

# The European Regulatory Frameworks for Facial Recognition. From the LED to the AI Act\*

Catherine Jasserand

(Senior Researcher - LawTech Research, Biometric Law Lab and Research Fellow – KU Leuven Centre for IT & IP Law (CiTiP))

**ABSTRACT** This chapter discusses the EU legal frameworks applicable to Facial Recognition Technologies (FRTs) deployed for law enforcement. It starts with a description of the concept of biometric data from a data protection perspective and presents the obligations linked to the processing of these data by law enforcement authorities for law enforcement purposes as resulting from the Law Enforcement Directive. Then, it delves into the new Artificial Intelligence Act (AI Act) rules on Remote Biometric Identification (RBI) systems, a generic category covering, among others, FRTs used for identification purposes. As a rule, the AI Act bans real-time RBI systems for law enforcement purposes in publicly accessible spaces, with three explicit exceptions, which must be implemented in national legislation to be used and comply with other rules. All other uses of the technologies, including the retrospective use of RBI systems for law enforcement purposes in publicly accessible spaces, fall in the category of high-risk systems. This chapter defines the terms of the discussion under the AI Act and explains the rules applicable to real-time and post RBI systems for law enforcement purposes.

**KEYWORDS:** Facial Recognition - LED - AI Act - Remote Biometric Identification Systems - Law Enforcement

**TABLE OF CONTENTS:** 1. Introduction. – 2. LED. – 2.1. Scope of application. – 2.2. Biometric data. – 2.2.1. Photographs, facial images, and biometric templates. – 2.3. Regime of sensitive data. – 2.4. Obligations linked to the processing of biometric data. – 2.4.1. Data Protection Impact Assessment (DPIA). – 2.4.2. Data Protection by Design and by Default. – 2.4.3. Other obligations. – 2.5. Experiments in various Member States. – 3. AI Act. – 3.1. Prohibition and exceptions. – 3.1.1. *Lex specialis* to Article 10 of the LED. – 3.1.2. Remote Biometric Identification (RBI) systems. – 3.1.3. Ban. – 3.1.3.1. Real-time versus post-event. – 3.1.3.2. Publicly accessible spaces. – 3.1.3.3. Biometric data and biometric identification. – 3.1.3.4. Law enforcement. – 3.1.4. Exceptions. – 3.1.4.1 The three cases. – 3.1.4.1.1. The targeted search for the victims of three serious crimes and the search for missing persons. – 3.1.4.1.2. Prevention of Imminent Threats to Life or Terrorist Attacks. – 3.1.4.1.3. Localisation and identification of suspects and perpetrators of listed serious crimes. – 3.1.4.2. Conditions and safeguards. – 3.2. Retrospective use. – 3.2.1. Justifications. – 3.2.2. Rules. – 3.2.2.1. RBI systems as high-risk systems. – 3.2.2.2. Retrospective use of RBI for law enforcement. – 4. Conclusions.

## 1. Introduction

Facial recognition technologies have been tested and are used by the police, be it in the context of criminal investigations on video feeds or in real-time during sports events or for other occasions in Europe and beyond.<sup>1</sup> Multiple reports, AI incidents databases, and newspaper articles describe these instances.<sup>2</sup>

In the European Union, until the adoption

of the Artificial Intelligence Act, facial recognition technologies were mainly regulated by data protection rules applicable to the processing of personal data. While the AI Act does not replace data protection rules,<sup>3</sup> it adds specific rules to the development, putting into the EU market, and use of AI technologies, which include biometric technologies.

Automated facial recognition technologies rely on artificial intelligence systems to detect the presence of faces in a frame (live or still video frame), extract facial features (i.e. measurable characteristics of a face) after enhancing image quality and transform them into machine-readable data to enable their

\* Article submitted to double-blind peer review.

<sup>1</sup> See contributions on national frameworks in this issue. See also C. Jasserand, *Experiments with Facial Recognition Technologies in Public Spaces: In Search of an EU Governance Framework*, in A. Zwitter and O. Gstrein (eds.), *Politics and Governance of Big Data and Artificial Intelligence*, Cheltenham, Edward Elgar Publishing, 2024.

<sup>2</sup> e.g. OECD, *AI Incidents and Hazards Monitor, AI Incident Database*; e.g. M. Ryder, *The Ryder Review*, commissioned by A. Lovelace, 2022; EDRi, *The Rise and Rise of Biometric Mass Surveillance in the EU*, 2021; T. Madiaga and H. Mildebrath, *Regulating Facial Recognition in the EU*, European Parliamentary Research Service, 2021; AI Now, *Regulating Biometrics: Global Approaches and Urgent Questions*, 2020; J. Zaugg, *Londres sous le diktat de la reconnaissance faciale*, in *Le Monde*, 12 January 2025.

<sup>3</sup> Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12 July 2024. See Art. 2(7) AI Act.

comparison for recognition purposes.<sup>4</sup> These data can be machine-readable facial images or biometric templates of the extracted features. Biometric templates are mathematical representations of the salient features used for biometric recognition.<sup>5</sup> Facial recognition covers identification and verification functionalities, which can be used for different applications. Beyond biometric recognition, FRTs can be used for other purposes, such as categorisation (classification of individuals based on shared characteristics) or emotion recognition based on facial traits.<sup>6</sup> However, technically speaking, when FRTs are used for those purposes, they do not perform biometric recognition.<sup>7</sup> The same technologies might therefore be used for different purposes. Yet this contribution does not address the legal rules applicable to FRTs when they are used for emotion recognition or biometric categorisation.

After this brief introduction, Section 2 explains the EU data protection rules, focusing on the scope of the Law Enforcement Directive, the legal definition of biometric data, their classification as sensitive data, and various obligations imposed on law enforcement authorities processing those data. Section 3 describes the rules of the AI Act, distinguishing those applicable to the real-time use of FRTs for law enforcement purposes in publicly accessible spaces from all the other uses.<sup>8</sup>

<sup>4</sup> For a detailed description of facial recognition, see A.K. Jain, A.A. Ross, K. Nandakumar and T. Swearingen (eds.), *Face Recognition in Introduction to Biometrics*, II ed., Switzerland, Springer Nature, 2025, 119-173.

<sup>5</sup> Biometric Recognition, Term 37.01.03, Note 3, International Standard ISO/IEC 2382-27:2022, Information Technology- Vocabulary – Part 37: Biometrics.

<sup>6</sup> Specific rules apply to biometric systems used for emotion recognition or biometric categorisation.

<sup>7</sup> *Ibid.* Some authors refer to facial processing applications to cover all the uses, from biometric recognition to face detection, facial emotion or facial attribute estimation. See I. Hupont, S. Tolan, H. Gunes and E. Gómez, *The Landscape of Facial Processing Applications in the Context of the European AI Act and the Development of Trustworthy Systems*, in *Nature Portfolio - Scientific Reports*, n. 12:10688, 2022.

<sup>8</sup> There are other topics that this contribution does not address, in particular, the prohibition of untargeted scraping of facial images for facial recognition purposes (Art. 5(1)(e) AI Act) that echoes Clearview AI's and PimEyes' practices and the regime of regulatory sandboxes (Arts. 57 to 59 AI Act) to discuss whether and under which conditions law enforcement authorities could experiment with real-time RBIs.

## 2. LED

The Law Enforcement Directive (LED) is the sibling Directive of the General Data Protection Regulation (GDPR) and provides specific rules for the processing of personal data by competent authorities for law enforcement purposes.<sup>9</sup> As a Directive, the LED is not directly applicable. However, this section will only detail the LED rules and not their national transposition.

### 2.1. Scope of application

The LED rules apply if two cumulative conditions are met. First, personal data are processed for law enforcement purposes, described as the 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'<sup>10</sup> The definition of these purposes is left at national level. Second, personal data are processed by competent authorities,<sup>11</sup> i.e. public authorities competent for the purposes covered by the LED and other bodies or entities entrusted by Member States to exercise public authority for the purposes covered by the LED.<sup>12</sup> Law enforcement authorities fall within the scope of the LED.<sup>13</sup>

### 2.2. Biometric data

Like the GDPR, the LED applies to the processing of personal data, defined as 'any information relating to an identified or identifiable natural person'.<sup>14</sup> This broad definition covers biometric data, which are specifically defined in Article 3(13) of the LED as:

Personal data resulting from specific

<sup>9</sup> Directive (EU) No. 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 L119, 4 May 2016, 89-131.

<sup>10</sup> Article 1(1) LED; see M. Brewczyńska, *Article 1. Subject Matter and Objectives*, in E. Kosta and F. Boehm (eds.), *The EU Law Enforcement Directive (LED): A Commentary*, Oxford, Oxford University Press, 2024, 51-65.

<sup>11</sup> Art. 2(1) LED.

<sup>12</sup> Art. 3(7)(a)-(b) LED.

<sup>13</sup> Rec. 12 LED.

<sup>14</sup> Art. 3(1) LED.

technical means relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.<sup>15</sup>

The notion of biometric data in the EU data protection instruments is a legal construction of what biometric data are from a data protection perspective. Therefore, it differs from the technical definition of biometric data outlined in the ISO/IEC standard on harmonised biometric vocabulary.<sup>16</sup>

From a data protection perspective, biometric data are defined according to four criteria.<sup>17</sup> First, as a pre-requisite, the data at stake must qualify as personal data, i.e. they relate to an identified or identifiable individual. Second, they result from specific technical means. Neither the LED nor the GDPR specifies what this specific technical processing is. However, while facial images are listed as an example of biometric data in Article 3(13) LED, photographs are not.<sup>18</sup> Third, the processed biometric characteristics are physical, physiological, or behavioural. Finally, the data are processed to *allow or confirm the unique identification* of a person. This last criterion relies on the functionality of biometric data or the purpose of their processing. However, what unique identification means remains unclear without clarification in the LED (or GDPR). What is problematic is that this criterion is used to classify biometric data as sensitive data.

According to Article 10 of the LED, and contrary to the other types of personal data listed in the category of sensitive data, biometric data are not considered sensitive due to their nature but rather due to their purpose of processing. Article 10 of the LED

applies to the processing of ‘biometric data for the purpose of uniquely identifying a natural person.’ Scholars are divided on the meaning of ‘unique identification’: some consider it should be understood as referring to the biometric identification functionality, excluding biometric data processed for verification purposes from the scope of sensitive data (unless they reveal other protected sensitive data, such as health condition).<sup>19</sup> Others argue that it is not the process (identification or verification) that uniquely links the data to an individual, but the data themselves have such characteristics that can be distinctively connected to an individual, whether those data are processed for identification or verification purposes. The processing of biometric data for either identification or verification purposes falls in the category of sensitive data.<sup>20</sup> The EDPB and the UK data protection authority, ICO, support this latter interpretation.<sup>21</sup> From a technical perspective, biometric technologies can never uniquely identify someone, as when they compare sets of data, they generate statistical results of similarities or differences between the data.<sup>22</sup>

### **2.2.1. Photographs, facial images, and biometric templates**

The EU data protection rules distinguish mere photographs from facial images. Photographs that are not processed for biometric recognition purposes, such as images extracted from CCTV cameras or social media, are not considered biometric data.<sup>23</sup> By contrast, when those images go through technical processing to perform biometric recognition, they fall under the

<sup>15</sup> Defined identically in Article 4(14) GDPR.

<sup>16</sup> Biometric Recognition, Term 37.01.03, Note 3, International Standard ISO/IEC 2382-27:2022, Information Technology- Vocabulary – Part 37: Biometrics.

<sup>17</sup> For a detailed analysis, see C. Jasserand, *Legal Nature of Biometric Data: From ‘Generic’ Personal Data to Sensitive Data*, in *European Data Protection Law Review*, vol. 2, Issue 3, 2016, 297-311 and C. Jasserand, *Biometric Data, Within and Beyond Data Protection*, in B. van der Sloot and S. van Schendel (eds.), *The Boundaries of Data*, Amsterdam University Press, 2024, 295-309.

<sup>18</sup> See recital 51 GDPR, ‘...photographs...are covered by the definition of biometric data only when they are processed through a specific technical means allowing the unique identification or authentication of a natural person’, although there is no equivalence in the LED.

<sup>19</sup> e.g. L. Tosoni and L.A. Bygrave, *Article 4(14) – Biometric Data*, in C. Kuner, L.A. Bygrave, and C. Docksey (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, Oxford University Press, 2020, 213-214.

<sup>20</sup> e.g. C. Jasserand, *Biometric Data, Within and Beyond Data Protection*, 295-309.

<sup>21</sup> Respectively, EDPB, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*, version 2.0, 26 April 2023, 10, para. 12, and ICO, *Biometric Data Guidance: Biometric Recognition*, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/>.

<sup>22</sup> EDPB, *Guidelines 05/2022*, 10, para. 11; A.K. Jain, A.A. Ross, K. Nandakumar, and T. Swearingen, *Introduction to Biometrics*, 1-50.

<sup>23</sup> As explained in Recital 51 GDPR; the original photographs are often referred to ‘raw data’ or ‘pre-processed’ data, i.e. untransformed data.

definition of biometric data. Those are referred to as ‘facial images’ in the definition of biometric data.<sup>24</sup> Thus, once the images are further enhanced to allow the extraction of facial features, the technically transformed images qualify as biometric data. But the distinction between ‘pre-processed’ photographs and transformed facial images is artificial, as photographs are a prerequisite to any facial recognition system. As pointed out by Kindt, photographs collected to be stored in a face database for facial recognition are not considered biometric data at the collection stage but become biometric data when they are further processed to perform facial recognition.<sup>25</sup> Other EU legislative instruments, such as those related to border control, also refer to facial images. However, in those instruments, facial images are considered biometric data not due to their technical transformation but rather to their quality and image resolution, which make them fit for automated biometric matching.<sup>26</sup> This approach is more logical than that in the EU data protection instruments.<sup>27</sup>

Biometric templates, which are mathematic representations of a face generated from facial images,<sup>28</sup> fall in the definition of biometric data.<sup>29</sup> Facial templates, rather than facial images, are usually stored in biometric databases for comparison purposes.

### 2.3. Regime of sensitive data

Biometric data processed to *uniquely identify* an individual fall in the category of sensitive data (officially called ‘special categories of data’). As explained above, biometric data fall into the category of sensitive data due to their purpose of processing rather than by their nature. Besides, if the data are processed for other purposes, they could still be considered sensitive if their processing reveals sensitive

information (such as an illness or a religious belief based on a photograph of someone wearing religious symbols).<sup>30</sup>

According to Article 10 of the LED, the processing of sensitive data is allowed if *strictly necessary* and accompanied by *appropriate safeguards*, and for one of the three situations: the processing is authorised by EU or national law, is strictly necessary to protect the vital interests of an individual (the data subject or a third-party),<sup>31</sup> or the processing relates to data that have been manifestly made public by the data subject. In Case C-205/21, the Court of Justice of the European Union (CJEU) interpreted the strict necessity requirement as ‘establishing strengthened conditions’ to process sensitive data lawfully<sup>32</sup> and assessed the strict necessity in light of the principles of purpose limitation, data minimisation, and lawfulness.<sup>33</sup> In its ‘Guidelines on the Use of Facial Recognition Technology in the area of Law Enforcement’, the European Data Protection Board (EDPB) viewed strict necessity as limited to what is absolutely necessary, limiting the margin of interpretation left to law enforcement authorities in assessing necessity.<sup>34</sup> The EDPB also emphasised that the ‘mere transposition’ of Article 10 of the LED into national law would not be sufficient as a legal basis to process biometric data through facial recognition systems.<sup>35</sup> As stated by the EDPB, national law must be ‘sufficiently clear in its terms to give individuals an adequate indication of conditions and circumstances’ in which law enforcement authorities are empowered to deploy FRTs and create ‘a biometric template of their face and compare it to police database.’<sup>36</sup>

Finally, concerning data manifestly made public by the data subjects, the EDPB introduced a meaningful distinction in its Guidelines. While photographs (such as those posted on social media) might have been

<sup>24</sup> Art. 3(13) LED.

<sup>25</sup> E. Kindt, *Having Yes, Using No? About the New Legal Regime for Biometric Data*, in *Computer Law & Security Review*, vol. 34, Issue 3, 2018, 530-532.

<sup>26</sup> e.g. Art. 2(1)(r) of Regulation (EU) No. 2024/1358 (Eurodac Recast Regulation), Art. 3(15) of Regulation No. 2018/1861 amending the Schengen Information System in the field of border checks.

<sup>27</sup> C. Jasserand, *Biometric Data, Within and Beyond Data Protection*, 295-309.

<sup>28</sup> e.g. A. Ross and A.K. Jain, *Biometrics, Overview*, in S.Z. Li and A.K. Jain (eds.), *Encyclopedia of Biometrics*, New York, Springer Nature, 2009, 168-172.

<sup>29</sup> EDPB, Guidelines 05/2022.

<sup>30</sup> Personal data revealing religious beliefs or data concerning health are also sensitive data; Art. 10 LED.

<sup>31</sup> According to Recital 37 LED, this legal ground can apply when there is no national or EU law that already authorises the processing of biometric data.

<sup>32</sup> Case C-205/21, *VS v Ministerstvo na vatreshnite raboti*, 26 January 2023 (ECLI:EU:C:2023:49), para. 117.

<sup>33</sup> *Ibid.*, para. 122; i.e. Arts. 4 and 8 of the LED.

<sup>34</sup> EDPB, Guidelines 05/2022, 21.

<sup>35</sup> *Ibid.*

<sup>36</sup> EDPB, Guidelines 05/2022, 19-20 and 44.

voluntarily disclosed by the data subjects themselves,<sup>37</sup> the transformation of these images into biometric data (facial images, templates) might not. Hence, as observed by the EDPB, ‘the fact that a photograph has been manifestly made public by the data subject does not entail that the related biometric data, which can be retrieved from the photograph by specific technical means, is considered as having been manifestly made public.’<sup>38</sup> There is a slim chance that an individual would voluntarily disclose their transformed facial images and biometric templates. Consequently, the processing of these data should either be based on a compelling interest to protect the vital interests of individuals (Article 10 (b) of the LED)<sup>39</sup> or on national or EU legislation specifically allowing the processing of biometric data for law enforcement purposes (Article 10 (a) of the LED). Thus, before the adoption of the AI Act and based on Article 10 of the LED, Member States could have allowed the processing of biometric data through real-time FRTs and other biometric technologies in their national legislation, provided they complied with the conditions outlined in Article 10 of the LED. However, as the EU co-legislators agreed to ban real-time RBI, except in three explicit cases, they introduced rules on the ban and exceptions as a *lex specialis* to Article 10 of the LED to prevent Member States from relying on Article 10 of the LED to adopt national legislation allowing such use.<sup>40</sup> In the section on the AI Act (section 3), the relationship between Article 10 of the LED and Article 5(1)(h) of the AI Act is further explained.

<sup>37</sup> Provided this can be established, as for instance, photographs of an individual could be published by third parties on social media.

<sup>38</sup> EDPB, Guidelines 05/2022, 21.

<sup>39</sup> This legal ground has not been the topic of interpretation; see C. Jasserand, *Article 10: Processing of Special Categories of Personal Data*, in E. Kosta and F. Boehm (eds.), *The EU Law Enforcement Directive (LED): A Commentary*, Oxford, Oxford University Press, 2024, 227-228.

<sup>40</sup> This issue was discussed during the first Artificial Intelligence Workshop organised by the European Association for Biometrics, 10 November 2021, <https://eab.org/events/program/277?ts=1737294528868>.

## **2.4. Obligations linked to the processing of biometric data**

### **2.4.1. Data Protection Impact Assessment (DPIA)**

Beyond finding the adequate legal basis, data controllers, such as law enforcement authorities deploying FRTs, must conduct a data protection impact assessment when the envisaged data processing is likely to result in a high risk to the rights and freedoms of individuals.<sup>41</sup> Although the EDPB did not provide any interpretation in the context of the LED, the guidance provided by the Article 29 Working Party (replaced by the EDPB) on the high-risk factors in the context of the GDPR can be used as a reference.<sup>42</sup> As a consequence, the processing of sensitive data alone is not sufficient to impose on law enforcement authorities the obligation to conduct a DPIA. Such processing must be associated with another factor, such as the use of new technologies (including CCTV or FRTs), systematic monitoring of publicly accessible areas on a large scale, or large-scale data processing.<sup>43</sup> Concerning the deployment of FRTs in public spaces for law enforcement, data controllers must conduct a DPIA before using the technologies and starting the processing, as more than two factors are present.

### **2.4.2. Data Protection by Design and by Default**

Data controllers must also comply with the obligation of data protection by design and default obligation.<sup>44</sup> Following that obligation, data controllers must adopt technical and organisational measures to implement the data protection principles of the LED. For the EDPB, this obligation implies that ‘when a LEA [law enforcement authority] intends to apply and use FRT[s] from external providers, it has to ensure, e.g. through the procurement

<sup>41</sup> Art. 27 LED.

<sup>42</sup> Art. 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is ‘Likely to Result in High-Risk’ for the Purposes of Regulation 2016/679*, WP248 rev.01, 2017, 9-11.

See as well, EDPB, *The List of Types of Personal Data Processing Operations, for which carrying out a Data Protection Impact Assessment is Required*, [hwww.edpb.europa.eu/sites/default/files/decisions/pl-dpia-list\\_monitor\\_polski.pdf](https://www.edpb.europa.eu/sites/default/files/decisions/pl-dpia-list_monitor_polski.pdf)

<sup>43</sup> *Ibid.*

<sup>44</sup> Art. 20 LED.

procedure, that only FRT[s] built upon the principles of data protection by design and by default are deployed.<sup>45</sup> The obligation also encompasses ensuring the security of the processing through compliance ‘with the relevant standards and implement[ation of] biometric template protection measures’<sup>46</sup> and accountability.<sup>47</sup>

### 2.4.3. Other obligations

Other obligations can be mentioned, such as the prohibition of generating decisions based solely on automated processing, including the processing of sensitive data, which would adversely affect concerned individuals.<sup>48</sup> Concerning the processing of sensitive data, an exception is possible only if ‘suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place.’<sup>49</sup> Such measures include the right to human intervention, such as human review of the decision (outcome of the system) or to obtain an explanation of the decision.<sup>50</sup>

### 2.5. Experiments in various Member States

Before the adoption of the AI Act, the rules mainly applicable to the deployment of FRTs in public spaces were the data protection rules. While the rules of the LED apply to the processing of personal data by law enforcement authorities (or on their behalf) for law enforcement purposes, the rules of the GDPR apply to other processing purposes by law enforcement authorities. For instance, in the context of the experiment conducted in Nice, the French data protection, the CNIL, highlighted that the FRT deployment for experimenting purposes by the public authorities was subject to the GDPR rules.<sup>51</sup> But if this experiment would have led to arrests or used for law enforcement purposes (i.e. prevention and detection of criminal offences, investigations, prosecution, or

safeguarding against threats to public security), they would have been subject to the LED rules.<sup>52</sup>

Many police forces trialled live FRTs in public spaces (including train stations, streets, outdoor festivals, football fields, etc.) for security and policing purposes.<sup>53</sup> In France, the municipal police and the City of Nice tested the technologies during the Carnival edition of 2019; in Germany, the federal police tested FRT at a train station in Berlin, among others.<sup>54</sup> Experiments were also conducted by the police forces in the UK. No less than ten UK police forces trialled FRTs at different public events.<sup>55</sup> Some of these trials led to arrests.<sup>56</sup> As observed by the then Biometrics Commissioner in the UK, these experiments were ‘hybrid’, combining trials with operational policing deployments.<sup>57</sup>

The different experiments were conducted without a clear legal framework. In the UK, for instance, the legal basis for processing biometric data was Section 35 DPA 2018, a mere ‘transposition’ of Article 10 of the LED on sensitive data processing.<sup>58</sup> Yet, as highlighted by the EDPB, such generally worded transposition lacked precision and foreseeability to be used as a legal basis for the processing of biometric data through FRTs.<sup>59</sup> Concerning the experiment conducted

<sup>52</sup> *Ibid.*

<sup>53</sup> e.g. EDRI, *The Rise and Rise of Biometric Mass Surveillance in the EU*, 2021.

<sup>54</sup> e.g. F. Ragazzi et al., *Biometric and Behavioural Mass Surveillance in EU Member States*, Report for the Greens/EFA; TELEFI project, *Summary Report of the project ‘Towards the European Level Exchange of Facial Images,’* version 1.0, 2021.

<sup>55</sup> According to the civil rights organisation Big Brother Watch, see Big Brother Watch, *Map: UK Facial Recognition in Detail*, <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/#facial-recognition-uk>.

<sup>56</sup> D. Hussain, *Met Police Make First Arrest Using Facial Recognition Technology as They Hold Woman, 35, Over Alleged Serious Assault on Emergency Service Worker* (Daily Mail Online, 28 February 2020), [www.dailymail.co.uk/news/article-8055001/Met-Police-make-arrest-using-facial-recognition-technology.html](http://www.dailymail.co.uk/news/article-8055001/Met-Police-make-arrest-using-facial-recognition-technology.html).

<sup>57</sup> House of Commons Science and Technology Committee, *Oral Evidence, Work of the Biometrics Commissioner and the Forensic Science Regulator*, HC 1970, 19 March 2019, Q53 <https://committees.parliament.uk/oralevidence/9142/pdf>. For more information on police’s trials with FRTs in the UK, see C. Jasserand, *Experiments with Facial Recognition in Public Spaces*, 315.

<sup>58</sup> When the experiments were conducted in the UK, the UK was still part of the EU and had implemented the data protection frameworks into its national laws.

<sup>59</sup> EDPB, Guidelines 05/2022.

<sup>45</sup> EDPB, Guidelines 05/2022, 27.

<sup>46</sup> *Ibid.*

<sup>47</sup> Art. 4(4) LED.

<sup>48</sup> Art. 11 (2) LED.

<sup>49</sup> Art. 11 (2) LED; see Article 29 Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, WP251 rev.01, 2018.

<sup>50</sup> Rec. 38 LED.

<sup>51</sup> Public Sénat, *Test de reconnaissance faciale à Nice : précisions de la CNIL*, 19 February 2019, [www.publicsenat.fr/actualites/politique/test-de-reconnaissance-faciale-a-nice-precisions-de-la-cnil-138122](http://www.publicsenat.fr/actualites/politique/test-de-reconnaissance-faciale-a-nice-precisions-de-la-cnil-138122).

in Nice, as reminded by the CNIL, the processing of biometric data was based on the explicit consent of the participants. No other legal basis was available for law enforcement authorities to deploy live FRTs for law enforcement purposes.<sup>60</sup>

The next section focuses on the rules introduced by the AI Act.

### 3. AI Act

In December 2023, after more than two and a half years of negotiations, the EU institutions agreed on the AI Act.<sup>61</sup> The text was officially adopted on 13 June 2024.<sup>62</sup> The AI Act follows a risk-based approach depending on the risks that AI systems may pose to fundamental rights, health, and safety. Those identified as posing unacceptable risks to fundamental rights are prohibited, while those posing a ‘significant risk’ to fundamental rights as well as health and safety are classified as high-risk systems. Finally, AI systems posing limited risks, i.e. transparency risks, are subject to transparency rules. One should observe that while most of the provisions of the AI Act are adopted based on Article 114 TFEU (internal market), rules on the restrictions of the use of RBIs for law enforcement purposes are based on Article 16 TFEU (data protection).<sup>63</sup>

A part of the negotiations revolved around the controversial use of RBI in publicly accessible areas, whether their use, in particular for law enforcement purposes,

should fall under the unacceptable practices or whether they should be considered high-risk. The European Parliament supported an almost complete ban on RBI use by public and private entities, whether in real-time or post-event, with the exception of their retrospective use by law enforcement authorities ‘for the targeted search connected to a specific criminal offence’ under specific conditions.<sup>64</sup> The European Commission and the Council were in favour of a partial ban for law enforcement use in real-time and publicly accessible spaces except in three cases.<sup>65</sup> In all the other situations, RBIs were considered high-risk systems. The adopted text has narrowed down the rules proposed by the European Commission. However, it kept the distinction between real-time and post deployments of RBI systems in publicly accessible spaces and for law enforcement purposes. This section mainly refers to the generic category of RBI but also mentions FRTs as an application of RBI systems. As the European Commission published its Guidelines on the prohibited AI practices during the drafting of this contribution, references to these guidelines are added. However, as acknowledged by the European Commission, these interpretative guidelines are non-binding. Ultimately, it will be up to the CJEU to interpret the provisions of the AI Act.<sup>66</sup>

#### 3.1. Prohibition and exceptions

Article 5(1)(h) of the AI Act prohibits ‘the use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the objectives’ outlined in Article 5(1)(h)(i)-(iii) of the AI Act.

Conceived as exceptions to the ban, these objectives are the following ones:

<sup>60</sup> As at the time of the experiment, no specific law (a decree adopted by the French Council of State) had been adopted to allow police authorities to deploy live FRTs in public spaces, in application of Article 10 of the LED. For further info, see C. Jasserand, *Experiments with Facial Recognition in Public Spaces*.

<sup>61</sup> European Parliament, *Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI*, 9 December 2023, [www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai](http://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai).

<sup>62</sup> Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12 July 2024.

<sup>63</sup> Rec. 3 AI Act. Article 16 TFEU is also the legal basis for the rules on the use of biometric categorisation for law enforcement purposes and the risk assessments of individuals for law enforcement purposes, while the other prohibitions listed in Art 5 AI Act are based on Article 114 TFEU. See Point (10) of the EC Guidelines.

<sup>64</sup> European Parliament, *Amendments adopted by the European Parliament on 14 June 2023 on the 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*, TA-9-2023-0236.

<sup>65</sup> Council, *General Approach on the Artificial Intelligence*, 6 December 2022, 14954/22. European Commission, 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, 21 April 2021.

<sup>66</sup> See Point (5) of the EC Guidelines.

(a) The targeted search for victims of three specific crimes (abduction, trafficking in human beings, and sexual exploitation) and the search for missing persons (Art. 5(1)(h)(i)).

(b) The prevention of threats to persons' life or public safety or a terrorist attack (Art. 5(1)(h)(ii)).

(c) The localisation or identification of suspects of certain serious crimes as listed in Annex II to the AI Act (Article 5(1)(h)(iii)).

In addition, RBI systems must be allowed by national law to be deployed in real-time and comply with the conditions and safeguards described in Article 5(2) to (7) of the AI Act.

Before explaining the prohibition and exceptions to the prohibition, the relationship between Article 5(1)(h) and the LED is addressed.

### 3.1.1. *Lex specialis to Article 10 of the LED*

As specified in Recital 38 of the AI Act, the rules that prohibit real-time RBI and the exceptions are conceived as *lex specialis* to Article 10 of the LED, which regulates the processing of sensitive data (including biometric data) for law enforcement by competent authorities.<sup>67</sup> To ban real-time RBI and provide exceptions to the ban, the EU co-legislators had to adopt special rules derogating from Article 10 of the LED. However, Article 10 of the LED remains the legal basis in the other situations, which include the processing of biometric data in the context of retrospective use of RBI for law enforcement purposes (e.g. *a posteriori* analysis of images extracted from CCTV for a criminal investigation).<sup>68</sup>

Article 5(1)(h)(i)-(iii) does not provide the legal basis to process biometric data for any of the exceptions allowed but a framework of rules, as Member States are free to regulate or not these exceptions in their national law.<sup>69</sup> Should they decide to allow the exceptions, they can authorise all of them or a few. In any case, they must authorise them through a national law that complies with the conditions and safeguards of Article 5(2)-(7) of the AI Act. The rules established in Article 5(1)(h)(i)-(iii) and Article 5(2)-(7) do not replace Article 10 of the LED, as the

processing of biometric data linked to real-time RBI for law enforcement purposes must still comply with the conditions set out in Article 10 of the LED, i.e. the strict necessity of the processing, the existence of appropriate safeguards, and the existence of a legal basis.<sup>70</sup>

### 3.1.2. *Remote Biometric Identification (RBI) systems*

The AI Act does not regulate FRT per se but the generic technology of RBI, which covers different applications, such as FRT among others.<sup>71</sup> RBI systems are defined as:

AI system[s] for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database. (Art. 3(41) AI Act).

This definition is linked to biometric identification defined as:

automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database. (Art. 3(35) AI Act).

The concept of RBI only covers the identification functionality of biometric recognition systems. Systems used for verification purposes, such as access control, are expressly excluded from the scope of RBIs.<sup>72</sup> Some scholars criticised the definition of RBIs because they viewed it as being modelled after the functioning of FRTs.<sup>73</sup>

<sup>70</sup> Rec. 94 AI Act.

<sup>71</sup> European Commission, *Staff Working Document, Impact Assessment Accompanying the 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*, 2021, SWD (2021) 84 final, 18. Other examples of RBI systems are voice or gait recognition systems, among others, see Impact Assessment of the Regulation on Artificial Intelligence, 21 April 2021, SWD (2021) 84 final, 18.

<sup>72</sup> Rec. 17 and Annex III, 1(a) AI Act. However, it is not clear if biometric systems used for identity control, while this constitutes a verification process, are excluded from the scope of RBI.

<sup>73</sup> In relation to voice biometric technologies, Hutiri explained the impossibility to distinguish identification and verification functionalities, see W. Hutiri, *The Proposed EU AI Act and the Case of Biometrics*, in *Mozilla*, 2022, <https://foundation.mozilla.org/en/blog/>

<sup>67</sup> As described in sub-section 2.2; Rec. 38 AI Act.

<sup>68</sup> Rec. 39 AI Act.

<sup>69</sup> Rec. 37 and Art. 5(5) AI Act.

FRTs are, indeed, the typical example of RBI as they operate at a distance ('remotely'), without the active involvement (and awareness) of the persons to identify. Finally, the definition of RBI mentions a reference database against which the captured biometric data are compared. One could note that due to the prohibition of untargeted scraping of facial images through an AI tool to constitute or expand facial recognition databases,<sup>74</sup> the Clearview AI database and similar databases could not be used as a reference database for RBI.<sup>75</sup>

### **3.1.3. Ban**

As a general rule, article 5(1)(h) bans the use of RBIs in real-time, in publicly accessible spaces, and for the purposes of law enforcement. The AI defines the different terms, although not with precision, as explained below. The Guidelines of the European Commission provide some clarifications.

#### **3.1.3.1. Real-time versus post-event**

The rules applicable to RBIs distinguish real-time (i.e. live) from post (i.e. retrospective) use of the technologies. In the AI Act, 'real-time' means that the different technical steps, from the capture of the biometric data to the feature extraction, template generation, and comparison, happen all at the same time or almost simultaneously, which can include 'limited short delays.'<sup>76</sup> But the AI Act does not provide any clues on the interpretation of 'limited short delay.' Is it a question of (nano) seconds, minutes, or more? This is problematic as there is no scientific consensus on what 'real time' means in the context of biometric recognition. Technical experts usually refer to 'image processing speed' or 'frame per second'(fps) to assess the performance of a system.<sup>77</sup> Besides, post RBI systems covers all the other situations as they are defined as 'remote biometric identification system[s] other than real-time remote biometric identification system[s].'<sup>78</sup> Recital

17 specifies that in the context of post RBI, the data on which identification is performed 'ha[ve] already been captured and the comparison and identification occur only after a significant delay.' In its Guidelines, the European Commission views the difference between 'real-time' and 'post' event as being temporal and specifies that 'a delay is significant at least when the person is likely to have left the place where the biometric data was taken.'<sup>79</sup> Although real-time cannot be defined from a technical perspective, the criterion chosen by the European Commission may raise interpretative issues, especially if the technologies are used during an event that lasts (e.g. a festival, a demonstration). Alternatively, the distinction between real-time and post event could be linked to the storage (or lack thereof) of the data used for comparison purposes. The cases where biometric data are stored for comparison purposes (e.g. recorded video feeds) could be considered 'post' deployment, while the cases where biometric data are compared on the fly, i.e. without being stored, could be viewed as 'real-time'.<sup>80</sup>

#### **3.1.3.2. Publicly accessible spaces**

Following Article 3(44) of the AI Act, publicly accessible spaces are spaces accessible to an undetermined number of persons, independently of who owns them (they can be owned by public or private parties), the activities for which the space is used (no requirement to use the spaces for public services) or access fees. These spaces include shops, restaurants, banks, doctors' offices, hotels, swimming pools, transport stations, airports, cinemas, conference halls, parks, forests, public roads, and many more.<sup>81</sup>

#### **3.1.3.3. Biometric data and biometric identification**

The AI Act provides a new definition of biometric data, which is based on the definition introduced in the EU data protection frameworks while scraping the functionality purpose of biometric data (i.e. *to allow or to confirm the unique identification*). Art. 3(34)

the-proposed-eu-ai-act-and-the-case-of-biometrics.

<sup>74</sup> Art. 5(1)(e) AI Act.

<sup>75</sup> But the use of such database would also not be allowed under the GDPR and LED rules.

<sup>76</sup> Art. 3(42) AI Act.

<sup>77</sup> e.g. A. Vina, *What is FPS? A Computer Vision Guide*, in *Roboflow*, 2024, <https://blog.roboflow.com/what-is-fps>.

<sup>78</sup> Art. 3(43) AI Act.

<sup>79</sup> See Point (310) of the EC Guidelines.

<sup>80</sup> This distinction based on storage or absence of storage of biometric data results from discussions with technical experts.

<sup>81</sup> Rec. 19 AI Act; prisons and border control areas are excluded as well as online spaces, see Points (315) and (317) of the EC Guidelines.

of the AI Act defines biometric data

as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data.

While Recital 14 acknowledges that the concept of biometric data, as defined in the AI Act, should be interpreted *in light of* the definition provided in the EU data protection instruments, it also explains that the concept of biometric data in the AI Act is not only relevant for verification or identification purposes but also for emotion recognition and biometric categorisation. As already explained, the GDPR and LED definitions of biometric data exclude from their scope ‘biometric data’ that are not processed to single out someone, i.e. those that are processed for either biometric categorisation or emotion recognition. As a result, two regulatory definitions of biometric data coexist: a more restrictive one, based on functionality in the data protection instruments, and a more inclusive one in the AI Act. In the context of RBI deployments, the distinction is not very relevant as biometric data in that context are precisely processed to identify someone, and more specifically for biometric identification purposes.<sup>82</sup> However, having two different definitions will be problematic in the context of biometric categorisation and emotion recognition. But this distinction goes beyond the scope of this paper.<sup>83</sup>

### 3.1.3.4. Law enforcement

In the context of Article 5(1)(h) of the AI Act, law enforcement refers to the ‘activities carried out by law enforcement authorities or on their behalf for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security.’ These activities are those described in Article 1 of

the LED and defined at national level.<sup>84</sup> Law enforcement authorities are defined identically to the national competent authorities in the LED, i.e. law enforcement authorities themselves (which include police, criminal justice authorities) and bodies or authorities entrusted by national legislation to exercise public authority and prerogatives of law enforcement authorities.

The rationale behind the prohibition is linked to the ‘intrusive nature’ of RBIs that impact the right to privacy of ‘a large part of the population’ through ‘the feeling of constant surveillance,’ and their chilling effect on other fundamental rights and freedoms, in particular the freedom of assembly.<sup>85</sup> Due to their interference with fundamental rights, real-time RBIs are, in principle, not allowed. Consequently, the police use of real-time FRTs to identify a shoplifter,<sup>86</sup> during a football game for security purposes (to detect potential troublemakers),<sup>87</sup> in the streets for crime prevention,<sup>88</sup> in a residential neighbourhood to identify suspects of burglaries,<sup>89</sup> to identify vulnerable persons (including due to mental health issues),<sup>90</sup> or persons of interest for police intelligence information<sup>91</sup> is prohibited under the EU AI Act. However, the co-legislators have

<sup>84</sup> Article 3(46) LED.

<sup>85</sup> As emphasised in Rec. 32 AI Act. See also EDPB’s Guidelines 05/2022, 6 and 13. FRA, *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*, 2019, 29-30.

<sup>86</sup> e.g. Point (328) of the EC Guidelines, [www.twenteinsite.nl/fc-twente-nieuws/gezichtsherkenning-in-stadions-goed-tegen-discriminatie-of-gaat-het-te-ver](http://www.twenteinsite.nl/fc-twente-nieuws/gezichtsherkenning-in-stadions-goed-tegen-discriminatie-of-gaat-het-te-ver).

<sup>87</sup> e.g. Flemming, *Gezichtsherkenning in Stadions: Goed tegen Discriminatie of Gaat het te ver?* [Facial Recognition in Stadiums: OK against discrimination or is it going too far?], in *FC Twente News*, 2022. [www.twenteinsite.nl/fc-twente-nieuws/gezichtsherkenning-in-stadions-goed-tegen-discriminatie-of-gaat-het-te-ver](http://www.twenteinsite.nl/fc-twente-nieuws/gezichtsherkenning-in-stadions-goed-tegen-discriminatie-of-gaat-het-te-ver); See Section 10.8, Examples of use in the EC Guidelines, 132-133; while the detection of emotions would not be prohibited, the identification of those troublemakers with RBIs by the police would, see example on pages 133-134.

<sup>88</sup> Point (360) and example on p.133 in the EC Guidelines.

<sup>89</sup> Section 10.8, example in the EC Guidelines, 133.

<sup>90</sup> As it was the case in the UK in 2017 during a commemoration; see M. Townsend, *Police to Use Facial-Recognition Cameras at Cenotaph Service*, the Guardian, 2017, [www.theguardian.com/technology/2017/nov/12/metropolitan-police-to-use-facial-recognition-technology-remembrance-sunday-cenotaph](http://www.theguardian.com/technology/2017/nov/12/metropolitan-police-to-use-facial-recognition-technology-remembrance-sunday-cenotaph). See Section 10.8, examples of use in the EC Guidelines, 132-133.

<sup>91</sup> *Ibid.*

<sup>82</sup> Art. 3(35) AI Act.

<sup>83</sup> For more information on the fragmented EU regulatory approach to the concept of ‘biometric data’, see the work of the Biometric Law Lab, and in particular, B. Sumer *et al.*, *AI Act’s Ripple Effect on Biometric Data: Harmonising or Fragmenting the Regulation of Biometric Data*, in K. Prifti *et al.* (eds.), *Digital Governance: Confronting the Challenges Posed by Artificial Intelligence*, The Hague, Springer, 2024, 165-181.

introduced three exceptions to the ban.<sup>92</sup>

### 3.1.4. Exceptions

Exceptions to the ban are justified based on the strictly necessary use of the technologies ‘to achieve a substantial public interest,’ which ‘outweighs the risks’ to fundamental rights. This substantial public interest corresponds to the three situations where real-time RBI can be permitted. Some scholars criticised this approach as the exceptions seem to result from a political will of the Member States (based on security risks) rather than on objective evidence of the need for these live technologies to be used in publicly accessible areas.<sup>93</sup> Indeed, neither the proposal for the AI Act nor the impact assessment accompanying it nor the adopted text provides evidence that real-time use of RBIs for these three objectives is the least restrictive solution that exists.<sup>94</sup>

#### 3.1.4.1 The three cases

Article 5(1)(h)(i) to (iii) outlines the three situations (‘objectives’) that can justify the real-time use of RBIs in publicly accessible spaces, provided the conditions and safeguards detailed in Article 5(2) to (7) are fulfilled. As already mentioned, Article 5(1)(h)(i)-(iii) does not constitute the legal basis for the real-time use of RBIs. Those exceptions need to be expressly allowed in national legislation.<sup>95</sup>

##### 3.1.4.1.1. The targeted search for the victims of three serious crimes and the search for missing persons

According to Article 5(1)(h)(i), RBI systems can be used in real-time for

the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons.

This exception does not cover potential victims but actual victims of the three serious crimes. Although not defined in the AI Act, victims are those who ‘ha[ve] suffered harm,

including physical, mental or emotional harm or economic loss which was directly caused by a criminal offence.<sup>96</sup> The technologies can also be used to search for missing persons, including children and adults.<sup>97</sup> As the exception does not apply to potential victims, the deployment of FRTs in real-time cannot be used to locate children who are at risk of being abducted (such as by a relative) and, more generally, for preventive purposes. As specified in the European Commission’s Guidelines, ‘in some Member States, the search for a missing person’ falls under administrative law. In these cases, if an RBI is deployed in real time, it would not be considered to fall under the exception of Article 5(1)(h)(i) as the purpose of use would not be for law enforcement.<sup>98</sup>

##### 3.1.4.1.2. Prevention of Imminent Threats to Life or Terrorist Attacks

According to Article 5(1)(h)(ii), RBI systems can be used in real-time for the

prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack

This exception covers two situations: the prevention of a threat to individuals’ life or physical safety and threats of terrorist attacks.

The first situation covers, for instance, hostage situations<sup>99</sup> or threats to the security of critical infrastructures with an imminent threat to persons’ life or safety.<sup>100</sup> The criteria of the threat, ‘specific, substantial and imminent’ suggest that immediate action must be taken to avoid the occurrence of a defined, real, and existing threat.

The second situation covers a threat of a terrorist attack, which needs to reach a certain threshold, be either *genuine* and *present* or *present* and *foreseeable*, to justify real-time

<sup>96</sup> Art. 2(1)(a)(i) of Directive 2012/29/EU.

<sup>97</sup> For voluntary disappearance of adults, specific rules exist at national level to trigger police investigation (such as the existence of circumstances that constitute a cause of concerns); see points (334) – (335) of the EC Guidelines.

<sup>98</sup> Point (336) of the EC Guidelines.

<sup>99</sup> See examples of emergency in the Second Additional Protocol to the Budapest Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (CETS No. 224).

<sup>100</sup> see Rec. 33 AI Act, as illustrated in Point (340) of the EC Guidelines.

<sup>92</sup> After several months of intensive political negotiations on that issue.

<sup>93</sup> e.g. C. Jasserand, *The Future AI Act and Facial Recognition Technologies in Public Spaces: Nice to Have or Strictly Necessary?*, in *European Data Protection Law Review*, vol. 9, n. 4, 2023, 430.

<sup>94</sup> *Ibid.*, 440-441.

<sup>95</sup> Art. 5(2) AI Act.

RBI. The level of terrorist threats is defined at national level because terrorism is mainly a national security issue,<sup>101</sup> while the characteristics of the threat derive from the CJEU case law on data retention and Passenger Name Record measures aimed at protecting national security.<sup>102</sup> Provided it is authorised by national law, this exception allows for the deployment of live FRTs as an investigative tool in the prevention phase of a terrorist attack.

### 3.1.4.1.3. Localisation and identification of suspects and perpetrators of listed serious crimes

Finally, according to Article 5(1)(h)(iii) live RBI use is allowed for

the localisation and identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member States concerned by a custodial sentence or a detention order for a maximum period of at least four years (Article 5(1)(h)(iii) AI Act)

If authorised by national law, live FRTs can be deployed to identify and locate a suspect or perpetrator of a criminal offence to conduct a criminal investigation, prosecute the suspect or perpetrator, or execute an existing sentence. The criminal offences are listed in Annex II of the AI Act, which are the most serious crimes for which a European Arrest Warrant (EAW) can be issued. However, the issuance of an EAW against a perpetrator or suspect of one of those crimes is not required to deploy the technologies.<sup>103</sup> Those crimes include terrorism, trafficking in human beings, sexual exploitation of children and child pornography, rape, murder, kidnapping, hostage taking, and environmental crime, among others.<sup>104</sup> Several of these criminal offences can be linked to terrorism.

If the exceptions are authorised at national level, in a case of human trafficking or child sexual exploitation,<sup>105</sup> live FRTs could be used to search for the victim of the crime (Article 5(1)(h)(i)) and to locate and identify the suspect or perpetrator of the crime (Article 5(1)(h)(iii)).<sup>106</sup>

### 3.1.4.2. Conditions and safeguards

Article 5(2) to (7) describes the rules that must be followed to use real-time RBI for the exceptions provided by Article 5(1)(h)(i) to (iii).

The first condition relates to the adoption of a national law that authorises the deployment of real-time RBI for all or some of the exceptions.<sup>107</sup> As noted, Member States are not obliged to allow any of the exceptions in their national laws.<sup>108</sup> But if they do, the national law must contain specific information about the procedure of authorisation by a judge or independent administrative authority,<sup>109</sup> the objectives pursued by the deployment,<sup>110</sup> the criminal offences for which real-time RBI is authorised to be deployed to locate or identify a suspect or perpetrator in case of the third exception,<sup>111</sup> and the competent authorities (e.g. police forces) allowed to use it.<sup>112</sup> Within 30 days of their adoption, the rules adopted by Member States must be notified to the European Commission.<sup>113</sup>

Second, the technologies can only be used to 'confirm the identity of a targeted individual.'<sup>114</sup> This implies that the competent authorities have received information about an individual. In the case of the first exception, that individual is either the victim of one of the three listed crimes or a missing person. In the case of the last exception, the individual is either the perpetrator or the suspect. Regarding the second exception, who can be a targeted individual in case of a threat to a

<sup>101</sup> But counterterrorism is also an EU 'internal security' issue due to the cross-border dimension of terrorism; see A Counter-Terrorism Agenda for the EU (COM(2020)) 795 final.

<sup>102</sup> Joined cases C-511/18, C-512/18, and 520/18, *La Quadrature du Net and Others*, judgment of 6 October 2020 (ECLI:EU:C:2020:791); case C-817/19, *Ligue des droits humains*, judgment of 21 June 2022 (ECLI:EU:C:2022:491)

<sup>103</sup> See also Point (354) of the EC Guidelines.

<sup>104</sup> Full list in Annex II of the AI Act.

<sup>105</sup> The third crime listed in Article 5(1)(h)(i) is abduction. While kidnapping is among the crimes that can trigger Article 5(1)(h)(iii), kidnapping and abductions are different crimes. In particular, kidnapping can involve force, while (child) abduction is often a specific criminal offence in national law.

<sup>106</sup> Point (356) of the EC Guidelines.

<sup>107</sup> Art. 5(2) and Art. 5(5) AI Act.

<sup>108</sup> Art. 5(5) AI Act.

<sup>109</sup> Art. 5(3) AI Act.

<sup>110</sup> Art. 5(5) AI Act.

<sup>111</sup> Art. 5(5) AI Act.

<sup>112</sup> Art. 5(3) AI Act.

<sup>113</sup> Art. 5(5) AI Act.

<sup>114</sup> Art. 5(2) AI Act.

terrorist attack where several individuals might be involved, and none of them might be considered a suspect?<sup>115</sup> This is a question that national laws allowing real-time RBI will have to answer, as these laws must be specific regarding the individuals against whom the technologies can be deployed.<sup>116</sup> Besides the purpose of use, the deployment of the technologies must be based on an assessment of the situation justifying the use against the consequences of the use on all the persons concerned.<sup>117</sup>

Third, except in case of emergency, the deployment of real-time RBI must be authorised a priori by a judge or independent administrative authorities.<sup>118</sup> The authorisation is delivered on ‘objective evidence or clear evidence’ that the use is proportionate and strictly necessary based on time, geographic and personal delimitation.<sup>119</sup> Such authorisation cannot be delivered if law enforcement authorities have not completed a fundamental rights impact assessment outlined in Article 27 of the AI Act and registered the system in the EU database according to Article 49 of the AI Act.<sup>120</sup>

Finally, no decision that would have an adverse effect on an individual with legal consequences can be taken solely on the output of the AI system. This obligation imposes a human decision, which should not be an automatic application of the result provided by the AI system.<sup>121</sup> The use of real-

time RBI must be documented and communicated to the relevant market and data protection authorities,<sup>122</sup> which write annual reports submitted to the European Commission.<sup>123</sup>

### **3.2. Retrospective use**

The AI Act only prohibits real-time RBI in publicly accessible spaces for law enforcement. All the other uses, as well as the development, placing on the market and putting into services of RBI systems fall in the category of high-risk systems defined in Article 6 of the AI Act. The other uses include real-time RBI for law enforcement purposes in spaces that are not publicly accessible (e.g. prisons) or online, real-time and post RBI for non-law enforcement purposes in publicly accessible spaces (such as the use of FRT for security purposes by a private company in a supermarket or the use of FRT in schools for security and school attendance), and post RBI for law enforcement purposes in publicly accessible spaces (e.g. facial identification based on recorded video feeds in the context of a criminal investigation). While the AI Act does not prohibit these RBI practices, they must still comply with other rules, in particular data protection rules and non-discrimination. Consequently, the use of live FRT in a supermarket to identify shoplifters will most likely not pass the test of necessity and proportionality.<sup>124</sup>

#### **3.2.1. Justifications**

Before the negotiations of the AI Act, several Member States had already adopted rules allowing the police retrospective use of FRTs in their national legislation.<sup>125</sup> This is the case in France. Since 2018, French police authorities have been able to perform retrospective facial recognition on a criminal record, called the TAJ (*Traitements des Antécédents Judiciaires*). The record contains photographs of suspects, victims, and missing persons. The recorded images must meet a certain quality standard, as they require

<sup>115</sup> In this sense, see also A. Gianni and S. Tas, *AI Act and the Prohibition of Real-Time Biometric Identification, Much Ado about Nothing?*, in *Verfassungsblog*, 10 December 2024; according to the European Commission, real-time RBI could be used to follow ‘terrorists on the move’ and not target one individual, based on Art. 5(1)(h)(ii), see Point (348) of the EC Guidelines.

<sup>116</sup> This exception could be challenging in the framework of criminal procedure law and criminal law.

<sup>117</sup> As a result of a risk assessment, based on Art. 5(2) AI Act.

<sup>118</sup> Art. 5(3) AI Act.

<sup>119</sup> Art. 5(2) AI Act.

<sup>120</sup> Art. 5(2) AI Act; it should be noted that law enforcement authorities themselves and not parties, entities, or persons acting on their behalf, must conduct FRIAs.

<sup>121</sup> On the retrospective use of FRTs by the police, see the cases of wrongful arrests of African American people in the USA. As reported by the American Civil Liberties Union, in Louisiana and Indiana, ‘police relied solely on an incorrect facial recognition search from Clearview AI’ to get an arrest warrant. [www.aclu.org/news/privacy-technology/police-say-a-simple-warning-will-prevent-face-recognition-wrongful-arrests-thats-just-not-true](http://www.aclu.org/news/privacy-technology/police-say-a-simple-warning-will-prevent-face-recognition-wrongful-arrests-thats-just-not-true).

<sup>122</sup> Art. 5(4) AI Act.

<sup>123</sup> Art. 5(6) AI Act.

<sup>124</sup> See Dutch data protection authority on the trial of FRT by a chain of supermarkets in the Netherlands. [www.edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition\\_en](http://www.edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_en).

<sup>125</sup> See TELEFI project, Summary Report, 70 *et seq.*, 2021.

specific technical characteristics to enable facial recognition.<sup>126</sup> According to the French Council of State, the use of retrospective FRT is ‘absolutely necessary’ considering the volume of images that the record contains (more than six million),<sup>127</sup> which would be an impossible task for police officers to review them manually.<sup>128</sup>

### 3.2.2. Rules

#### 3.2.2.1. RBI systems as high-risk systems

RBI systems that are not covered by the scope of Article 5(1)(h) and its three exceptions are subject to the obligations imposed on high-risk systems. These rules include pre- and post-market conformity assessments,<sup>129</sup> FRIAs for deployers that are public entities governed by public law (such as police authorities),<sup>130</sup> data governance,<sup>131</sup> record-keeping,<sup>132</sup> risk management systems,<sup>133</sup> technical documentation,<sup>134</sup> transparency obligations imposed on law enforcement authorities as deployers,<sup>135</sup> human oversight,<sup>136</sup> accuracy, robustness and cybersecurity.<sup>137</sup>

#### 3.2.2.2. Retrospective use of RBI for law enforcement

In addition to the rules above, retrospective use of RBI for law enforcement purposes is subject to specific rules. These rules are detailed in Article 26(10) of the AI Act.

First, deployers of the systems (e.g. law enforcement authorities) should obtain authorisation to use RBI from a judge or administrative authority before deployment or within 48 hours of use at latest (without the requirement of an emergency that would justify ex-post authorisation).<sup>138</sup> An exception applies if the system is used for ‘the initial

identification of a potential suspect based on objective and verifiable facts directly to the offence.’<sup>139</sup> In case the authorisation is rejected, any use of the technologies should be stopped, and the personal data already processed should be deleted.

Second, RBI systems can only be used retrospectively in a targeted way, i.e. ‘in link with a criminal procedure, criminal proceeding, a genuine and present or genuine and foreseeable threat of a criminal offence, or the search for a specific missing person.’<sup>140</sup> The obligation is worded differently than in the context of real-time RBI, as the retrospective use of RBI is not limited to ‘confirming the identity of a targeted individual.’<sup>141</sup> It needs to be targeted but not necessarily to an individual. No decision that would adversely affect an individual can be taken solely on the system’s output, i.e. without human review or intervention.

Third, each retrospective use of RBI must be documented, and annual reports must be submitted to market surveillance and data protection supervisory authorities. Last, Member States are not prevented from adopting more restrictive laws in compliance with EU law.<sup>142</sup>

## 4. Conclusions

The legal frameworks under which law enforcement authorities, mainly police forces, can deploy FRTs for law enforcement purposes are based on the data protection rules of the Law Enforcement Directive and the rules established in the AI Act. Other rules apply, such as non-discrimination rules, which have not been discussed as they were not the topic of this contribution.

While the LED rules govern the processing of biometric data and the obligations that law enforcement authorities must comply with, the AI Act provides a framework of rules for the real-time and the post use of Remote Biometric Identification systems, such as FRTs, for law enforcement purposes. First, the ban on the real-time use of RBIs for law enforcement in publicly accessible spaces with its three exceptions is conceived as *lex specialis* to Article 10 of the LED, which applies to the processing of sensitive data

<sup>126</sup> Article R40-26 of the French Criminal Procedure Code.

<sup>127</sup> According to the TELEFI Summary Report, 2021.

<sup>128</sup> Conseil d’Etat, decision no. 442364, 26 April 2022, para 5; this assessment of strict necessity of FRT based on the volume of images to review has been criticised by NGOs and scholars.

<sup>129</sup> Art. 43 AI Act.

<sup>130</sup> Art. 27 AI Act.

<sup>131</sup> Art. 10 AI Act.

<sup>132</sup> Art. 12 AI Act.

<sup>133</sup> Art. 9 AI Act.

<sup>134</sup> Art. 11 AI Act.

<sup>135</sup> Art. 26 AI Act.

<sup>136</sup> Art. 14 AI Act.

<sup>137</sup> Art. 15 AI Act.

<sup>138</sup> Contrary to the deployment real-time use of RBI for law enforcement, as specified in Art. 5(3) AI Act.

<sup>139</sup> Art. 26(10) AI Act.

<sup>140</sup> *Ibid.*

<sup>141</sup> As observed, this targeting can be challenging in the context of a threat of a terrorist attack.

<sup>142</sup> Art. 26(10) AI Act.

(including biometric data). Concerning the exceptions, i.e. the three cases for which real-time RBI is considered acceptable despite their impact on fundamental rights, the AI Act does not constitute the legal basis for law enforcement authorities to deploy the systems. Such authorisation must be granted at national level through a national law that must comply with different conditions and safeguards. If Member States decide to allow the exceptions, partially or fully, they will, most likely, adopt detailed provisions in their criminal law and criminal procedure law. Some of the conditions might be challenging, such as the use of live RBI to confirm the identity of a targeted individual in the context of prevention of a genuine threat to a terrorist attack. But Member States are also free not to allow any of the exceptions. In that case, law enforcement authorities would not be allowed to deploy live RBI systems in publicly accessible areas for any law enforcement purposes. In February 2025, the European Commission issued non-binding guidelines on the implementation of the prohibitions covered by Article 5 of the AI. These guidelines provide practical examples of application, including for the real-time use of RBI in publicly accessible spaces for law enforcement purposes.

Concerning the retrospective (post-event) use of RBI systems for law enforcement in publicly accessible spaces, the AI Act does not ban them, but it subjects their use to the obligations applicable to high-risk systems, with several additional rules. The AI Act does not provide the legal basis for the processing of biometric data linked to the retrospective use of RBI systems. The data protection rules subsist. For instance, if no national law allows the processing of biometric data, such as for the retrospective use of FRT in criminal investigations, law enforcement authorities will not be authorised to perform retrospective facial recognition on criminal files. Currently, several Member States authorise the retrospective use of FRTs (including France). As the AI Act introduces specific conditions for the retrospective use, existing national laws will likely need to be amended.

Finally, whether for live or retrospective purposes, the national regulations and deployments of FRTs and similar biometric technologies will be subject to scrutiny by data protection authorities, national courts, and the CJEU to assess their compliance with

fundamental rights.

