a terrorist attack or of another immediate danger for national security.

Furthermore, Article 5 refers to geographical, temporal and personal limitations to ensure a proportionate use of AFR in public places for law enforcement purposes. Clearly, these criteria are drawn from the approach consistently applied by the CJEU in (mass) data retention cases since *Digital Rights Ireland*. The Court considers indeed that the goal of fighting against serious crime does not allow in itself an indiscriminate surveillance: any monitoring measure needs to be

[91] *Id.* The same opinion is shared by the Consultative Committee (2021), p. 5 [emphasis added].
[92] For instance, it has emerged that controllers often give insufficient consideration to necessity and proportionality issues tied to the deployment of such systems. See ICO (2021), p. 11.
[93] Above, Sect. 2.
[94] The same categories of offences are listed as constituting serious crime in the Annex II of the Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149.
[95] On the issues that the growing proximity between intelligence and law enforcement has raised, see generally Vervaele (2005); De Hert (2005).
[96] CJEU, *La Quadrature du Net*, paras. 135-137.
[97] Ienca and Malgieri identify "mental data" with emotions or other thoughts that are not "related to health status, sexuality or political/religious beliefs". See Ienca, Malgieri (2021), p. 1.

circumscribed by objective criteria presenting an objective link with the stated aims.[98] These criteria can for instance limit data collection measures to particular areas or categories of people presenting – in specific timeframes – objective risks related to the commission of serious criminal offences.[99] In absence of personal criteria of scope delimitation, temporal and geographical restrictions should be interpreted even more strictly than it would be the case for AFR. Quantifying the length and breadth of the surveillance measure remains however difficult at a theoretical level. As provided by Article 5 of the Proposal, decisions authorizing practical implementations of the technology need to be guided by risk-informed criteria, such as the likelihood of the foreseen negative event and the seriousness of its consequences. Only in light of such information, it would be possible to perform a balancing test to decide on the specific timeframe and location of EFR implementations. However, in order to avoid leaving a too wide margin of appreciation to public authorities, the relevant legislation should establish with sufficient clarity maximum delays and procedures for renewal of the measure.

According to the long-standing surveillance case law of the ECtHR and the CJEU,[100] clear and precise rules should also govern the procedures to be followed for subsequent storing of the data. In addition to data security standards, access to stored data shall be granted only to specifically trained officers, who should probably be less in number compared to those authorized to analyze AFR feeds. In this context, precautions to be taken before communicating data are also important. The expertise of the deployed officers has indeed a bearing on the effective application of the right not to be fully subject to an automated decision, foreseen in the EU general data protection framework.[101] In the preventive phase specifically, this right should be triggered automatically, regardless of any request of the data subject who is often unaware of the processing. This means that before taking any further action towards an individual flagged as suspicious, law enforcement agencies should *proprio motu* submit the assessment made by the AI agent to a manual review.[102]

When it comes to storage conditions, also maximum periods of retention play a significant role when assessing the proportionality of the surveillance system. To keep the intrusion within the limits of what strictly necessary, a difference should be made between data relating to individuals identified as potentially dangerous, and those that have not been determined to be so.[103] Similarly to what had been foreseen in the AFR Locate regime, data relating to the individuals that have not been labelled as dangerous should be immediately erased.[104] Also, retention periods for data relating to people flagged as suspicious should be severely restricted. Two scenarios can be discerned in this regard. If the initial positive match does not overcome the manual review, data shall be immediately erased as in the first case. If, however, the human agent esteems that the pinpointed individual does actually express a suspicious attitude, the data storage should be limited to the time strictly necessary for the authorities to decide whether and how to take action, or for the notified individual to challenge the decision.[105] Especially in real-time EFR scenarios, these decisions should be made in a very short timeframe to satisfy the preventive purposes of the surveillance initiative. In other words, EFR should only function as a tool for highlighting promising targets of intervention, assuming that one considers these systems capable of such a task. Thus, data should be retained for a very limited amount of time. Also, immediate erasure of the data should prevent any further use or "leak" in subsequent criminal proceedings, where these could be used as evidence.

---

[98] CJEU, *Digital Rights*, para. 57; CJEU, *Maximilian Schrems v Data Protection Commissioner*, para. 93; *Tele2/Watson*, para. 110; CJEU, *Opinion 1/15*, para. 191; CJEU, *La Quadrature du Net*, para. 133; CJEU, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, judgement of 6 October 2020, Case C-623/17, para. 78. With regard to the application of these criteria to the case of the AFR app Clearview, see Neroni Rezende (2020), 385 ff.

[99] This approach has also made inroads outside the EU legal system with the recent decision *R (Bridges) v the Chief Constable of South Wales Police* [2020] EWCA CIV 1058. Specifically, the Court of Appeal stated that two concerns arose within the legal framework of AFR Locate, namely the "who question" and the "where question". Indeed, in relation to the people that could be inserted in the watchlists and the locations where the technology could be deployed, legal rules were too generic and left an excessive margin of appreciation to public authorities.

[100] Starting from the *Huvig* judgement, the ECtHR elaborated a set of foreseeability criteria against which surveillance laws need to be assessed. These criteria have been later refined in the *Weber and Saravia* case, and have been thus called "Huvig" or "Weber" criteria since then. According to De Hert and Malgieri, these criteria have been implicitly integrated in the CJEU case law since the *Digital Rights Ireland* case. See De Hert, Malgieri (2020), p. 32.

[101] See Art. 11 Police Directive and Art. 22 GDPR.

[102] A similar mechanism is already provided in Art. 6(5) of the PNR Directive.

[103] The need for establishing difference in the storing regime according to the specific situation of the data subjects emerges clearly in the case law of the CJEU. See CJEU, *Opinion 1/15*, paras. 196-203.

[104] The AFR Locate program, implemented by the Welsh police and censured in the *Bridges* case, provided that when the facial data processing of passers-by did not lead to any positive match, such data should have been immediately erased. See *R (Bridges) v Chief Constable of the South Wales Police* [2019] EWHC 2341, para. 16.

[105] See paragraph below.

With regard to the nature and organization of *ex ante* and *ex post* supervision of EFR processing, one first concern is the system of authorization of EFR deployments. To ensure that these are circumscribed to what strictly necessary and that competing interests are reasonably balanced, the authorization should be given by an independent authority, in compliance with Article 8(3) of the Charter and the case law of both the CJEU and the ECtHR. Even though the ECtHR has expressed in the past a preference for judicial control, it suffices that the authority in question is capable to freely adjudicate without suffering interference by the government.[106] In the case at stake, this requirement does not seem to pose problems, as it is already foreseen by Article 5(4) of the Proposal.

Instead, a second set of concerns regards notification obligations for surveilled individuals. To ensure a fair balancing of the interests at stake, the interference with the rights to privacy and data protection should be compensated by strong safeguards, among which the right to an effective remedy. Regardless of their being checked by the police, should individuals targeted by EFR be notified of that a positive match has occurred in their situation? Different answers may be given depending on how the surveillance scheme put in place by EFR-equipped cameras is qualified. For instance, expressing a difficulty in totally embracing notification requirements,[107] the ECtHR esteems that bulk surveillance systems may not require a regime of bespoke individual notification, if remedies against inaccurate or unlawful processing are granted on a general basis to the population as a whole. According to the Court, in some cases this may even be the best solution to provide the highest standards of protection.[108] Nonetheless, when the intrusiveness of the technology is so serious, nothing would prevent legislators from cumulating two systems of remedies: one generalized and independent from the previous notification, and one based on notification for people having been specifically targeted by the system.

Considering the opposing interests at stake, it would indeed seem reasonable to generally exempt law enforcement EFR processing from transparency requirements, as provided by Article 52 of the Proposal. On the other hand, however, this derogation from the general regime does not appear to achieve a fair balance between security and fundamental rights needs when it comes to people singled out as dangerous by the system. In this case, the potential negative consequences for the data subject and the seriousness of the intrusion in her private sphere should outweigh the exigencies of opacity normally underlying law enforcement activities. Therefore, in conclusion, a fair balancing of the needs at stake could probably be obtained only with a bespoke regime of subsequent notification for individuals labeled as dangerous by the EFR system.

## 6 EFR and the Presumption of Innocence

It is widely acknowledged in the literature that emerging technologies are bringing about new challenges for the presumption of innocence.[109] Foreseen in different constitutional traditions,[110] as well as at the international[111] and EU level,[112] this principle is at the core of the notion of fair trial as foreseen in Article 6(1) of the Convention.[113]. In criminal

[106] De Hert, Malgieri (2020), p. 10. See also Malgieri, De Hert (2017).
[107] See De Hert, Malgieri (2020), pp. 26-29.
[108] *Big Brother Watch*, para. 358.
[109] See, e.g., Caianiello (2019); Hadjimatheou (2017), p. 40; De Hert (2005), p. 85.
[110] As indicated by Sayers (2014), p. 1305 ff. In 2012, the CJEU recognized the presumption of innocence as "a feature of the constitutional traditions common to the Member States". See CJEU, *Criminal proceedings against Marcello Costa and Ugo Cifone*, judgement of 16 February 2021, Joined Cases C-72/10 and C-77/10, para. 86.
[111] All EU Member States are part to the International Covenant on Civil and Political Rights, whose Art. 14(2) explicitly refers to the accused's right "right to be presumed innocent until proved guilty according to law".
[112] In primary EU law, the presumption of innocence is enshrined in Art. 48 of the Charter, whose explanations equate to the contents of Art. 6(2) of the Convention. Even before the entry into force of the Charter, however, the CJEU had already recognized the presumption of innocence as one of the fundamental rights protected in Union law (see CJEU, *Montecatini S.p.A*, judgement of 8 July 1999, Case C-235/92, para. 175). At the level of secondary law, this right is explicitly recalled at Art. 2 of the Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings OJ L 65, 11.3.2016, p. 1–11. On the protection of the presumption of innocence in the EU legal system, see generally Sayers (2014); Balsamo (2018), pp. 253-255.
[113] ECtHR, *Konstas v. Greece*, judgement of 24 May 2011, Appl. No.53466/07, para. 29. It is no surprise that the ECtHR frequently examines complaints of violations of the presumption of innocence with joint reference to both the first and second paragraph of Art. 6.

proceedings, the presumption of innocence functions both as a rule of judgement[114] and as a rule of treatment.[115] While the presumption finds application only in *ongoing* criminal proceedings, it is not specifically devised for the preventive phase.[116] Only persons that have been "charged" with a criminal offence can benefit from this important safeguard.[117] Despite the statutory limits of the principle, surveillance scholarship has raised multiple concerns over a supposedly increasing erosion of the presumption of innocence, weakened by emerging mass surveillance programs.[118]

These positions rely on an extensive interpretation of the principle, which is reworked as a "moral entitlement" based on civic trust. People have a right to be treated as trustworthy and should be presumed as acting in compliance with their main obligations in society, thus making any unfettered monitoring measure implemented by the State unjustified (e.g. mass data retention systems, ANPR, live facial recognition in public places). Where surveillance is not grounded on individual suspicion, the presumption of innocence is subverted by assuming everyone to be guilty of something. In the domain of criminal legal scholarship, Ashworth and Zedner have proposed a similar concept, i.e. the presumption of *harmlessness*. Like the presumption of innocence, this principle is underlined by the respect for each individual's status as a responsible agent in society.[119] This implies that, setting aside high-risk settings (e.g. airport security), people should not be subject to universal risk assessments as they should be "presumed free from harmful intentions".[120] Albeit being suggestive, these attempts to broaden the interpretation of the presumption of innocence have been criticized by some other scholars holding that this safeguard should continue to be understood in strict legal terms, i.e. as a specific fair trial entitlement applicable only within the boundaries of ongoing criminal proceedings.[121]

It can nonetheless be observed that preventive criminal justice cannot avoid all considerations associated to the presumption of innocence. If that were the case, eluding individual fair trial safeguards would be extremely easy for public authorities. Indeed, these would simply have to make recourse to preventive instruments to subtly circumvent the rights that are granted to suspects in the framework of criminal proceedings.

Against this background, there emerges in this case as well the need to pay a closer attention to the scope of the principle, possibly "anticipating" its protective effects also to the preventive phase. In a world where individuals are increasingly singled out thanks to ever more insidious technologies,[122] indeed, the risks for individuals to be wrongfully stigmatized are only destined to grow, dramatically. When it comes to EFR, specifically, potential issues with the presumption of innocence are twofold: (i) the lack of personal limitations in the scope of surveillance operations; (ii) the possibility of drawing adverse inferences against the suspect from inaccurate or unreliable processing carried out by the EFR system. In tackling these gaps, procedural safeguards attached to the rights to privacy and data protection seem to offer comparable standards of protection.

### *6.1 Absence of Personal Limitations*

As said, the first issue with EFR implementations – contrary to remote biometric identification – is the lack personal limitations in scope. People having no connection whatsoever with the commission of criminal offences may in fact suffer the negative consequences of EFR surveillance, and be wrongfully stigmatized because of it.[123] Interestingly, the absence of personal criteria and the resulting risks of undue criminalization seem to generate concerns for both the presumption of innocence and the rights to privacy and data protection. On the one hand, the ECtHR has indeed stated that the presumption of innocence shields the individual from the stigmatizing effect of an allegation of criminal liability, thus preserving her dignity.[124] On the other, the rights to privacy and data protection are – as pointed out above[125] – ultimately

[114] This means that the burden of proof is placed on the prosecution, and any doubt on the criminal responsibility of the accused should profit the latter. Cf. ECtHR, *John Murray v. United Kingdom*, judgement of 8 February 1996, Appl. No.18731/91, paras. 54; ECtHR, *Telfner v.* Austria, judgement of 20 March 2011, Appl. No.33501/96.

[115] This rule prohibits that the accused person is considered or treated as guilty before her responsibility is established by a court of law. Cf. ECtHR, *Shyti v. Romania*, judgement of 19 November 2013, Appl. No. 12042/05.

[116] De Hert (2005), p. 85.

[117] In this regard, it should also be noted that the Charter used a more neutral language compared to the Convention. Indeed, while Art. 6(2) ECHR employs the expression "charged with a criminal offence" – which should be nonetheless interpreted in light of the so-called '*Engel* criteria' – the Charter only uses the term 'charged', avoiding any explicit reference to criminal offences.

[118] Hadjimatheou (2017), pp. 41, 43 ff.

[119] Ashworth, Zedner (2014), p. 66.

[120] *Id.*, p. 130 (citing Floud, Young (1982)).

[121] Hadjimatheou (2017), p. 41.

[122] On the preventive turn taken by policing and the role played by digital technologies, see van Brakel, De Hert (2011); Brayne (2017); Ferguson (2017).

[123] Wrongful criminalization can be defined as "treating someone as if they have a particular propensity towards criminality or indeed are already involved in criminal activity, without proper grounds for doing so". See Hadjimatheou (2017), p. 45

[124] Balsamo (2018), p. 116.

[125] Above, Sect. 4.

aimed at the preservation of human dignity. Their relevance to this end is only increasing with the world's digital transformation, as personal data processing can easily result in discriminatory and otherwise stigmatizing practices.

The conceptual links between these safeguards could be spotted in the case law of the CJEU. While anchoring its considerations to the rights to privacy and data protection – and not specifically the presumption of innocence – the CJEU has raised concerns over the absence of personal limitations with regard to the provision of unfettered surveillance systems in the Union. In *Digital Rights*, for instance, the CJEU stated that the Directive 2006/24/EC (the Data Retention Directive) was susceptible for its indiscriminate scope of creating in the minds of the people concerned a (rather stigmatizing) "feeling that their private lives are the subject of constant surveillance".[126] Since this landmarking judgement, the approach taken by the Court in data retention cases has continued to be consistent. As confirmed in the recent *La Quadrature du Net* judgement, indeed, a data retention system targeting "persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with that objective of combating *serious crime*"[127] is simply not compatible with the principle of proportionality as enshrined in EU law.

In the same line of reasoning, more invasive measures involving the *real-time* collection and analysis of communication metadata directly by law enforcement can only be justified with regard to specific individuals, thus requiring "a valid reason to suspect that they are involved in one way or another in terrorist activities".[128] What emerges from this analysis is that particular serious forms of interference with the rights to privacy and data protection – if not justified by objectives of national security – need to be circumscribed by criteria of a personal nature, may these operate at a group or individual level. Further evidentiary elements need to substantiate a reasonable suspicion that such individuals may be involved in a criminal undertaking of a serious nature. As things stand, EFR seems not to be fit for ensuring the enforcing of such subjective limitations.

Thus, the use of EFR seems to be at odds with the requirements of the CJEU, and this gap cannot probably be overcome. Overall, if legal theorists are still struggling to stretch the applicability of the presumption of innocence – understood as a component of the fair trial – the rights to privacy and data protection seem to offer an equivalent coverage for individuals in less safeguarding phases of law enforcement activities broadly understood (including preventive one). It goes outside the scope of this contribution to explore the implications of this argument. Nonetheless, it can be observed here that the link between the presumption of innocence and the rights to privacy and data protection should probably be found in the centrality of the value of fairness in the safeguards they provide. These rights share a common concern for undue stigmatization, and more broadly for any *unfair* adverse treatment against the individual. This underpinning strive for fairness translates into safeguards of a *procedural* nature, aimed at providing of justifications for encroachments on individuals' personal freedoms. This aspect further emerges in the guarantees that the rights to privacy and data protection can afford with regard to adverse inferences that can be leveraged against the individual based on the processing of her personal data.

### *6.2 Adverse Inferences*

Another way in which the presumption of innocence could negatively be affected by EFR surveillance is the use of adverse inferences against the suspect or accused. In the case of EFR, these may be drawn from the "emotional demeanor" of the individual, caught in situations that the police find to be connected to the commission of a criminal offence. The use of presumptions can raise tensions with the presumption of innocence, as these can subtly reverse the burden of proof that should always weigh on the prosecution. Still, the ECtHR has clarified that the existence of presumptions of fact or law that may operate against the accused does not necessarily violate the presumption of innocence. This only requires such presumptions to be circumscribed within reasonable boundaries, ensuring a fair balancing of the interests at stake and the rights of the defence.[129]

Looking at these requirements, could someone be fairly presumed to be "suspicious" only based on EFR processing? It seems difficult to argue in this direction. At the outset, it could be assumed that the use of such invasive technology may be proportionate in relation to most serious criminal offences and threats to national security. However, several issues would persist so as to the *fairness* of these operations. As argued above,[130] the scientific unsoundness of EFR and its

[126] CJEU, *Digital Rights*, para. 37.
[127] CJEU, *La Quadrature du Net*, para. 143 [emphasis added].
[128] CJEU, *La Quadrature du Net*, para. 188.
[129] ECtHR, 20 October 1998, *Salabiaku v. France*, Appl. No.10519/83, para. 28. More recently, see also ECtHR, 26 January 2016, *Iasir v. Belgium*, Appl. no. 21614/12, para. 30. In EU law, this approach was confirmed in the Directive on the presumption of innocence. Its Recital (22) indicates that the principle is not impinged by the use of presumptions, provided that these are "rebuttable", "used only where the rights of the defence are respected", and "confined within reasonable limits", also considering the proportionate use of means employed in relation to the aims pursued.
[130] Above, Sect. 4.

underlying technology makes the decisions of such software opaque and thus difficult to challenge for targeted individuals. If garnered datapoints – even where collected in preventive operations – were introduced in the proceedings, these could hardly be considered rebuttable by the defence,[131] also in light of an aura of objectiveness that often surrounds scientific evidence. Needless to say, this would irremediably impair the individual's rights of defence, her right to the equality of arms, to an effective remedy and the overall fairness of the proceeding.

Once again, similar procedural concerns are also supported in the data protection legislation, applicable to the preventive phase as well. Fairness as a basic tenet of data protection law prevents data controllers from taking any unjustified adverse or stigmatizing action towards the data subject based on the processing of its personal data. The right not to be fully subject to an automated decision represents another an important entitlement in this sense, as it ensures that EFR processing is surrounded by adequate safeguards, among which the right to obtain human intervention and – as added by Recital (38) of the Police Directive – the rights to express her point of view, to obtain an explanation for the decision or to challenge it. All in all, whether presumptions based on EFR processing were introduced at trial or taken as bases for preventive and investigative measures, similar safeguards are available to individuals to defend their presumption of innocence.

## 7 Conclusions

In this contribution preventive uses of EFR technologies in public places were examined. In light of recent developments suggesting an increasing use of such tools in the law enforcement context, it was considered appropriate to evaluate them in light of the European standards of fundamental rights protection. Specifically, EFR deployments were assessed against four fundamental rights, sharing a common rationale: the rights to privacy and data protection, the freedom of thought and – to some extent – the presumption of innocence.

Ostensibly, a certain degree of speculation could not be avoided in this preliminary assessment of EFR. Indeed, two levels of unpredictability are involved. On the one hand, the legal framework for regulating the use of AI in the EU is still underway and the future work of legal interpreters may further impact on its concrete application. On the other, specific instances of implementation of EFR technologies are still surrounded by many uncertainties and tailored assessments can only be supported by a substantial factual basis. These information gaps can only be tackled in future research.

All in all, the surveillance case law elaborated both by the ECtHR and the CJEU is still under development, but provides by now a comprehensive framework through which new technological advancements can be assessed. While it is acknowledged that such tools may have a beneficial impact on the efficiency of law enforcement activities, their use should also be critically evaluated in democratic societies. This implies that relevant actors should not only be able to determine when and how new technologies can be fairly deployed, but also which uses should simply be rejected in a democratic society. In the case of EFR, the latter seems to be the most obvious conclusion.

**Acknowledgement** This project was funded by the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie ITN EJD 'Law, Science and Technology Rights of Internet of Everything' grant agreement no. 814177.

## References

2021/0106(COD) Artificial Intelligence Act, Legislative Observatory. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en. Accessed 9 July 2021.

Ackerman S (2017) TSA screening program risks racial profiling amid shaky science – study. The Guardian. https://www.theguardian.com/us-news/2017/feb/08/tsa-screening-racial-religious-profiling-aclu-study. Accessed 3 July 2021.

Adam R, Tizzano A (2014) Manuale di Diritto dell'Unione Europea. Giappichelli Editore, Torino.

Albino V et al (2015) Smart Cities: Definitions, Dimensions, Performance and Initiatives. Journal of Urban Technology:1-19.

[131] On the issues brought about the use of AI system with regard to the defence rights, especially in adversarial systems, see Contissa, Lasagni (2020); Quattroccolo (2019).

Article 19 (2021) Emotional Entanglement: China's emotion recognition market and its implications for human rights. https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf. Accessed 22 June 2020.

Article 29 Data Protection Working Party (2012), Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN, WP 192, Brussels, 22 March 2012.

Balsamo A (2018) The Content of Fundamental Rights. In: Kostoris RE (ed) Handbook of European Criminal Procedure. Springer: 99-170, 114-117; Manes V, Caianiello M (2020) Manuale di Diritto Penale Europeo. Giappichelli: 249-251.

BBC News (2018) 2,000 wrongly matched with possible criminals at Champions League. https://www.bbc.com/news/uk-wales-south-west-wales-44007872. Accessed 11 July 2021.

Berle I (2020) Face Recognition Technology. Springer, Law, Governance and Technology Series 41.

Brayne S (2017) Big Data Surveillance: The Case of Policing. American Sociological Review 82(5):977-1008.

Brkan M (2018) The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core. European Constitutional Law Review 14:332-368.

Caianiello M (2019) Criminal Process faced with the Challenges of Scientific and Technological Development. European Journal of Crime, Criminal Law and Criminal Justice 27(4):267-291.

Caianiello M (2021), Dangerous Liaisons. Potentialities and risks deriving from the interaction between Artificial Intelligence and preventive justice. European Journal of Crime, Criminal Law and Criminal Justice 29(1):1-23.

Castelvecchi D (2020) Is Facial Recognition Too Biased to Be Let Loose? Nature 587, 347-349. https://www.nature.com/articles/d41586-020-03186-4. Accessed 28 June 2020.

Chen C et al (2018) Distinct Facial Expressions Represent Pain and Pleasure Across Cultures. Proceedings of the National Academy of Sciences of the United States of America 115(43):E10013–E10021. https://www.pnas.org/content/pnas/115/43/E10013.full.pdf. Accessed 2 July 2021.

Christofi A, Verdoodt V (2019) Exploring the essence of the right to data protection and smart cities. CiTiP Working Paper. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3483616. Accessed 2 July 2021.

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (2021) Guidelines on Facial Recognition, 6. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Accessed 8 July 2021.

Contissa G, Lasagni G (2020) When it is (also) Algorithms and AI that decide on Criminal Matters: In Search of an Effective Remedy. European Journal Of Crime, Criminal Law And Criminal Justice 28:280-304.

Crawford K (2021) Time to regulate AI that interprets human emotions. Nature 592(7853):167. https://www.nature.com/articles/d41586-021-00868-5. Accessed 11 July 2021.

De Hert P (2005) Balancing Security and Liberty within the European Human Rights Framework. A critical Regarding of Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11. Utrecht Law Review 1(1):68-96.

De Hert P, Malgieri G (2020) Article 8 ECHR Compliant and Foreseeable Surveillance: The ECtHR's expanded legality requirement copied by the CJEU. A Discussion of European Surveillance Case Law. Brussels Privacy Hub Working Paper 6(1):1-40.

EDPB-EDPS (2021) Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 3. https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf. Accessed 6 July 2021.

EDPS (2017) Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit.

European Union Agency for Fundamental Rights (2019) Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement. https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law. Accessed 6 July 2021.

European Parliament (2021) Artificial Intelligence in policing: safeguards needed against mass surveillance. Press Release. https://www.europarl.europa.eu/news/en/press-room/20210624IPR06917/artificial-intelligence-in-policing-safeguards-needed-against-mass-surveillance. Accessed: 30 June 2021.

Feldman Barrett L (2017) The theory of constructed emotion: an active inference account of interoception and categorization. Social Cognitive and Affective Neuroscience, 1–23.

Ferguson AG (2017) Big Data Surveillance: The Convergence of Big Data and Law Enforcement. In: Gray D and Henderson SE (eds) The Cambridge Handbook of Surveillance Law. Cambridge University Press.

Gallagher R, Jona L (2019) We Tested Europe's New Lie Detector for Travelers — and Immediately Triggered a False Positive. The Intercept. https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/. Accessed 8 July 2021.

Hadjimatheou K (2017) Surveillance Technologies, Wrongful Criminalisation, and the Presumption of Innocence. Philos. Technol. (2017) 30:39–54.

Heaven D (2020) Expression of Doubt. Nature 578:502-504.

Heilweil R (2020) Big tech companies back away from selling facial recognition to police. That's progress. The Vox. https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police. Accessed 11 July 2021.

Hildebrandt M (2010) Some Caveats on Profiling. In: Gutwirth S, Poullet Y, de Hert P (eds) Data Protection in a Profiled World. Springer.

Hogdson C (2019) AI lie detector developed for airport security. The Financial Times. https://www.ft.com/content/c9997e24-b211-11e9-bec9-fdcab53d6959. Accessed 8 July 2021.

iBorderCrtl (2016) The Project. https://www.iborderctrl.eu/The-project. Accessed 11 July 2021.

Ienca M, Malgieri G (2021) Mental Data Protection and the GDPR, 7-8. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3840403. Accessed 8 July 2021.

Information Commissioner's Office (ICO) (2021) The Use of Live Facial Recognition Technology by Law Enforcement in Public Places, 9. https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf. Accessed 5 July 2021.

Kindt EJ (2018) Having Yes, Using No? About the New Legal Regime for Biometric Data. Computer Law & Security Review 34(3):523-538.

Koops BJ, Newell BC, Timan T, Škorvánek I, Chokrevski T, Galič M (2017) A Typology of Privacy. U Pa J Int'l L 38(2): 483-575.

Korte A (2020) Facial-Recognition Technology Cannot Read Emotions, Scientists Say. American Association for the Advancement of Science. https://www.aaas.org/news/facial-recognition-technology-cannot-read-emotions-scientists-say. Accessed 8 July 2020.

Kostoris RE (2018) The Protection of Fundamental Rights. In Kostoris RE (ed) Handbook of European Criminal Procedure. Springer.

Kotsoglou KN, Oswald M (2020) The long arm of the algorithm? Automated Facial Recognition as evidence and trigger for police intervention. Forensic Science International: Synergy 2:86-69.

Kummitha RKR, Crutzen N (2017) How do we understand smart cities? An evolutionary perspective. Cities 67:43-52

Lasagni G (2021) La Falsa Confessione come Causa di Errori Giudiziari. In: Lupària Donati L (ed) L'Errore Giudiziario, 194-95. Giuffrè.

Liao S (2018) Chinese facial recognition system mistakes a face on a bus for a jaywalker. The Verge. https://www.theverge.com/2018/11/22/18107885/china-facial-recognition-mistaken-jaywalker. Accessed 11 July 2021.

Malgieri G, De Hert P (2017) European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but not Necessarily by Judges. In: Gray DC, Henderson S (eds), The Cambridge Handbook on Surveillance, New York: Cambridge University Press, 2017, 509-532.

Malgieri G, Ienca M (2021) The EU regulates AI but forgets to protect our mind. European Law Blog. https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/#more-7784. Accessed 7 July 2021.

Marat E, Sutton D (2021) Technological Solutions for Complex Problems: Emerging Electronic Surveillance Regimes in Eurasian Cities. Europe-Asia Studies 73(1):243-267.

McStay A (2018) The Right to Privacy in the Age of Emotional AI. https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/AndrewMcStayProfessor%20of%20Digital%20Life,%20BangorUniversityWalesUK.pdf. Accessed 2 July 2021.

Mc Stay A (2020) Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy. Big Data & Society January-June 2020:1-12.

Murgia M (2021) Emotion recognition: can AI detect human feelings from a face?. Financial Times. https://www.ft.com/content/c0b03d1d-f72f-48a8-b342-b4a926109452. Accessed 30 January 2022.

Neroni Rezende I (2020) Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective. New Journal of European Criminal Law 11(3):375-389.

Neroni Rezende I (2021) Predictive Policing: Safeguards for the Choice of Data and Automated Processing in the Preventive Context. In: Barona Vilar S (ed) Justicia Algorítmica y Neuroderecho: Una mirada multidisciplinaria. Tirada lo Banch, Valencia, pp 361-387.

Nussbaum MC (2001) Upheavels of Thought: The Intelligence of Emotions. Cambridge University Press.

O'Flaherty M (2020) Facial Recognition Technology and Fundamental Rights. European Data Protection Law Review 6(2):170-173, 170.

Ojanen T (2016) Making the essence of fundamental rights real: The court of justice of the European Union clarifies the structure of fundamental rights under the Charter. European Constitutional Law Review 12(2):318-329.

Papakostantinou V, De Hert P (2021) EU lawmaking in the Artificial Intelligent Age: Act-ification, GDPR Mimesis, and Regulatory Brutality. European Law Blog. https://europeanlawblog.eu/2021/07/08/eu-lawmaking-in-the-artificial-intelligent-age-act-ification-gdpr-mimesis-and-regulatory-brutality/#more-7788. Accessed 8 July 2021.

Peeters B (2020) Facial recognition at Brussels Airport: face down in the mud. CiTiP Blog. https://www.law.kuleuven.be/citip/blog/facial-recognition-at-brussels-airport-face-down-in-the-mud/. Accessed 11 July 2021.

Prosser WL (1984) Privacy [A legal analysis]. In: Schoeman F (ed) Philosophical Dimensions of Privacy. An Anthology. Cambridge University Press (original work published in 1960).

Quattroccolo S (2019) Equità del processo penale e *automated evidence* alla luce della Convezione europea dei diritti dell'uomo. Revista Ítalo-Española de Derecho Procesal 2:1-17.

Raab T (2019) Germany. Video surveillance and face recognition: Current developments. European Data Protection Law Review 5(4):544-547.

Rivers J (2006) Proportionality and variable intensity of review. Cambridge Law Journal 65(1):174-207.

Rouvroy A, Poullet Y (2009) The Right to Informational Self-Determination and the Value of Self-Developments: Reassessing the Importance of Privacy for Democracy. In Gutwirth S, Poullet Y, De Hert P, de Terwangne C, Nouwt S (eds), Reinventing Data Protection?. Dordrecht: Springer, pp. 45-76

Sánchez-Monedero J, Dencik L (2020) The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl. Information, Communication & Society. DOI: 10.1080/1369118X.2020.1792530.

Sayers D (2014) Article 48 (Criminal Law). In: Peers S, Hervey T, Kenner J, Ward A (eds) The Eu Charter of Fundamental Rights. A Commentary. Bloomsbury: 1305-1350

Schabas WA (2017) The European Convention of Human Rights. A Commentary. Oxford University Press.

Schoeman F (1984) Privacy. Philosophical dimensions of the literature. In: Schoeman F (ed) Philosophical Dimensions of Privacy. An Anthology. Cambridge University Press.

Schwartz O (2019) Don't look now: why you should be worried about machines reading your emotions. The Guardian. https://www.theguardian.com/technology/2019/mar/06/facial-recognition-software-emotional-science Accessed 3 July 2021.

Science Daily (2017) Emotions are cognitive, not innate, researchers conclude. https://www.sciencedaily.com/releases/2017/02/170215121100.htm. Accessed 12 July 2021.

Sedenberg E, Chuang J (2017) Smile for the Camera: Privacy and Policy Implications of Emotion AI. http://arxiv.org/abs/1709.00396. Accessed 3 July 2021.

Thomas D (2018) The Cameras that Know if You're Happy – or a Threat. BBC. https://www.bbc.com/news/business-44799239. Accessed 2 July 2021.

Tzanou M (2017) Data Protection as a Fundamental Right. In Tzanou (ed) The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance. Oxford: Hart Publishing.

US Government Accountability Office (2013) Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities. https://www.gao.gov/products/gao-14-159. Accessed 3 July 2021.

Vaele M, Borgesius FZ (2021) Demystifying the Draft EU Artificial Intelligence Act. https://osf.io/preprints/socarxiv/38p5f. Accessed 8 July 2021.

van Brakel R, De Hert P (2011) Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. Cahiers Politiestudies 20:163-192.

Vervaele J A E (2005) Terrorism and Information Sharing between the Intelligence and Law Enforcement Communities in the US and the Netherlands: Emergency Criminal Law. Utrecht Law Review 1(1):1-27.

Wiewieorowski W (2019) Facial recognition: A solution in search of a problem? European Data Protection Supervisor. edps.europa.eu/node/5551. Accessed 2 July 2021.