

# Facial Recognition Before the European Court of Human Rights\*

Francesca Palmioto  
(IE University, Madrid, Spain)

**ABSTRACT** This article holistically analyses the European Court of Human Rights (ECtHR) case law on Article 8 of the European Convention of Human Rights (ECHR) to show how the Court’s jurisprudence significantly delimits the use of facial recognition technology (FRT) by law enforcement authorities. Its core aim is to distil principles from established case law that can set normative guardrails for this technology. The original methodological approach lies in conceptualising FRT as an “Architecture of Surveillance” comprising a threefold interference with the rights enshrined in Article 8 of the ECHR. 1) The collection of facial images as input data, the creation of police databases containing facial images and the use of the automated identification match for law enforcement purposes. After reviewing the case law following this tripartite structure, the paper derives the following core principles from the ECtHR jurisprudence. The principle of extrema ratio, which posits that FRT can be only used as a measure of last resort; the principle of targeted suspicion, which requires the use of facial recognition to be grounded in concrete, verifiable facts linking an individual to a previously committed crime; and the principle of selective legitimacy, which delimits the use of FRT for identifying limited categories of data subjects, namely only suspects and convicted individuals of serious offences. Notably, these principles apply to both “real-time” and “post” remote uses of facial recognition.

**KEYWORDS:** Facial Recognition - Human Rights - Artificial Intelligence - ECHR - European Court of Human Rights

**TABLE OF CONTENTS:** 1. Introduction. – 2. The Architecture of Surveillance. – 2.1. The Technology. – 2.2. A Threefold Interference. – 3. The Collection of the Input Data. – 3.1. Data collection through video cameras and secret surveillance. – 3.2. Data collection through investigative operations. – 4. The Creation of the Database. – 4.1. Nature of data stored and collected. – 4.2. Duration of the retention period. – 5. The Use and Purpose of the Output. – 5.1. Investigations and pre-emptive surveillance. – 5.2. Evidence in legal proceedings. – 6. Conclusions.

## 1. Introduction.

Is Facial Recognition Technology (FRT) compatible with human rights? This question has attracted significant academic attention in recent years. Normative scholars have analysed the profound impact that FRT has on a wide range of fundamental rights, from privacy to non-discrimination, underscoring the fundamental shift that the use of FRT, as a tool of mass surveillance, entails for democratic systems.<sup>1</sup> Beyond the impact on

the right to privacy, scholarly work also points to the chilling effects of FRT on other protected rights, particularly on the right to freedom of expression,<sup>2</sup> and the risks of discrimination and inaccuracy of this technology.<sup>3</sup> Some scholars have argued more radically that FRT is inherently incompatible with the human rights system and democracy, calling for regulatory interventions, moratoriums and legal bans.<sup>4</sup>

\* Article submitted to double-blind peer review.

<sup>1</sup> See among many others M. Zalnieriute and R. Matulionyte (eds.), *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge, Cambridge University Press, 2024; D. Dushi, *The Use of Facial Recognition Technology in EU Law Enforcement: Fundamental Rights Implications*, in *Global Campus of Human Rights*, 5, <http://doi.org/20.500.11825/1625>; M. O’Flaherty, *Facial Recognition Technology and Fundamental Rights Opinions*, in *European Data Protection Law Review*, vol. 6, 2020, 170; K. Kouroupis, *Facial Recognition: A Challenge for Europe or a Threat to Human Rights?*, in *European Journal of Privacy Law & Technologies*, vol. 2021, 2021, 142; N. Menéndez González, *Development or Dystopia?: An Introduction to the Accountability Challenges of Data Processing by Facial Recognition Technology*, in *Communications law*, vol. 26, 2021, 81; These concerns have been widely echoed by civil society organisations through significant campaigns advocating for prohibiting this technology. See, among many others, the coalition

#protectnotsurveil.

<sup>2</sup> M. Zalnieriute, *Facial Recognition Surveillance and Public Space: Protecting Protest Movements*, in *International Review of Law, Computers & Technology*, vol. 39, n. 1, 2025, 116.

<sup>3</sup> D. Leslie, *Understanding Bias in Facial Recognition Technologies*, Alan Turing Institute, 2020, [doi.org/10.5281/zenodo.4050457](https://doi.org/10.5281/zenodo.4050457); M. O’Flaherty, *Facial Recognition Technology and Fundamental Rights Opinions*, cit., 170.

<sup>4</sup> D. Murray, *Facial Recognition and the End of Human Rights as We Know Them?*, in *Netherlands Quarterly of Human Rights*, vol. 42, 2024, 145; E. Selinger and W. Hartzog, *The Inconsistency of Facial Surveillance Consentability*, in *Loyola Law Review* vol. 66, n. 1, 2020, 33; W. Hartzog and E. Selinger, *Surveillance as Loss of Obscurity*, in *Washington and Lee Law Review*, vol. 72, n. 3, 2015, 1343; L. Barrett, *Ban Facial Recognition Technologies for Children - And for Everyone Else*, in *Boston University Journal of Science and Technology Law*, vol. 26, n. 2, 2020, 223; K. Crawford, *Halt the Use of Facial-Recognition*

From a doctrinal perspective, legal scholars have investigated the use of FRT under the EU data protection framework and national criminal procedural law, showing potential gaps in protection under existing legal frameworks.<sup>5</sup> More recently, a growing number of articles and commentaries are focusing attention on the complex regulation of facial recognition under the EU Artificial Intelligence Act (hereafter AI Act).<sup>6</sup>

However, the case law of the European Court of Human Rights (hereafter ECtHR or “Court”) has attracted considerably less attention from a doctrinal perspective. Besides some case notes on *Glukhin v. Russia*,<sup>7</sup> the first judgment from an international court on facial recognition, a comprehensive analysis of the Court’s case law is still lacking. As this article shows, in addition to *Glukhin v. Russia*, the Court’s surveillance jurisprudence and data retention case law offer significant limitations to the concrete use of this advanced technology. This contribution, therefore, analyses the use of FRT by law enforcement authorities, applying the

underutilised doctrinal lens to the ECtHR case law.

The article seeks to investigate how the Court’s jurisprudence shapes the legitimate bounds of facial recognition and asks, in particular, whether and under which conditions law enforcement authorities can use this advanced technology for countering crimes. By reviewing the extensive case law on surveillance, police practices and data retention, the article reviews comparable interferences under Article 8 of the European Convention of Human Rights (hereafter ECHR or Convention), their justification under the “necessary in a democratic society” sub-test and apply them to the context of facial identification through AI systems. In doing so, it sheds light on the critical case law that significantly delimits the use of police activities gathering personal data for automated facial identification.

The article argues that the right to privacy, as interpreted by the ECtHR, provides significant guardrails to the use of FRT by law enforcement authorities. More specifically, the limits on the collection of facial images of individuals ought to be identified, the prohibition of indiscriminate police databases, and the respect for the principle of reasonable suspicion when authorising the deployment of facial identification significantly reduce the scope and purpose of legitimate uses of this technology.

To support this claim, the article first introduces the conceptual framework informing the case law review. After providing a brief overview of the technical functioning of FRT, it illustrates the “Architecture of Surveillance”, conceptualising FRT as a threefold interference with the right to privacy. Next, the article reviews the ECtHR jurisprudence following a structured analysis of the justifications and conditions that can support the collection of input data, the creation of databases and the use of FRT for preventing, investigating and prosecuting crimes. Finally, the article draws conclusions from the vast body of case law analysed for the context of FRT, distilling three core normative principles that delimit the use of facial identification by law enforcement authorities: the principle of extrema ratio, the principle of targeted suspicion and the principle of selective legitimacy. Although the article’s scope is limited to facial recognition, its findings can

*Technology until It Is Regulated*, in *Nature*, vol. 572, 2019, 565; S. Ovide, *A Case for Banning Facial Recognition*, in *The New York Times*, 9 June 2020.

<sup>5</sup> See among many others D. Dushi, *The Use of Facial Recognition Technology in EU Law Enforcement: Fundamental Rights Implications*, cit., 4; V.L. Raposo, *The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal*, in *European Journal on Criminal Policy and Research*, 2022, doi.org/10.1007/s10610-022-09512-y; I.N. Rezende, *Facial Recognition in Police Hands: Assessing the ‘Clearview Case’ from a European Perspective*, in *New Journal of European Criminal Law*, vol. 11, n. 3, 2020, 375; For a US perspective see A.G. Ferguson, *Facial Recognition and the Fourth Amendment*, in *Minnesota Law Review*, vol. 105, n. 3, 2020, 1105.

<sup>6</sup> See among others C.N. Pehlivan, N. Forgó and P. Valcke (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary*, Alphen aan den Rijn, Wolters Kluwer, 2025; P. Voigt and N. Hullen, *The EU AI Act*, Berlin, Springer Nature, 2024; N. Menéndez González and G. Mobilio, *Between Prohibited Risks and High Risks: The Regulation of Facial Recognition Technology*, in F. Donati, G. Finocchiaro and O. Pollicino (eds.), *La disciplina dell’Intelligenza Artificiale*, Milan, Giuffrè, 2025, 199. See also the relevant contributions in this Special Issue.

<sup>7</sup> F. Palmiotto and N. Menéndez González, *Facial Recognition Technology, Democracy and Human Rights*, in *Computer Law & Security Review*, vol. 50, 2023, 105857; M. Zalmieriute, *Glukhin v. Russia*. *App. No. 11519/20 Judgment*, in *American Journal of International Law*, vol. 117, 2023, 695; A. Dadashov, *Facial Recognition System as a Violation of Human Rights in the Context of ECHR Regional Systems*, in *Human Rights Brief*, vol. 27, n. 1, 2023, 45.

be applied to a broader range of biometric identification technologies, including emerging techniques such as gait analysis and iris scanning.

## 2. The Architecture of Surveillance

On 4 July 2023, the ECtHR issued its first ruling on the human rights implications of FRT in the case of *Glukhin v. Russia*.<sup>8</sup> The case involved the use of FRT to track the applicant, Mr. Glukhin, following his solo protest in the Moscow underground metro. The Court unanimously found that Russia violated Article 8 and Article 10 of the ECHR. In its reasoning, the Court held that employing such an invasive form of surveillance is incompatible with the ideals and values of a democratic society governed by the rule of law.<sup>9</sup> It also ruled that the use of FRT requires a high level of justification, with the highest level required for live facial recognition.<sup>10</sup>

Although *Glukhin v. Russia* provides critical insights into how FRT interacts with human rights protections, it fails to address some pressing legal and normative questions. Chief among these is whether the technology, by its very nature, violates Article 8 of the ECHR.<sup>11</sup> Echoing its earlier stance in *S. and Marper v. UK*,<sup>12</sup> the Court clarified that it would not assess the general permissibility of FRT under the Convention. Instead, it would focus solely on whether the use of FRT was justified under Article 8(2) of the ECHR in the specific case. As the Court put it: “The question is not whether the processing of biometric personal data by facial recognition technology may, in general, be regarded as justified under the Convention. The only issue to be considered by the Court is whether the processing of the applicant’s personal data was justified under Article 8(2) of the Convention in the present case.”<sup>13</sup>

This approach underlines some critical legal tensions in the judgment. On the one hand, the Court appears open to the use of FRT, acknowledging its usefulness in law enforcement when adequate safeguards are in place. On the other hand, it expresses serious

concerns about the use, in particular, of “live” FRT, describing it as “highly intrusive,” capable of chilling the exercise of other rights, and incompatible with the foundational ideals of democracy and the rule of law. Ultimately, while generally not excluding the possibility to use (even live) facial recognition, the Court cautiously warned that its use requires the “highest level of justification”.<sup>14</sup>

In a previous article co-authored with Natalia Menéndez González, we criticised the Court’s approach to the application of Article 8 ECHR to facial recognition.<sup>15</sup> More specifically, we pointed to the fact that the Court’s reasoning overlooked a crucial aspect of FRT – the broader surveillance architecture that this technology enables. The intrusive nature of FRT lies not only in its concrete use and purpose but also in the large-scale data processing it relies on. FRT requires mass data collection, the creation of facial image databases, and the widespread deployment of surveillance cameras to operate. Consider, for instance, that the number of FRT-enabled CCTV cameras in Moscow increased from 3,000 in 2017 to 220,000 in 2022.<sup>16</sup> This architecture of surveillance is the foundation upon which FRT operates.<sup>17</sup>

This article, therefore, aims to determine when FRT can be used for law enforcement purposes holistically, analysing each data processing activity that constitutes the FRT surveillance architecture. After a concise overview of the technology and its operations, this section will set the stage for the ECtHR case law tripartite analysis.

### 2.1. The Technology

Facial recognition is “digital matching technology”<sup>18</sup> that involves the automated processing of biometric data,<sup>19</sup> namely facial

<sup>8</sup> *Glukhin v. Russia* [2023] ECtHR 11519/20.

<sup>9</sup> *Ibid.*, para. 90.

<sup>10</sup> See more below in Section 5.

<sup>11</sup> For a critique of this approach see M. Zalnieriute, *Glukhin v. Russia. App. No. 11519/20 Judgment*, 698.

<sup>12</sup> *S and Marper v the United Kingdom* [2008] ECtHR [GC] 30562/04, 30566/04.

<sup>13</sup> *Glukhin v. Russia*, para. 85.

<sup>14</sup> *Ibid.*, para. 86.

<sup>15</sup> F. Palmiotto and N. Menéndez González, *Facial Recognition Technology, Democracy and Human Rights*, cit., 105857.

<sup>16</sup> *Glukhin v. Russia*, para. 5.

<sup>17</sup> See also D. Murray, *Facial Recognition and the End of Human Rights as We Know Them?*, cit., 148 [arguing that the surveillance capabilities made possible with FRT are “staggering - and unprecedented - in its power”].

<sup>18</sup> A.G. Ferguson, *Facial Recognition and the Fourth Amendment*, cit., 1110.

<sup>19</sup> Biometric data is defined in Art. 4(14) of Regulation (EU) 2016/679 (GDPR), as “personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the

images, to recognise an individual's identity. Simply put, facial recognition allows one to automatically match a facial image with a similar facial image in a stored database.<sup>20</sup> In order to generate a probabilistic match, the technology performs the following steps:<sup>21</sup>

*Analysis of the biometric sample.* FRT processes the input data, which can be a photograph or a video, to detect the location of the face and eventually enhance the quality of the sample.

*Creation of the template.* After these preliminary steps, it extracts a digital representation of the distinct characteristics of the detected face (so-called "template"). Akin to fingerprints, the face template is allegedly a unique identifier of an individual's face and, in principle, immutable over time.<sup>22</sup>

*Comparison of the template for face recognition.* Once the template for the biometric sample is created, the final step is to compare it with other templates stored in a database. Based on probabilistic statistics of resemblance, the system will return matches in order of the closeness of overlap between the target template and the template stored in the database.<sup>23</sup>

*Verification or identification.* Facial recognition can be either an identification or a verification process. Identification is a "one-to-many" process whereby "the target face image is compared with a database of many known facial images".<sup>24</sup> A typical example is the use of FRT by the police doing a check, where a newly taken photo is compared against a database of criminal mugshots to identify the individual. On the contrary, verification is a "one-to-one" process whereby the target facial image is compared with a previously confirmed photo to verify the identity of the subject. A classic example is the e-gate at airports, where the passenger's

face is compared with the passport's picture.<sup>25</sup> For the purpose of this article, I will exclusively refer to facial recognition for identification purposes.<sup>26</sup>

Facial identification can operate in two distinct ways.<sup>27</sup> When the comparison with a database and the identification occurs simultaneously with the capturing of the input data, thus resulting in instant identification and location of the data subject, FRT operates in "real-time".<sup>28</sup> These technologies involve the use of "live video feeds" from security cameras. A prominent example of real-time remote biometric identification is the use of FRT at public events to search for known fugitives in a crowd.

On the contrary, when the biometric data has already been captured, and the comparison and identification occur only after a significant delay, FRT operates "ex-post".<sup>29</sup> In this case, the technology uses pre-recorded data to identify individuals after the fact. This would be the case of law enforcement authorities analysing a CCTV footage or a video stored in a private device from a past crime scene to determine the identity of a suspect. A notorious example of post-remote biometric identification is the case of Daniela Klette, a member of Germany's Red Army Faction militant group, who was arrested on 26 February 2024. After decades on the run, the police managed to locate and identify her thanks to a biometric identification system that matched the last photograph they had of her with an image of a woman captured while participating in a capoeira course in Berlin.

Post-remote biometric identification is often portrayed as an essential tool to solve cold cases, as in the case of Daniela Klette, and to uncover child exploitation networks, as

---

unique identification of that natural person, such as facial images or dactyloscopic data".

<sup>20</sup> A.G. Ferguson, *Facial Recognition and the Fourth Amendment*, cit., 1109.

<sup>21</sup> On the technical side of FRT see A. Akbari, *Facial Recognition Technologies 101: Technical Insights*, in M. Zalnieriute and R. Matulionyte (eds.), *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge, Cambridge University Press, 2024, 29.

<sup>22</sup> *Ibid.*, 29-30.

<sup>23</sup> A.G. Ferguson, *Facial Recognition and the Fourth Amendment*, cit., 1111-1112.

<sup>24</sup> A. Akbari, *Facial Recognition Technologies 101: Technical Insights*, 29.

<sup>25</sup> *Ibid.*, 29.

<sup>26</sup> See the difference between verification and identification in the AI Act. According to Article 3(41), remote biometric identification systems operate without the "active involvement" of the individual and "typically at a distance". In contrast, biometric verification (e.g., using facial recognition to unlock a phone or pass through an airport security gate) occurs in the presence of the data subject. It is, therefore, considered less intrusive, as the individual maintains control over the process.

<sup>27</sup> Drawing a clear line between real-time and ex post facial recognition remains challenging, both technically and legally. However, for the purposes of this contribution, the article will adopt the distinction between real-time and post remote biometric identification as adopted by the EU AI Act.

<sup>28</sup> See Article 3(42) AI Act.

<sup>29</sup> See Article 3(43) and Recital 17 AI Act.

matches with victims from previous investigations may unveil a broader network of criminals.<sup>30</sup>

FRT is a powerful technology that law enforcement can use to investigate and prevent crimes, generate evidence in criminal proceedings, and conduct pre-emptive surveillance. As this section illustrates, to work as intended, facial recognition requires the collection of facial images to be compared with a dataset to find a probabilistic match.

The processing of facial images as input data, the creation and maintenance of police databases, and the concrete purpose and use of the automated match are necessary steps in the functioning of FRT, which constitute its “Architecture of Surveillance.” As the next section will show, each building block of such architecture (the input, the database, the output) constitutes an interference with the right to private life, which must, therefore, be justified under Article 8(2) of the ECHR.

## **2.2. A Threefold Interference**

Article 8 of the ECHR guarantees the right to respect for private and family life, home, and correspondence. This provision encompasses a broad range of interests, including personal autonomy, physical and psychological integrity, protection of personal data, and the confidentiality of communications. It plays a fundamental role in safeguarding individuals against arbitrary interference by public authorities and has become a cornerstone of privacy jurisprudence in Europe.<sup>31</sup>

The structure of Article 8 is twofold. Paragraph 1 establishes the substantive right to respect for private and family life, while paragraph 2 sets out the conditions under which a public authority may lawfully interfere with that right. According to the Court’s well-established case law, any such interference must satisfy three cumulative criteria: it must be in accordance with the law, pursue one or more legitimate aims - such as national security, public safety or the prevention of disorder or crime - and be necessary in a democratic society. The

necessity requirement implies that the interference must respond to a pressing social need and be proportionate to the aim pursued.<sup>32</sup> This proportionality assessment lies at the heart of the Court’s analysis and often determines whether an interference with Article 8 is justified. The Court has consistently underscored the importance of striking a fair balance between the interests of the individual and those of the community while ensuring that sufficient safeguards are in place to prevent abuse and arbitrariness. The interpretation of Article 8 is thus dynamic and evolutive, shaped by societal change and technological advancements.<sup>33</sup>

FRT is a data-thirsty technology that comprises several interferences with the right to private life to operate as intended. It requires, at minimum, the processing of two typologies of personal data: the facial image of the individual ought to be identified (the input), and a set of images to match that facial image against for the purpose of identification (the database).<sup>34</sup>

Under the ECHR, the collection of personal data is per se an interference with the right to private life. Despite not being an autonomous right, the ECtHR has widely recognised the fundamental importance of

<sup>30</sup> Europol Innovation Lab, *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement*, 2024, 25.

<sup>31</sup> On Article 8 ECHR, see generally D. J. Harris, M. O’Boyle, E.P. Bates, and C. M. Buckley (eds.), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press, 2014.

<sup>32</sup> On proportionality in the ECHR see Y. Arai-Takahashi and Y. Arai, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*, Cambridge, Intersentia, 2002; C. Hagenau-Moizard and Y. Sanchez, *The Principle of Proportionality in European Law*, in S. Ranchordás and B. de Waard (eds.), *The Judge and the Proportionate Use of Discretion*, Milton Park, Routledge, 2015; For a specific account of proportionality and digitalisation see J. Czarnocki and P. Palka (eds.), *Proportionality in EU Digital Law: Balancing Conflicting Rights and Interests*, London, Hart, 2024.

<sup>33</sup> With regard to technological advancements, the Court has been particularly sensitive in striking a proper balance between the legitimate aim of countering crimes and the protection of human rights. In cases concerning the collection of personal data by law enforcement authorities, the Court has repeatedly stated that “the use of modern scientific techniques cannot be authorised at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests”. See, among others, *S. and Marper v. the United Kingdom* [GC], 2008, para 112; *Podchasov v. Russia*, 2024, para. 62. With regard to more advanced technologies, such as Artificial Intelligence and facial recognition, the Court recognised that the mere availability of such technologies makes the collection and retention of facial images particularly concerning. See *Gaughran v. the United Kingdom*, 2020, para 70.

<sup>34</sup> A.G. Ferguson, *Facial Recognition and the Fourth Amendment*, cit., 1115.

protecting personal data for rights guaranteed in Article 8 of the ECHR<sup>35</sup> and developed extensive case law on data collection by law enforcement authorities. Section 3 thoroughly reviews this case law, distinguishing between personal data collection through live cameras and means of secret surveillance measures (real-time facial identification) from data collection through police searches and other investigative measures (ex-post facial identification). It aims to identify under which conditions, and through which means, law enforcement authorities can collect facial images for the purpose of identification through FRT.

The second interference of FRT with Article 8 of the ECHR is the creation of police databases, which are necessary for the facial identification process. Under the ECHR, the storage of personal data by a public authority, such as facial images, amounts to an interference with Article 8, whether or not the data is subsequently used.<sup>36</sup> The Court has considered several cases relating to the retention of personal data in databases designed for the purpose of preventing and combating crimes, which will be extensively reviewed in Section 4. The aim of this section is to discern under which conditions police databases can be created for using FRT, which data can be stored therein and what specific safeguards must accompany their maintenance.

The third interference of FRT with the rights enshrined in Article 8 ECHR relates to the use of the technology. FRT could be deployed by law enforcement authorities for different objectives, such as subjecting a suspect to investigations, using the automated match as evidence in legal proceedings, or preventing crimes through surveillance practices. Each of these activities constitutes a distinct interference with privacy, which must be, therefore, proportional and necessary in a democratic society. Arguably, the standard of justification will differ depending on the purpose for which the technology is deployed

and the way in which it operates (in real-time or ex-post).<sup>37</sup> Section 5 focuses on the justifications that can support the use of FRT for law enforcement purposes, distinguishing between generalised surveillance, crime investigations, and prosecution. Attention will be on the principle of reasonable suspicion, a foundational principle of human rights law that delimits the discretionary powers of law enforcement authorities and, therefore, their use of advanced technologies. A summary of the threefold interference with Article 8 ECHR, constituting the Architecture of Surveillance, is provided in the table below.

	Real-time Remote	Post Remote
<i>The Input</i>	Live cameras and secret surveillance	Investigative material
<i>The Database</i>	Creation and maintenance of police databases containing sensitive data	
<i>The Output</i>	Investigations and pre-emptive surveillance Evidence in legal proceedings	

**Table 1 - The Architecture of Surveillance and Its Threefold Interference**

**3. The Collection of the Input Data**

The first component of the “Architecture of Surveillance” refers to the collection, storage and processing of facial images of individuals that ought to be identified (“input data”). Facial images are biometric data, a sensitive category of personal data since their processing allows for uniquely verifying the identity of the data subject.<sup>38</sup> As such, facial images are subject to particularly stringent limits regarding their collection and analysis under data protection law. In the context of law enforcement, authorities collect facial images for the purpose of facial recognition identification in two ways: in real-time, using video cameras or other means of secret surveillance, or *ex-post facto* through the gathering of investigative materials and evidence. This section systematically reviews the Court’s case law on the police use of video cameras, secret surveillance and police powers

<sup>35</sup> See among many others *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017] ECtHR [GC] 931/13 para 137; *L.b v Hungary* [2023] ECtHR [GC] 36345/16 para 103.

<sup>36</sup> *Amann v Switzerland* [2000] ECtHR [GC] 27798/95 para 69; *Rotaru v Romania* [2000] ECtHR [GC] 28341/95 para. 46; *M.k v France* [2013] ECtHR 19522/09 para. 29; *S. and Marper v. the United Kingdom* (n 12) para. 67; *Aycaguer c France* [2017] ECtHR 8806/12 para. 33.

<sup>37</sup> *Glukhin v. Russia*, para. 86.

<sup>38</sup> See Art. 4(14) GDPR.

to gather personal data during investigations. Its aim is to identify limits to police data collection, which, therefore, defines the breadth of facial recognition technology's legitimate use.

### 3.1. Data collection through video cameras and secret surveillance

Regarding video surveillance, the Court generally draws a distinction between the use of cameras for security purposes and the recording of those acts for other unforeseeable purposes, including the identification of individuals and their use as evidence in criminal proceedings, in order to establish the boundaries of the right to private life.<sup>39</sup> According to the Court, the recording of a video and the "systematic or permanent nature" of the record may constitute an interference with Article 8 ECHR. In *Perry v UK*, a case from 2003, the Court considered whether the filming of a suspect at the police station using a covert closed-circuit camera would amount to interference with the applicant's right to a private life. Contrary to the Government's argument that the applicant had no reasonable expectation of privacy when held in police custody, the Court concluded that the recording of a video constituted a processing of personal data, therefore covered by the right to private life.<sup>40</sup> The fact that the police recorded the video for later identification of the suspect and used it as evidence during the proceeding was an element that particularly weighed on the Court's analysis. Additionally, the applicant could not reasonably expect that his footage was being recorded as part of an identification procedure and, potentially, as prejudicial evidence at trial.<sup>41</sup>

More recently, the Court further developed this reasoning in light of the fast technological advancement witnessed in the past decade. *Gaughran v. UK*, a seven-year case older than *Perry v. UK*, concerned the indefinite storage of the applicant's custody photograph taken by the police.<sup>42</sup> In considering whether there had been an interference, the Court gave

considerable attention to the fact that, *potentially*, the police may also apply facial recognition for the purpose of identification. Even though no evidence of the actual use of FRT was available, the Court had "no doubt that the taking and retention of the applicant's photograph amounts to an interference with his right to private life" for the mere possibility that FRT may be applied.<sup>43</sup>

*Perry v UK* and *Gaughran v. UK* hold significant importance for facial recognition technology, as they univocally clarify that the collection of facial images for the purpose of identification amounts to severe interference with Article 8 ECHR. Such interference also extends to situations where video cameras are installed in public spaces.<sup>44</sup> The subsequent question is whether such interference can be justified under Article 8(2) ECHR.

In addressing the second step of the analysis, the Court has clarified in *Glukhin v. Russia* that facial recognition technology attracts a heightened level of protection for individuals and, thus, a higher standard of justification for its use by States, with the "highest" level of justification required for real-time remote identification.<sup>45</sup> In the judgment, the Court pointed to the fact that the use of FRT is a distinct form of surveillance, which can hardly be compared to traditional security camera surveillance. Indeed, FRT profoundly changed the very nature of video surveillance, making it more pervasive, indiscriminate, and prone to abuses. FRT also operates secretly and remotely, without the active knowledge and involvement of data subjects. Considering these distinct characteristics, it is arguably more appropriate to qualify FRT as a means of secret and potentially mass surveillance to draw the boundaries of justified interference with privacy.

The ECtHR has dealt with a considerable number of cases concerning covert surveillance, espionage and mass surveillance operations.<sup>46</sup> Without the ambition of

<sup>39</sup> *Peck v the United Kingdom* [2003] ECtHR 60898/00 paras 59-62; *Perry v the United Kingdom* [2003] ECtHR 71962/10, 13847/11, 61228/12, 31786/15, 17900/15 paras. 41-42.

<sup>40</sup> *Perry v. the United Kingdom*, para. 40.

<sup>41</sup> *Ibid.*, para. 41.

<sup>42</sup> *Gaughran v The United Kingdom* [2020] ECtHR 45245/15, paras. 6-9.

<sup>43</sup> *Ibid.*, para. 70.

<sup>44</sup> *Perry v. the United Kingdom*, para 36; *Gaughran v The United Kingdom*, para. 70.

<sup>45</sup> *Glukhin v. Russia*, para. 86.

<sup>46</sup> For an updated collection of more recent case law, see the *Guide on Article 8 of the European Convention on Human Rights*, in *Registry of the European Court of Human Rights*, 2024, 65-67; In the literature, see G. Malgieri and P. De Hert, *European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not*

providing an exhaustive illustration of the large body of case law on the matter, the following overarching principles can be derived from its jurisprudence.<sup>47</sup>

The Court has consistently held that secret surveillance measures are tolerable only “in so far as strictly necessary for safeguarding the democratic institutions”.<sup>48</sup> This is particularly relevant in modern societies where technological developments have advanced the means of espionage and surveillance, which States may use for the legitimate aim of preventing disorder, crime, or terrorism.<sup>49</sup> In *Szabó and Vissy v. Hungary*, the Court highlighted that to be “necessary in a democratic society”, the measure must be strictly necessary to safeguard democratic institutions and strictly limited to obtain essential intelligence in an individual operation. Any measure of secret surveillance which did not fulfil the strict necessity criterion would be prone to abuse by the authorities.<sup>50</sup> Strict necessity, therefore, requires an individual justification for its use. Indiscriminate mass surveillance practices cannot be regarded as justifiable interferences with privacy.<sup>51</sup>

Moreover, the existence of guarantees against abuse, including “end-to-end safeguards” illustrated in *Big Brother Watch and Others v. UK*, is essential.<sup>52</sup> National law

---

*Necessarily by Judges*, in D. Gray and S. E. Henderson (eds.), *The Cambridge Handbook of Surveillance Law*, Cambridge, Cambridge University Press, 2017; A.R. Peall, *A Contextual Analysis of the European Court of Human Rights’ Secret Surveillance Jurisprudence*, PHD thesis, University of Leicester, 2025; P. Notermans, *Surveillance Measures and the Exception of National Security in the Case Law of the European Court of Human Rights*, in K. McCall-Smith, A. Birdsall and E. Casanas Adam (eds.), *Human Rights in Times of Transition*, Cheltenham, Edward Elgar, 2020.

<sup>47</sup> See among many others the landmark cases *Roman Zakharov v Russia* [2015] ECtHR [GC] 47143/06; *Big Brother Watch and Others v the United Kingdom* [2021] ECtHR [GC] 58170/13, 62322/14, 24960/15; *Centrum För Rättvisa v Sweden* [2021] ECtHR [GC] 35252/08.

<sup>48</sup> *Klass and Others v Germany* [1978] ECtHR 38581/16, 41914/16, 57510/16, 62644/16, 7190/17, 10973/17, 12530/17, 19411/17, 22087/17, 28475/17, 78165/17 para. 42; *Szabó and Vissy v Hungary* [2016] ECtHR 37138/14 paras. 72-73.

<sup>49</sup> *Klass and Others v. Germany*, para. 48; *Glukhin v. Russia*, para 85.

<sup>50</sup> *Szabó and Vissy v. Hungary*, paras. 72-73.

<sup>51</sup> See, however, in *Centrum För Rättvisa v. Sweden*, para 261, and *Big Brother Watch and Others v the United Kingdom*, paras. 322-323, where the Court expressly admitted that the use of a bulk interception regime was not per se contrary to Article 8.

<sup>52</sup> *Big Brother Watch and Others v. the United*

must ensure that it is sufficiently precise, effective, and comprehensive for ordering and executing surveillance measures and securing potential redress.<sup>53</sup> Additionally, the scope of secret surveillance measures must be foreseeable, clearly detailing the circumstances, the nature of the offence and the definition of categories of people liable for being under surveillance.

### 3.2. Data collection through investigative operation

A second modality to obtain input data for facial recognition identification is gathering photographs or videos during investigations. After the facial images are collected, police may use FRT to identify the individual portrayed in the video or picture. This typology of identification is defined in the law as “post-remote” biometric identification. It differs from real-time insofar as the identification occurs with a significant delay from the collection of the facial images that ought to be processed by the system. From a human rights perspective, the core difference between real-time and post-remote lies in the fact that the latter does not require live surveillance of public or private spaces and the processing of biometric data of any individual transiting in that area to operate. Through their coercive powers, the police may gather facial images from several sources, such as social media, private devices, publicly available data, or recorded videos from CCTV cameras.

Under the Convention, facial images are covered by the right to protect one’s image and presuppose the right to control how they are used.<sup>54</sup> According to the Court, such right includes the possibility to refuse publication and the right to object to the recording, conservation and reproduction of the image by another person.<sup>55</sup> In principle, the processing of facial images presupposes obtaining prior consent of the concerned person at the time when the picture is taken.<sup>56</sup> In the context of law enforcement, however, the police enjoy broader powers to collect and retain facial

---

*Kingdom*, para. 350.

<sup>53</sup> *Szabó and Vissy v. Hungary*, para. 89.

<sup>54</sup> *Reklos and Davourlis v. Greece* [2009] ECtHR 1234/05 para 40-43; *Glukhin v. Russia*, para. 66; *Margari v Greece* [2023] ECtHR 36705/16, para. 28.

<sup>55</sup> *López Ribalda and Others v Spain* [2019] ECtHR [GC] 1874/13, 8567/13. Para. 89.

<sup>56</sup> *Reklos and Davourlis v. Greece*, paras. 37-40.

images. Data processing activities by the police may, in fact, be regarded as “necessary in a democratic society” even without the prior consent of the data subject.<sup>57</sup>

The Court has, for instance, justified the taking and retention of photos of a suspect taken after their arrest for the purpose of countering crimes,<sup>58</sup> or of a suspect of a terrorist offence for the purpose of preventing terrorism.<sup>59</sup> In *Murray v. UK*, the Court has also admitted, in principle, the recording and retention of personal details of even other persons present at the arrest.<sup>60</sup> The Court also declared manifestly ill-founded an application concerning the retention in the Interior Ministry’s computer system of the applicant’s photo, which had been taken by the authorities when he was arrested by the police on suspicion of committing an offence.<sup>61</sup> In the case of *P.N. v. Germany*, the Court found no violation of Article 8 as regards a collection ordered by the police following the opening of fresh criminal proceedings against an individual who had been previously convicted of information identifying him, such as photographs of his face and body, especially any tattoos, together with fingerprints and palmprints.<sup>62</sup>

However, the Court found violations of Article 8 ECHR when the photographs were retained for an unlimited duration, especially in cases where the individual suspected of committing an offence was later acquitted.<sup>63</sup> The Court, thus, requires a higher standard of justification for retaining photographs of individuals who are not convicted or charged with a criminal offence, due to the higher risk of stigmatisation that may result from the unlimited duration of data retention.

Notwithstanding the broader margin of appreciation afforded to Member States in this area, it is relevant to highlight a notable difference in the Court’s approach to assessing the “necessary in a democratic society” in recent case law. In light of technological advancements, the Court has remarked on the

necessity of considering the possibility that facial recognition technology may be used when examining the necessity of interference with the right to private life when law enforcement authorities take photographs.

In the case *Gaughran v. the United Kingdom*, the Court gave specific consideration to the possibility that facial recognition might have been used by the police, despite being unclear from the facts of the case if it actually occurred.<sup>64</sup> The case concerned the indefinite retention of the photograph of an individual convicted of driving with excess alcohol, in addition to his DNA profile and fingerprints. The Court found a violation of Article 8 ECHR, considering the retention of personal data disproportionate in the absence of any real possibility of review and without reference to the seriousness of the offence.<sup>65</sup> Similarly, in *Glukhin v. Russia*, despite the lack of certainty as to the State’s use of FRT, the Court concluded that the identification of the applicant from his photographs and videos constituted a violation of Article 8 ECHR. Even if the facial images that allowed for the identification were published through a public Telegram channel, the Court considered the biometric identification a particularly intrusive measure that requires a high level of justification to be deemed a lawful interference.<sup>66</sup>

Arguably, the widespread availability of FRT to law enforcement authorities in Europe significantly shapes the Court’s approach to Article 8 ECHR. As the ECtHR now presumes that FRT may be used, it, therefore, requires a higher level of justification for the police collection and retention of facial images.

#### **4. The Creation of the Database**

Facial recognition identification essentially compares the facial image of unidentified individuals with the facial images of identified individuals to find a potential match. Therefore, law enforcement authorities must establish and maintain a database of faces to effectively use FRT. Clearly, the quality and quantity of the stored data, as well as the period of retention of such data, increase the effectiveness of the technology. The more comprehensive and long-term these

<sup>57</sup> *Suprunenko v. Russia* [2018] ECtHR 8630/11, paras. 63-65.

<sup>58</sup> *Ibid.*, paras. 63-65.

<sup>59</sup> *Murray v. the United Kingdom* [1994] ECtHR [GC] 14310/88, paras. 92-93.

<sup>60</sup> *Ibid.*, para. 93.

<sup>61</sup> *Suprunenko v. Russia*, para. 65.

<sup>62</sup> *P.N. v. Germany* [2020] ECtHR 74440/17, paras. 76-91.

<sup>63</sup> *S. and Marper v. the United Kingdom*, para. 122; *Gaughran v. The United Kingdom*, para. 82-84.

<sup>64</sup> *Gaughran v. The United Kingdom*, paras. 67-70.

<sup>65</sup> *Ibid.*, paras. 96-98.

<sup>66</sup> *Glukhin v. Russia*, paras. 64-91.

databases are, the more powerful the technology becomes from an operational standpoint. From a human rights perspective, however, creating large police databases raises several issues. The Court has been particularly concerned with the risk of abuse and stigmatisation raised by the indiscriminate and undifferentiated nature of police databases and the unlimited storage period of the data contained therein.<sup>67</sup> In several cases, the Court found a violation of Article 8 ECHR and developed guiding principles restricting police powers in collecting and retaining personal data. This section carefully reviews this Court's jurisprudence to show how its case law on police databases provides crucial guardrails to the use of FRT.

#### 4.1. Nature of data stored and collected

The ECtHR has developed a consistent body of case law concerning the compatibility of police databases with Article 8 of the ECHR. Across its jurisprudence, the Court has reiterated that the collection and retention of personal data must be necessary in a democratic society and proportionate to the legitimate aim pursued. This proportionality assessment is particularly sensitive to the risk of stigmatisation and the extent to which state measures respect the presumption of innocence.<sup>68</sup>

In its case law, the Court has consistently drawn a clear distinction between the individuals subject to a criminal investigation or proceeding (as a suspect, defendant or convicted for a criminal offence) and other data subjects, such as activists and protesters. In the latter case, the Court has generally found that storing their data in a police database was not a justified interference under the Convention.<sup>69</sup> The Court has also emphasised the need for heightened scrutiny when data retention concerns individuals engaged in lawful protest or activism. In *Catt v. the United Kingdom*, the retention of data on a peaceful protester was found to be unjustified. The Court considered that retaining information on individuals who had not been involved in criminal activity posed a serious threat to democratic freedoms and

lacked a sufficient justification under Article 8.<sup>70</sup>

On the contrary, the “objective usefulness” of photos taken of individuals subject to criminal investigation or prosecution may render their retention “necessary in a democratic society”.<sup>71</sup> In these cases, while the Court acknowledges the risks of stigma to individuals resulting from the storing of their data in police databases, it also recognises the need for law enforcement to collect facial images for the purposes of countering crimes. Central to its analysis is the distinction between individuals based on the seriousness of the offence committed,<sup>72</sup> and their status within the criminal process - whether they are suspects, convicted persons, or acquitted individuals.<sup>73</sup>

The ECtHR has been especially critical of data retention policies that fail to distinguish between convicted individuals and suspected or accused of a criminal offence. In *S. and Marper v. the United Kingdom*, the Court ruled that the indefinite retention of fingerprints and DNA profiles from individuals who had been suspected but not convicted of criminal offences amounted to a violation of Article 8. The Court emphasised the blanket and indiscriminate nature of the policy, the absence of time limits, and the lack of independent review. These shortcomings were found to be particularly problematic when applied to minors, given the importance of their social reintegration and development.<sup>74</sup> Retention of personal data following an acquittal or dismissal of charges has also been found incompatible with Article 8. In *Brunet v. France* and *M.K. v. France*, the Court ruled that maintaining personal data in police databases despite the termination of criminal proceedings was unjustified.<sup>75</sup>

However, the Court's approach has been more lenient towards individuals who were suspected of serious offences, such as terrorism. In *Murray v. the United Kingdom*, the taking and retention of a photograph of an individual suspected of a terrorist offence was not found to violate Article 8. The Court held

<sup>70</sup> *Ibid.*

<sup>71</sup> *Suprunenko v. Russia*, paras. 63-65.

<sup>72</sup> *M.K. v. France*, para 41; *Aycaguer v. France*, para. 43; *Gaughran v. The United Kingdom*, para. 94.

<sup>73</sup> *S. and Marper v. the United Kingdom*, para. 119; *M.K. v. France*, para. 42; *Brunet v. France* [2014] ECtHR 21010/10, para. 41.

<sup>74</sup> *S. and Marper v. the United Kingdom*, para. 124.

<sup>75</sup> *Brunet v. France*, para. 45; *M.K. v. France*, para. 47.

<sup>67</sup> See among others, *M.K. v. France*, para 35; *Aycaguer v. France*, para. 34; *S. and Marper v. the United Kingdom*, para. 122.

<sup>68</sup> *S. and Marper v. the United Kingdom*, para. 122.

<sup>69</sup> *Catt v the United Kingdom* [2019] ECtHR 43514/15, 128.

that the interference was proportionate to the legitimate aim of preventing terrorism and acknowledged the margin of appreciation that states have in investigating serious threats to public safety.

With regard to individuals convicted of serious crimes or those with a record of repeat offending, the Court has generally upheld the compatibility of data retention with Article 8 ECHR. In *Peruzzo and Martens v. Germany* and *B.B. v. France*, data collection and retention measures were found to be proportionate, given the applicants' convictions for serious offences. Similarly, in *P.N. v. Germany*, the collection of identification data, including photographs and fingerprints, was deemed proportionate in light of the applicant's status as a repeat offender and the presence of protective measures, such as limited data retention periods and individualised review.

By contrast, the retention of personal data following convictions for minor offences has generally not withstood scrutiny under Article 8 ECHR. In *Gaughran v. the United Kingdom*, the Court found a violation where the indefinite retention of the applicant's biometric data and photographs followed a conviction for driving with excess alcohol. The authorities' failure to consider the relatively low seriousness of the offence or to implement tailored retention policies was considered disproportionate.<sup>76</sup> Likewise, in *Aycaguer v. France*, the Court criticised the indiscriminate data retention following a conviction for non-violent conduct during a political demonstration. The acts in question - hitting law enforcement officers with an umbrella - were not deemed comparable to serious crimes such as terrorism or human trafficking and thus did not justify the broad application of data retention laws.<sup>77</sup>

#### **4.2. Duration of the retention period**

In its case law under Article 8 of the ECHR, the Court has consistently emphasised that the proportionality of data retention by law enforcement authorities depends not only on the seriousness of the offence but also on the existence of effective procedural safeguards, such as time-limited retention periods and mechanisms for independent review or deletion. The combination of these

factors determines whether interfering with the right to privacy can be justified in a democratic society.

The Court has regularly found violations of Article 8 where data retention affected individuals who had not been convicted or had been involved in minor offences, particularly when such retention was indefinite or lacked sufficient safeguards.<sup>78</sup> In the landmark case *S. and Marper v. the United Kingdom*, the Court found a violation arising from the indefinite retention of fingerprints and DNA data from individuals suspected but not convicted of an offence.<sup>79</sup> The absence of time limits, independent review, and differentiation based on the seriousness of the offence were central to the Court's reasoning. Similarly, in *Gaughran v. the United Kingdom*, the Court concluded that the indefinite storage of biometric data and a photograph of an individual convicted of a non-violent traffic offence was disproportionate. The lack of regard for the nature and gravity of the offending, as well as the absence of safeguards allowing early deletion of the data, contributed to the finding of a violation.<sup>80</sup>

The Court has taken a comparable position in cases such as *Brunet v. France*, *M.K. v. France*, and *Aycaguer v. France*, all of which concerned either suspects or individuals whose criminal proceedings had been discontinued or who had been convicted for relatively minor infractions. In each of these cases, even when domestic law provided maximum retention periods - ranging from twenty to forty years - the Court criticised the absence of mechanisms for erasure and the failure to tailor retention periods to the seriousness of the offence.

By contrast, the Court has generally found no violation of Article 8 where data retention involved individuals convicted of serious offences or where there was a risk of recidivism, particularly when adequate safeguards were in place. In *B.B. v. France*, the retention of data for up to thirty years concerning an individual convicted of sexual assault was upheld. The Court noted that the retention period was predetermined, automatically terminated at its expiry, and accompanied by procedures allowing early deletion once the data was no longer

<sup>76</sup> *Gaughran v. The United Kingdom*, para. 96.

<sup>77</sup> *Aycaguer v. France*, paras. 42-43.

<sup>78</sup> See among others *Gaughran v. The United Kingdom*; *Aycaguer v. France*; *M.K. v. France*; *Brunet v. France*.

<sup>79</sup> *S. and Marper v. the United Kingdom*, para. 119.

<sup>80</sup> *Gaughran v. The United Kingdom*, para. 88.

relevant.<sup>81</sup> Similarly, in *Gardel v. France* and *M.B. v. France*, data retention policies lasting up to thirty years were found to comply with Article 8, as they were accompanied by sufficient procedural safeguards, including clear legal bases, automatic review procedures, and deletion mechanisms.<sup>82</sup>

The importance of procedural safeguards was further underscored in *Peruzzo and Martens v. Germany*. The Court accepted the practice on the basis that domestic law required periodic review at intervals not exceeding ten years. The review procedures had to take into account the nature and gravity of the offence, the likelihood of reoffending, and whether the original purposes of data retention remained valid. In *P.N. v. Germany*, the Court found no violation in the five-year retention of identification data from a repeat offender, where the measure followed the opening of new proceedings. The limited impact on the applicant's private life, the existence of time-limited retention, and individualised review contributed to the Court's conclusion that the interference was proportionate.<sup>83</sup>

Throughout its jurisprudence, the Court has stressed that the existence and effective operation of safeguards are often decisive in assessing the proportionality of data retention. Time limits are necessary but insufficient; what matters is whether individuals have a realistic opportunity to have their data erased once the initial justification no longer applies. The Court has cautioned that nominal maximum retention periods, such as those of twenty or forty years, may fail to meet Convention standards if early deletion is effectively unavailable or purely hypothetical.<sup>84</sup>

Drawing on this illustrated data collection and retention jurisprudence, one can reflect on what normative constraints can be derived for the deployment of facial recognition technology. As facial recognition identification relies on the comparison of images with a dataset of known individuals, its effective operation presupposes the existence of extensive repositories of facial

data. However, the Court's case law on police databases significantly restricts the capabilities of facial recognition technology. It establishes that the legitimacy of data retention must be assessed through a proportionality analysis that weighs the seriousness of the offence against the necessity of data processing. Generally, legitimate police databases would be restricted to the collection of personal data of convicted individuals or suspects of serious offences only. The collection of facial images of protestors, individuals acquitted or discharged of a criminal offence, suspects, and even convicted individuals of minor offences would likely fail to meet the standard of proportionality.

### 5. The Use and Purpose of the Output

FRT is a multi-purpose technology that law enforcement authorities can use to achieve different objectives. Post-remote FRT generally allows individuals to be identified *ex post facto*. When used retrospectively, FRT aids investigators in identifying potential suspects and solving cold cases. Real-time remote FRT allows not only the identification but also the location and tracking of the identified individual. Both typologies of FRT could also be used at a later stage of the criminal process to generate evidence against the defendant. This section aims to review the Court's case law to ascertain which purpose and triggering conditions can justify the use of FRT.

#### 5.1. Investigations and pre-emptive surveillance

The use per se of FRT is a particularly severe interference with the right to privacy, which, therefore, requires specific conditions to be deemed lawful, necessary and proportionate under Article 8 ECHR. Generally, to ascertain whether a measure interfering with the protection of personal data under Article 8 fulfils the condition of being "necessary in a democratic society", the Court has examined whether it has complied with the requirements listed in Article 5 of the Convention 108+,<sup>85</sup> namely the requirement of data minimisation, accuracy, and the purpose limitation principle.

<sup>85</sup> Council of Europe Convention for the protection of individuals with regard to the processing of personal data (CETS n° 108).

<sup>81</sup> *BB v France* [1998] ECtHR 30930/96, para. 67.

<sup>82</sup> *Gardel v. France* [2009] ECtHR 16428/05, para. 69; *M.B. v France* [2024] ECtHR 31913/21, para. 59.

<sup>83</sup> *Peruzzo and Martens v Germany* [2013] ECtHR 7841/08, 57900/12, paras. 44-49.

<sup>84</sup> *M.K. v. France*, paras. 42-44; *Brunet v. France*, paras. 43-45; *Aycaguer v. France*, paras 44-47.

More specifically, in the context of law enforcement activities, the requirement for reasonable suspicion serves as the primary limitation on the discretionary powers of the police. This principle, explicitly recognised in Article 5(1)(c) of ECHR, requires any restrictions of liberty must be based on “reasonable suspicion of having committed an offence or when it is reasonably considered necessary to prevent his committing an offence or fleeing after having done so”. In the context of arrest and pre-trial detention, the ECtHR has held that a reasonable suspicion that a criminal offence has been committed presupposes the existence of facts or information which would satisfy an objective observer.<sup>86</sup> In the case of preventive detention, it must be linked to a concrete and imminent offence and not used as a general measure based on a vague perception of risk.<sup>87</sup>

Beyond restrictions of liberty, the ECtHR has extended the application of the reasonable suspicion standard to the activities of police interfering with the right to privacy. For instance, in *Ivashchenko v. Russia*, the customs authorities’ powers to consult and collect individuals’ electronic data amounted to a violation of Article 8 ECHR in the

absence of reasonable suspicions of wrongdoing.<sup>88</sup> In the context of stop-and-search powers<sup>89</sup> and surveillance and data collection,<sup>90</sup> the ECtHR has consistently required intrusive police activities to be based on an objective and individualised suspicion of involvement in criminal activity. Any deviation from this standard risks violating the rights protected under the ECHR, leading to unlawful state interference with individual rights.<sup>91</sup> It follows that if the reasonable suspicion standard must be respected in activities such as stop-and-searches or mere data collection, then *a fortiori* must be met when law enforcement authorities use FRT, which is a severe form of interference with privacy.

The respect of the reasonable suspicion standard to privacy interferences, therefore, categorically excludes the use of FRT, both real-time and post, for the sake of deterrence and general crime prevention. The triggering conditions for the use of technology must be linked to a reasonable suspicion that an individual has committed a crime. This requirement serves both as a procedural and a substantive constraint on States’ use and abuse of FRT.

Procedurally, the use of FRT justified on the grounds of suspicion requires concrete and objective facts. A vague or general assumption about an individual’s potential

<sup>86</sup> *Selahattin Demirtaş v. Turkey* App no 14305/17 (ECtHR, 22 December 2020), para. 314; *Ilgar Mammadov v. Azerbaijan* App no 15172/13 (ECtHR, 29 May 2019), para 88; *Erdagöz v. Turkey* App no 36219/97 (ECtHR, 16 March 1999), para. 51; *Fox, Campbell and Hartley v. the United Kingdom* App nos. 12244/86, 12245/86 and 12383/86 (ECtHR, 27 March 1991), para. 32.

<sup>87</sup> *Selahattin Demirtaş v. Turkey*, para. 314 [“Having a reasonable suspicion presupposes the existence of facts or information which would satisfy an objective observer that the person concerned may have committed the offence”]; *Ječius v. Lithuania* App no 3457/97 (ECtHR, 31 July 2000), para. 50 [“A person may be detained, in the context of criminal proceedings, only for the purpose of bringing him or her before the competent legal authority on reasonable suspicion of having committed an offence”]; *Schwabe and M.G. v. Germany* App nos 8080/08 and 8577/08 (ECtHR, 1 December 2011), paras 110-118 [preventive detention must be specifically linked to a concrete and imminent offense, not used as a general measure against groups perceived as dangerous]; *Kurt v. Austria* App no. 62903/15 (ECtHR, 15 June 2021), paras. 188 and 190 [“While pre-trial detention can never be used as a purely preventive measure, the facts and results of any risk assessment carried out with an eye to the possible need for preventive operational measures may be taken into account in the context of the assessment of the risk of further offences”]. More specifically, “The authorities must establish whether there exists a real and immediate risk to the life of one or more identified victims of domestic violence by carrying out an autonomous, proactive and comprehensive risk assessment”].

<sup>88</sup> *Ivashchenko v Russia* [2018] ECtHR 61064/10, para. 59-95.

<sup>89</sup> Among others, *Gillan and Quinton v. UK* App no. 4158/05 (ECtHR, 12 December 2010), para. 83-86 [holding that top-and-search by the police must be based on reasonable suspicion of wrongdoing]; *Beghal v. UK* App no 4755/16 (ECtHR, 28 February 2019), para 109 [holding that border stop-and-search powers that do not require individualized suspicion lack adequate protection against arbitrary use].

<sup>90</sup> Among others, *Zakharov v. Russia* App no. 47143/06 (ECtHR, 4 December 2015), para 260 [holding that mass surveillance and indiscriminate phone tapping without individualised suspicion violate Article 8]. See also the case law of the Court of Justice of the EU, Case C-205/21 *V.S.* [2023] OJ C 94, paras 128-135 [holding that mass biometric data collection from all accused persons must be based on reasonable suspicion for each individual]; Case C-511/18 *La Quadrature du Net and Others v. Premier ministre and Others* (Grand Chamber 6 October 2020), para. 180 [holding that blanket retention of telecommunications data without specific suspicion violates privacy rights].

<sup>91</sup> For an overview of European case law and surveillance see R. Van Brakel and P. De Hert, *Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies*, in *Cahiers Politicestudies*, vol. 3, n. 20, 2011, 163.

involvement in a criminal offence or perceived dangerousness does not satisfy the requisite standard.<sup>92</sup> What would amount to a reasonable suspicion depends on all the circumstances of the case. However, the Court clarified that the facts that raise suspicions need not be of the same level as those necessary to justify a conviction or even bring a charge.<sup>93</sup> In the context of surveillance technologies, the Court made explicit in *Roman Zakharov v. Russia* that authorising bodies must verify the presence of factual indications “for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security”.<sup>94</sup> The Court has pointed to the importance of establishing procedures under national law for the authorisation of surveillance measures, such as FRT, that allow the authorising body to verify the presence of reasonable suspicion.<sup>95</sup>

Substantively, reasonable suspicion of any crime, regardless of its severity and gravity, would not suffice to justify the use of FRT. In its case law, the Court has made it clear that not all offences warrant the same degree of interference with fundamental rights. The existence of reasonable suspicion is a necessary but not sufficient condition for the use of highly intrusive surveillance measures, such as FRT. In *Glukhin v. Russia*, the Court reiterated that in the assessment of the “necessity in a democratic society” of the processing of personal data in the context of investigations, the nature and gravity of the offences in question are important elements to be taken into account.<sup>96</sup> The seriousness of the offence has, thus, become a substantive filter in the Court’s assessment of whether the use of surveillance technology is necessary in a democratic society, particularly with regard to FRT, which requires a “high” or “highest” level of justification.

The Court has provided some guidance, albeit not exhaustive, on the types of crimes that would meet the threshold of seriousness and, therefore, likely justify the use of FRT.

These include terrorism-related offences,<sup>97</sup> sexual offences and offences against minors,<sup>98</sup> violent crimes such as aggravated bodily harm,<sup>99</sup> as well as repeat offences and recidivism.<sup>100</sup>

Drawing some conclusions for FRT, this body of case law suggests that the deployment of FRT must be both targeted and grounded in reasonable suspicion of serious criminal activity. Notably, the respect of this normative principle applies to both post-remote and real-time FRT, provided that the latter would require a higher level of justification due to its intrusiveness. The mere availability and use of FRT as a tool of generalised surveillance, for monitoring protests or other public events, or as a part of deterrence strategies are categorically excluded.

## 5.2. Evidence in legal proceedings

While much of the jurisprudence analysed so far focused on investigations and surveillance contexts, a different set of legal issues arises when FRT is deployed as a tool for generating evidence in criminal trials. Consider the case where FRT is deployed to establish a defendant’s presence at the scene of a crime, particularly in the absence of eyewitness testimony or other forms of traditional identification.

The use of FRT for evidentiary purposes still engages with Article 8 ECHR, as the processing of personal data for generating evidence constitutes an interference with the right to private life. This was explicitly acknowledged by the Court in *Glukhin v. Russia*, where the applicant’s facial image was extracted from publicly available videos and matched against a biometric database to identify the applicant and ultimately used in the administrative proceeding against him. Interestingly, the Court recognised that the use of FRT as evidence is a distinct and particularly intrusive form of data processing and must, therefore, be subject to a high level of justification under Article 8(2) ECHR.<sup>101</sup> What clearly emerges from *Glukhin v. Russia*

<sup>92</sup> *Akgün v Turkey* [2021] ECtHR 19699/18, paras. 167 and 175.

<sup>93</sup> *Merabishvili v Georgia* [2017] ECtHR [GC] 72508/13, para. 184.

<sup>94</sup> *Roman Zakharov v. Russia*, para. 260.

<sup>95</sup> *Ibid* para 259; *Glukhin v. Russia*, para. 83.

<sup>96</sup> *Glukhin v. Russia*, para 87; *P.N. v. Germany*, para. 72.

<sup>97</sup> *Murray v. the United Kingdom*, paras. 91-94.

<sup>98</sup> *Gardel v. France*, para. 6.

<sup>99</sup> *Peruzzo and Martens v. Germany*, paras. 6-13.

<sup>100</sup> *P.N. v. Germany*, para. 81 and *Peruzzo and Martens v. Germany*, paras. 37-38 both confirm that repeat offending or a high likelihood of reoffending contributes to the seriousness assessment. This applies even if the underlying offences, taken in isolation, might not be among the most serious.

<sup>101</sup> *Glukhin v. Russia*, paras. 68-73.

is that even when FRT is used to produce potentially inculpatory evidence, it remains subject to strict scrutiny under the proportionality principle of Article 8(2) ECHR. This principle demands that public prosecutors prefer other means of identification, such as eyewitnesses or low-tech solutions, over the use of FRT.

Besides Article 8 ECHR, the evidentiary use of FRT also raises distinct concerns under Article 6 ECHR, particularly with respect to the right to a fair trial, the equality of arms, and the right to examine or challenge evidence. While these concerns were not addressed in *Glukhin v. Russia*, the potential implications for Article 6 are significant and widely reported in the literature.

A critical point of concern is the opacity of facial recognition systems and AI systems more generally, especially when based on machine learning techniques.<sup>102</sup> Defendants may face substantial barriers in understanding how the evidence against them was generated, challenging the reliability of the technology, or cross-examining expert witnesses who interpret the FRT results.<sup>103</sup> This asymmetry of information has been largely problematised in legal scholarship as a challenge to the principle of equality of arms, particularly where defendants are unable to access the algorithmic processes, datasets, or accuracy metrics behind the automated identification.<sup>104</sup>

<sup>102</sup> On opacity, see the seminal work by J. Burrell, *How the Machine “Thinks”*: Understanding Opacity in Machine Learning Algorithms, in *Big Data & Society*, vol. 3, n. 1, 2016; F. Pasquale, *Inalienable Due Process in an Age of AI: Limiting the Contractual Creep toward Automated Adjudication*, in A. Reichman and others (eds.), *Constitutional Challenges in the Algorithmic Society*, Cambridge, Cambridge University Press, 2021.

<sup>103</sup> J.C. Celentino, *Face-to-Face With Facial Recognition Evidence: Admissibility Under the Post-Crawford Confrontation Clause*, in *Michigan Law Review*, vol. 114, n. 16, 2016, 1317; F. Palmiotto, *The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in M. Ebers and M. Cantero Gamito (eds.), *Algorithmic Governance and Governance of Algorithms*, Springer, 2020; A. Roth, *Machine Testimony*, in *Yale Law Journal*, vol. 126, 2017, 1972.

<sup>104</sup> More broadly on AI and fair trial rights see S. Quattrocchi, *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion*, Springer International Publishing, 2020; A. Sachoulidou, *Going beyond the “Common Suspects”: To Be Presumed Innocent in the Era of Algorithms, Big Data and Artificial Intelligence*, in *Artificial Intelligence and Law*, 2023; F. Palmiotto, *Artificial Intelligence and the Transformation of Criminal Trials: Preserving Fairness in Europe*, PHD Thesis, European University Institute, Florence, 2023;

The ECtHR has had limited opportunity to examine these issues in its case law, though it took a tentative step in *Sigurður Einarsson and Others v. Iceland*, the first case involving Artificial Intelligence systems in criminal proceedings.<sup>105</sup> The case concerned the use of an e-discovery system named Clearwell to analyse and filter evidence in the case file. The applicants complained that their defence had not been given access to the vast amount of data collected by the prosecution during the investigation phase and, among other things, were unable to have a say in the prosecution’s electronic sifting of that data to gather relevant information for inclusion in the investigation file. They maintained that no one had reviewed the prosecution’s cherry-picking of the documents submitted to the court and that they had been denied the possibility of carrying out a search using the e-discovery system. While the Court ultimately did not find a violation of Article 6 ECHR, the dissenting opinion criticised the majority for a “missed opportunity” to engage with the fairness implications of AI systems in criminal proceedings.<sup>106</sup>

Indeed, as facial recognition and other AI systems become increasingly integrated into criminal justice systems, there is an urgent need to develop a coherent jurisprudence that recognises both the informational asymmetries and potential inaccuracies inherent in such technologies. This will require a shift from viewing FRT solely as a privacy issue to also considering its implications for fair trial rights.

## 6. Conclusions

This article has shown that the case law of the European Court of Human Rights, when read holistically through the lens of the “Architecture of Surveillance”, significantly delimits the permissible scope of facial recognition technology under Article 8 ECHR. Each building block of FRT - namely the collection of input data, the creation and management of facial databases, and the use

A. Završnik, *Criminal Justice, Artificial Intelligence Systems, and Human Rights*, in *ERA Forum*, 2020; More specifically on information asymmetries, see the seminal work by R. Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, in *UCLA Law Review*, vol. 68, n. 1, 2021.

<sup>105</sup> *Sigurður Einarsson and Others v Iceland* [2019] ECtHR 39757/15.

<sup>106</sup> *Ibid.*, para 4 of the partly dissenting opinion of Judge Pavli.

of automated biometric matching - constitutes a distinct interference with the right to private life and, therefore, demands an independent assessment of proportionality.

Starting with *Glukhin v. Russia*, the only case in which the Court directly addressed facial recognition, the article has shown how the standard of justification varies depending on the function and context in which FRT is used. A key distinction must be drawn between real-time and post-remote uses of FRT. The Court has recognised the real-time use of FRT as the most intrusive form of biometric surveillance, which, accordingly, requires the highest level of justification. By contrast, post or retrospective uses of FRT - while generally regarded as less intrusive - still entail significant privacy implications and require a high level of justification. Finally, regarding the use of FRT as evidence in criminal proceedings, while the ECtHR has not yet fully addressed the implications under Article 6 ECHR, its decision in *Glukhin* recognised that the evidentiary use of biometric data is still subject to a strict proportionality assessment under Article 8 ECHR.

Besides *Glukhin*, the article has comprehensively reviewed leading cases related to surveillance, data collection and creation of police databases, as well as privacy interferences in law enforcement contexts. From this jurisprudence, we can derive the following normative principles that apply to FRT: the principle of extrema ratio, the principle of targeted suspicion and the principle of selective legitimacy.

The *principle of extrema ratio* states that facial recognition should only be used as a measure of last resort. This principle encapsulates the judgment of *Glukhin v. Russia*, where the Court explicitly recognised that FRT represents one of the most, if not the most, intrusive technologies available to law enforcement authorities nowadays.<sup>107</sup> The requirement of strict necessity also clearly emerged from the analysis of the Court surveillance jurisprudence. Therefore, to meet the necessity standard the use of FRT can only be considered if no other less intrusive means of identification are available. Less intrusive,

low-tech alternatives must always be preferred, and FRT should never become a standard practice in criminal investigations. More importantly, this principle applies to both real-time and post-remote FRT, despite the more lenient approach of the EU AI Act, towards the latter.<sup>108</sup>

The *principle of targeted suspicion* posits that facial recognition may only be based on specific, individualised suspicion. This principle reflects the extension of the standard of reasonable suspicion to law enforcement activities that are capable of interfering with the right to private life enshrined in Article 8 ECHR. In the case law analysed, the article has shown the insistence of the Court that any interference with privacy, such as stop-and-searches or data collection, must be grounded in concrete, verifiable facts capable of linking an individual to a previously committed offence. The application of this standard to FRT serves not only as a procedural safeguard but also as a categorical limitation on its use. FRT cannot, under any circumstances, be used pre-emptively or for general deterrence. As a result, the legitimate use of FRT is restricted to backwards-looking scenarios, excluding any deployment aimed at speculative identification or monitoring the population at large.

Finally, the *principle of selective legitimacy* requires that the collection of facial images as input data or storage in police databases be restricted to limited categories of data subjects. This principle is derived from the analysis of the Court's case law provided in Sections 3 and 4, which showed that the Court has imposed strict limitations on whose data may be lawfully collected and retained in databases. The Court has repeatedly stated that blanket or indiscriminate data collection practices are incompatible with Article 8 ECHR. In its case law, a consistent criterion used relates to the seriousness of the offence and the status of the data subject in the proceeding. Only individuals suspected or convicted of serious offences - such as terrorism, violent crimes, or sexual offences - may be legitimately included in databases, provided that strong safeguards against abuse and data protection rights are in place. It

<sup>107</sup> The Court also showed sensitivity to FRT in collection of facial images by law enforcement authorities, which, as the Court clarified in *Gaughran v. UK*, attract a heightened protection of privacy for the mere fact that FRT may be employed.

<sup>108</sup> Under the AI Act, only real-time remote biometric identification is subject to restrictive limits of use and safeguards. On the contrary, the use of post remote biometric identification is more widely permissible, despite being classified as high risk.

follows that the use of FRT for identification purposes is limited to individuals suspected or previously convicted of serious offences. In relation to minor offences, acquitted individuals, protesters, or those discharged from proceedings, the use of FRT for their identification fails to meet the required threshold of necessity in a democratic society.

Conclusively, these findings demonstrate that the ECtH's case law imposes strict normative constraints and doctrinal limits on the "Architecture of Surveillance" enabled by facial recognition. Provided that no other less intrusive means are available, the deployment of FRT by law enforcement can only be backwards-looking, targeted, and grounded in individualised suspicion of having committed a serious offence. Notably, these principles apply to both "real-time" and "post" remote uses of facial recognition.

