UDK 343.98:342.722
Original scientific paper

FACIAL RECOGNITION TECHNOLOGY IN EU CRIMINAL JUSTICE - HUMAN RIGHTS IMPLICATIONS AND CHALLENGES*

Ante Novokmet, PhD, Associate Professor
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
Stjepana Radića 13, Osijek, Croatia
ante.novokmet@pravos.hr

Zvonimir Tomičić, PhD, Associate Professor
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
Stjepana Radića 13, Osijek, Croatia
tomz@pravos.hr

Ivan Vidaković, Master of Laws, Teaching Assistant
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
Stjepana Radića 13, Osijek, Croatia
ivan.vidakovic@pravos.hr

ABSTRACT

This paper considers the legal justification for the application of various advanced systems of facial recognition technology for the purpose of initiating and conducting criminal proceedings. Therefore, the theoretical foundations and minimum European standards are first analyzed as a basis for the deployment of various facial recognition technology (hereinafter: FRT) systems in practice of law enforcement agencies. Then the legislative framework of selected European countries that have already established certain forms of FRT in criminal proceedings are presented. The experiences and legal consequences of the application of such systems are analyzed, and the first decisions of the judiciary on the admissibility of the results of actions and measures based on FRT as evidence in criminal proceedings are presented. Finally, the existing normative solutions are critically reviewed and, based on common European standards established to protect citizens from the repressive power of state bodies, the minimum conditions that must be

* This article is a product of work that has been fully supported by the Faculty of Law Osijek Josip Juraj Strossmayer University of Osijek under the project IP-PRAVOS-18 'Artificial intelligence and criminal law'.

met in order to harmonize the use of FRT with the basic principles of contemporary European criminal proceedings are proposed.

***Keywords**: artificial intelligence, criminal proceedings, Facial recognition, fair trial, in dubio pro reo, presumption of innocence*

1. INTRODUCTION

In recent years, various systems of biometric technology based on artificial intelligence have settled into the daily reality and become a part of generally accepted everyday living.[1] Today, due to their mostly benign nature and ease of use, various biometric technologies are widely used in order to carry out the identification and verification of a specific person based on a verifiable and unique set of data, among which fingerprint recognition, signature recognition, voice recognition, etc. can be mentioned.[2] Among them, facial recognition technology (FRT) has become particularly popular in everyday life as a biometric technology aimed at verification (matching the passport photo during border control), identification (comparison of a photo of a certain person with a large database of photos) and categorization of individuals taking into account their personal characteristics such as age, gender, etc.[3]

All the mentioned techniques aim to profile a person, taking into account the facial appearance in order to determine the identity, gender, age, and race, but also to determine certain gestures or the emotional state of a person.[4] Although the FRT technology itself is not so new, it has gained importance with the development of modern software solutions that, through the use of advanced artificial intelligence systems, enable a computer program to search a large amount of data precisely and almost instantly in order to achieve the set purpose. At the same time, with the prior and informed consent of a person, such a simple and benign way of profiling is used to facilitate and speed up a series of regular private and

---

1 Yassin, K.; Jridi, M.; Al Falou, A.; Atri, M., *Face Recognition Systems: A Survey*, Sensors Vol. 2., No. 2., 2020, pp. 1-36, [https://doi.org/10.3390/s20020342].

2 Kak, A., *The State of Play and Open Questions for the Future*, in: Kak, A. (ed) Regulating Biometrics: Global Approaches and Urgent Questions. AI now Institute, pp. 16-43, available at: [https://ainowinstitute.org/regulatingbiometrics.html], Accessed 20 June 2022.

3 Buolamwini, J.; Ordóñez, V.; Morgenstern, J.; Learned-Miller, E., *Facial Recognition Technologies: A Primer*, Algorithmic Justice League., 2020, p. 5, available at: [https://assets.websitefiles.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf.], Accessed 28 July 2022.

4 Park, SJ.; Kim BG.; Chilamkurti, N., *A Robust Facial Expression Recognition Algorithm Based on a Multi-Rate Feature Fusion Scheme*, Sensors Vol. 21, No. 21., 2021, p. 2, [https://doi.org/10.3390/s21216954].

business activities such as various consumer applications, business and payment applications, and surveillance and access control in different areas.[5]

However, contemporary development of FRT has opened up space for a new, faster, and more advanced way of acting, on the basis of which law enforcement agencies, using the advantages of FRT based on artificial intelligence, solve criminal offenses and discover perpetrators of criminal offenses. A typical example of this progress can be seen on the basis of surveillance camera footage that the police regularly take at the crime scene to discover the perpetrator of criminal offenses.[6] With the classic method of search, a police officer examines the footage in question and tries to determine the identity of the person from the footage based on a manual comparison of the footage with the pictures in police databases. On the other hand, the use of advanced FRT solutions based on artificial intelligence allows the recording to be reviewed by a computer program using advanced review capabilities and much faster than a human is capable of.[7] Therefore, it is common to hear today that many law enforcement agencies in certain countries have already developed highly sophisticated solutions aimed at the faster identification of previously known perpetrators of criminal offences as well as solutions by which FRT is used as a predictive method in the detection of other, previously unknown perpetrators of criminal acts.[8]

On the one hand, it is a completely legitimate expectation of the community that the state must have at its disposal effective means for deterring, detecting and finding the perpetrators of criminal offences, the question of compliance of the FRT with the unquestionable standards of protection of fundamental human rights and freedoms appears to be a stumbling block for its implementation in contemporary criminal proceedings.[9] Since the FRT system is based on a specially programmed software solution that uses a given database, the key question is how

---

5 Rowe, EA., *Regulating Facial Recognition Technology in the Private Sector*. Stanford Technology Law Review Vol. 24, No. 1. 2020, pp. 9-19.

6 Raposo, VL*, The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal*, European Journal on Criminal Policy Research, 2022, p. 14., [https://doi.org/10.1007/s10610-022-09512-y].

7 Dushi, D., *The use of facial recognition technology in EU law enforcement: Fundamental rights implications*, Policy Briefs, 2020, available at: [https://tinyurl.com/3dnc69j3], Accessed 28 July 2022.

8 Kayser-Bril, N., *At least 11 police forces use face recognition in the EU*, AlgorithmWatch, 2020, available at: [https://algorithmwatch.org/en/face-recognition-police-europe/], Accessed 15 July 2022.

9 Sarabdeen, J., *Protection of the rights of the individual when using facial recognition technology*, Heliyon, Vol. 8, No. 3., 2022, pp. [https://doi.org/10.1016/j.heliyon.2022.e09086]; Ritchie, KL., Cartledge, C., Growns, B., Yan, A., Wang, Y., *et al.*, *Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world*. PLOS ONE, Vol. 16, No. 10, 2022., p. 2, [https://doi.org/10.1371/journal.pone.0258241].

this data was collected, systematized and adapted to a specific purpose. This is important because wrongly pre-set instructions on the basis of which the system performs certain operations can produce incorrect identifications that result in biased decisions on the basis of which groups of people can be discriminated[10] and also consequently make decisions that can result in initiating and conducting criminal proceedings against an innocent person.[11] The question arises, under what conditions and circumstances can such profiling systems be used for the purposes of initiating and conducting criminal proceedings? Is such profiling necessary and appropriate in a democratic society? How can independent and objective control over the use of such systems be ensured? Does the legal system provide control of the legal consequences that have occurred as well as effective legal means by which the affected person can *ex post facto* request an independent and objective judicial review of the legality of the actions taken? The above questions are based on the democratic legal standards of legitimacy, necessity and proportionality as fundamental common values of the European judicial area developed in the practice of the ECtHR and accepted in EU law.

Despite the strong opposition of numerous non-governmental organizations[12] requesting to ban FRT and the very restrictive stance of the European Parliament[13], it is simply not realistic to expect that the EU will prohibit FRT technologies for the purposes of criminal proceedings.[14] Even if this were to happen, it would not be possible to provide solid guarantees or preventive mechanisms that would make it impossible for law enforcement bodies to secretly and covertly use such advanced systems in order to fight against modern criminal offences. For this reason, it is necessary to establish a solid normative framework that, while appreciating European legal standards for the protection of fundamental human rights and freedoms, will determine an acceptable limit of minimum conditions that must be

---

10 Bacchini, F.; Lorusso, L., *Race, again: how face recognition technology reinforces racial discrimination*, Journal of Information Communication and Ethics in Society, Vol. 17, Issue 3, 2019, pp. 321-335, [http://dx.doi.org/10.1108/JICES-05-2018-0050].

11 Stoykova, R., *Digital evidence: Unaddressed threats to fairness and the presumption of innocence*, Computer, Law & Security Review, Vol. 42, 2021, pp. 1-20, [https://doi.org/10.1016/j.clsr.2021.105575].

12 Big Brother Watch, *Stop Facial Recognition,* 2020, available at: [https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/#breadcrumb], Accessed 15 June 2022.

13 European Parliament, *Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*, 2020/2016(INI), 2021, available at: [https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html], Accessed 18 June 2022.

14 Wired, *Europe Is Building a Huge International Facial Recognition System*, 2020, available at: [https://www.wired.com/story/europe-police-facial-recognition-prum/], Accessed 16 June 2022.

met in each specific case in order to secure that FRT for the purposes of criminal proceedings would be legitimate, necessary and balanced in democratic society.

Therefore, this paper first theoretically considers the legal justification of the application of FRT in the operation of law enforcement agencies and analyzes the current normative framework established at the EU level that governs the application of FRT for the purposes of criminal proceedings. Then it presents the legislative framework of selected European countries that have already established certain forms of FRT in criminal proceedings, analyzes the experiences and legal consequences of the application of such systems, and presents the first reactions of the judicial system on the permissibility of using the results of actions and measures based on FRT as evidence in criminal proceedings. Finally, the existing normative solutions are critically reviewed and, based on common European standards established to protect citizens from the repressive power of state bodies, the minimum conditions that must be met in order to harmonize the use of FRT with the basic principles of contemporary European criminal proceedings are proposed.

2. MINIMUM EUROPEAN STANDARDS AS A GUIDE FOR REGULATING FRT FOR THE PURPOSES OF CRIMINAL PROCEEDINGS

The way in which contemporary criminal procedural law is going to shape the legal basis for the permitted use of FRT in the investigation of criminal offenses is directly related to the standards developed in the law of the Council of Europe and the law of the European Union. These standards, on the one hand, refer to the right to protection of personal and family life prescribed in Art. 8. ECHR and Art. 7 CFR, and on the other hand, they refer to the protection of personal data guaranteed in accordance with Art. 7. CFR and Art. 8. ECHR. Simultaneously, Directive (EU) 2016/680 addresses 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.[15]

---

[15] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, available at: [https://eur-lex.europa.eu/legal content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=HR.], Accessed 18 June 2022.

2.1. Right to respect for private and family life and data protection in ECHR

As already mentioned, the use of FRT presupposes the collection and processing of the biometric data of a specific person, which may consequently lead to interference with the right to private and family life and the protection of personal data prescribed in Art. 8. ECHR.[16] In general, Art. 8. of the ECHR excludes government interference in respecting private and family life except when it is in accordance with the law and when it is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country to prevent disorder or crime, to protect health or morality or to protect the rights and freedoms of others.[17] For this reason, certain minimum standards have been developed in the practice of the ECtHR in order to establish minimum preconditions for its deployment. In addition to respect for the rule of law, predictability is an important requirement.[18] In order for this requirement to be fulfilled, it is necessary that the legislative solution clearly prescribes the preconditions under which restrictions can occur so that the individual is informed of the circumstances and conditions under which the state authorities are authorized to take such measures that limit his rights and freedoms. Therefore, it is precisely why the use of FRT in the process of detection, investigation and prosecution of criminal offenses has come under the recent supervisory activity of the ECtHR. One of the first cases in which the ECtHR considered the legality and proportionality of the use of FRT in criminal proceedings is the case of *Gaughran v. The United Kingdom*.[19] Starting from unquestionable criteria such as the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained, the Court found that domestic authorities violated the applicant's right to privacy guaranteed by Art. 8. ECHR because the photograph obtained during the arrest was retained indefinitely in the police database, and the police were able to subject the photograph to advanced facial recognition and facial mapping techniques. Therefore, the Court found that the taking and retention of the applicant's photograph amounted to an interference with the right to one's image.[20] It went on

---

16 Callanan, G., *Does the Right to Privacy Apply to Facial Biometrics? Specifically, When Analyzed Under the European Convention on Human Rights*, Georgia Journal of International & Comparative Law, Vol. 49, 2021: pp. 358-368.

17 European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence*, 2022, available at: [https://www.echr.coe.int/documents/guide_art_8_eng.pdf.], Accessed 15 June 2022.

18 *Ibid.*

19 Judgment *Gaughran v The United Kingdom* (2020) EHRR, No. 45245/15, 13 February 2020, § 40-49.

20 Judgment *Gaughran v The United Kingdom* (2020) EHRR, No. 45245/15, 13 February 2020, § 70.

to find that the interference was not necessary in a democratic society[21], following the reasoning that the right to the protection of one's image is one of the essential components of personal development and presupposes the right to control the use of that image.[22] The ECtHR took a somewhat different position regarding the retention of an individual's photograph in police records in the case of *P.N. v. Germany*[23], pointing out that there was no violation of the right from Art. 8. ECHR. Namely, the court made such a conclusion after previously determining that the retention of the photograph was limited to a period of five years, that the domestic court conducted an individual assessment of the probability that the applicant could commit a criminal offense again in the future, and that it was ensured control (review) of the need for further retention of the data in question.[24]

The European Court of Human Rights already encountered issues in its practice of using algorithms and artificial intelligence as important technological steps forward in the detection of criminal offenses and, accordingly, the interception, collection and storage of private data for crime-prevention purposes.[25] Therefore, considering the scope of the powers of state authorities to encroach on the rights and freedoms of individuals, it pointed out that with regard to fingerprints, biological samples and DNA profiles of persons suspected or convicted of criminal offenses, the use of modern scientific techniques cannot be authorized at any cost or without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.[26] For this reason, every newly developed technology obliges the state to first conduct a test of the proportionality of its use for crime prevention and prosecution purposes.[27] The court particularly highlighted this in relation to FRT. Besides, it emphasized that facial recognition and facial mapping techniques represent an undoubted encroachment on the rights and freedoms of individuals, which has multiple effects because it affects not only the taking of their photographs, but also the storage and possible dissemination of the resulting data. That is why domestic courts must take these factors into account when weighting the necessity and proportionality of any interference that

---

21 Judgment *Gaughran v The United Kingdom* (2020) EHRR, No. 45245/15, 13 February 2020, § 90.

22 Judgment *Reklos and Davourlis v Greece* (2009) EHRR, No. 1234/05, 15 January 2009 § 40-43.

23 Judgment *P. N. v Germany*, (2020) EHRR, No. 74440/17, 11 June 2020.

24 Judgment *P. N. v Germany*, (2020) EHRR, No. 74440/17, 11 June 2020, § 76-90.

25 European Court of Human Rights, *Guide to the Case-Law of the European Court Human Rights – Data protection*, 2022, available at: [https://echr.coe.int/Documents/Guide_Data_protection_ENG.pdf.], Accessed 20 June 2022.

26 Judgment *S. and Marper v. the United Kingdom* (2008) EHRR, No. 30562/04 and 30566/04, 4 December 2008, § 112.

27 Judgment *S. and Marper v. the United Kingdom* (2008) EHRR, No. 30562/04 and 30566/04, 4 December 2008, § 112.

facial recognition and facial mapping techniques represent for the private life and private data of the person concerned.

There are multiple possible ways in which Art. 8 of the ECHR can be infringed, as elucidated by the court in the case of *Peck v. United Kingdom*. In this particular instance, it was determined that the act of conducting video surveillance in public areas, wherein visual information is captured, subsequently stored, and disclosed to the public, falls within the purview of Article 8.[28]

2.2. Right to respect for private and family life and data protection in CFR

Just like in Convention law, the processing of personal data for the purpose of prevention, investigation, detection and prosecution of serious crime, such as organized crime and terrorism, interferes with the fundamental rights guaranteed in the CFR, primarily, respect for private life and communications under Article 7 and 8 of the Charter.[29] Simultaneously, it is important to point out that the data processing calls into question the compliance of the performed action with the requirements of Art. 7 and 8, regardless of whether it led to a "positive outcome", and even when, after a comparison with the police databases, the personal data was deleted from the records.[30] It follows that the CFR does not exclude the possibility of using FRT as an advanced investigative technique to detect criminal offenses and perpetrators but sets minimum standards that must be met in each specific case. Thus, Art. 52 (1) CFR provides that any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.[31] Therefore, four fundamental conditions must be met for any measure or action based on the application of the FRT in criminal

---

[28] Judgment *Peck v. United Kingdom* (2003) EHRR, No. 44647/98, 28 January 2023, § 57-63; see also Bu, Q. *The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges*, International Cybersecurity Law Review, Vol. 2, p. 117, 2021, [https://doi.org/10.1365/s43439-021-00022-x].

[29] O'Flaherty, M., *Facial Recognition Technology and Fundamental Rights*, European Data Protection Law Review, Vol. 6, Issue 2, pp. 170-173, [https://doi.org/10.21552/edpl/2020/2/4].

[30] European data protection board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, 2020, available at: [https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.], Accessed 20 June 2022.

[31] Nesterova, I., *Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world*, The 19th International Scientific Conference Globalization and its Socio-Economic

proceedings to be considered compliant with EU law: such a measure or action must be based on law; respect the core of guaranteed rights; have a legitimate aim; and fulfill requirements for necessity and proportionality.[32]

"Based on the law" implies not only the obligation to prescribe a specific FRT measure or action, but the prescribed measure must be sufficiently clearly defined so that citizens are informed in advance of the conditions under which state authorities are authorized to collect and process their data.[33] Setting up from the fact that FRTs are based on artificial intelligence and that each such system has its own specifics regarding the processing of personal data, the requirement of the clearly determined legal norm presupposes the obligation to prescribe the conditions and methods of its application in order to ensure sufficient guarantees of respect for the fundamental rights of citizens.

Respect for the core of guaranteed rights presupposes the obligation of domestic authorities that the prescribed FRT measure. Even though its implementation legitimately encroaches on the fundamental right, domestic authorities must essentially ensure respect for the essence of that right. Thus, for example, a violation of the core of the guaranteed right would exist through a provision that imposes restrictions regardless of the individual behavior of the person or exceptional circumstances[34] when the person affected by the measure would not have the guaranteed right to access the court in order to demand a review of the applied measure due to non-compliance with the basic principles of personal data protection, i.e., protection of the security of personal data.[35]

Legitimate aim implies that an intervention in the rights and freedom of an individual can be accepted in the community as legitimate only if it is aimed at protecting beliefs about the value on which rests the legal norm that justifies the intervention.[36] Therefore, the application of the FRT for the purposes of initiating and conducting criminal proceedings can achieve this legitimate goal only if they protect values such as the interest of state security, public order and peace, the economic well-being of the country, the prevention of disorder and crime, the protection of health or morals, and the protection of rights and the freedom of

Consequences 2019 – Sustainability in the Global-Knowledge Economy, 2020, SHS Web Conferences Vol. 74, pp. 1-8, [https://doi.org/10.1051/shsconf/20207403006].

32 Madiega, T.; Mildebrath, H., *Regulating facial recognition in the EU. European Parliamentary Research Service, 2020*, p. 10., available at: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf], Accessed 15 August 2022.

33 European data protection board, *loc. cit.*, note 30.

34 *Ibid.*

35 *Ibid.*

36 Krapac, D., *Kazneno procesno pravo*, Narodne novine, 2015, Zagreb, pp. 304-305.

other people. Therefore, it is about the general interests of the European Union, that is, the rights and freedoms of individuals protected by the law of the EU and individual member states.[37]

The criteria of *necessity and proportionality* set the requirement that the specific legislative activity aimed at implementing the FRT must be suitable for the achievement of a legitimate goal.[38] Namely, no matter how vehemently the public expresses interest in the need to apply the FRT in a specific case, this does not justify encroaching on the rights and freedoms of an individual at any cost. Therefore, any limitation of freedoms and rights must be evaluated taking into account the nature of the need for limitation in each specific case and only as far as it is absolutely necessary. Hence, the application of FRT for the purposes of criminal proceedings should be proportional to the severity of the criminal offense in such a way as to determine a narrow catalogue of criminal offenses in which the application of such a measure is justified and necessary.[39] Therewith, the person whose rights and interests are affected by the application of such a measure must be provided with sufficient guarantees that his personal data will be protected against any form of abuse and other unauthorized access. This, in turn, means that the national legal order must clearly prescribe the material and procedural prerequisites for the application of the FRT in order to be able to carry out an objective and independent control of the legality and justification of restrictions on individual rights for the purposes of initiating and conducting criminal proceedings.

2.3. Law enforcement directive (Directive (EU) 2016/680)

Taking into account the abstract legal standards established at the level of the ECHR and CFR, it is clear that any use of the FRT for the purposes of initiating and conducting criminal proceedings against a specific person leads to an encroachment on the rights and freedoms of the individual, which consequently manifest as interferences of Art. 7. CFR (right to data protection) and Art. 8. CFR (right to private life). Equally, the standards specified in Art. 52(1) CFR represent the minimum conditions that must be met in any case in order for advanced technological solutions based on FRT to be considered compliant with European legal standards.

When it comes to the processing of personal data by competent authorities for the purpose of initiating and conducting criminal proceedings, the basic regulation

37 European data protection board, *loc. cit.* 30.

38 *Ibid.*

39 *Ibid.*

that elaborate the abstract requirements established at the CFR level is Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties and on the free movement of such data, repealing Council Framework Decision 2008/977/JHA (hereinafter: LED). It is a fundamental regulation that determines the minimum European standards for the processing of personal data from competent state authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (Art. 1(1) and 2(1) LED). However, it should be noted that the scope of application of the LED directive is wider; it not only includes prevention, investigation, detection and prosecution of criminal offenses, but also police activities that are undertaken without prior knowledge as to whether an incident is a criminal offense or not (LED, rec. 12). In this sense, it should be noted that the LED directive provides basic principles that must be respected in each member state in relation to the processing of personal data[40], and they shall be respected equally when it comes to different FRT systems that must be a) lawful, fair and transparent; b) follow a specific, explicit and legitimate purpose; c) comply with the requirements of data minimization, data accuracy, storage limitation, data security and accountability.[41]

2.3.1. Lawful

In order to secure the legal application of the FRT for the purposes of criminal proceedings, it is necessary that the legislative solution is established on the law of the European Union or the law of a member state and that its application is necessary and reaches only to the extent necessary for the competent authority to perform the tasks which achieve the purpose of personal data processing (Art. 8(1) LED). However, since the use of FRT processes data related to the physical, psychological and behavioural characteristics of a person, it is mandatory to follow Art. 10 LED, which determines the criteria for processing special categories of data only if it is strictly necessary and subject to appropriate safeguards for the

---

40 Leiser, MR.; Custers; BHM., *The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680*. European Data Protection Law Review, Vol. 5, Issue 3, pp. 367-378, [https://doi.org/10.21552/edpl/2019/3/10].

41 Madiega; Mildebrath, *op. cit.* note 32, pp. 15-17.

rights and freedoms of the data subject.[42]The application of FRT in the framework of law enforcement agencies primarily infringes on the highest values of the community. The violation of these values is protected by criminal law, which criminalizes certain behaviours that violate these values. Thus, it is clear that the legal basis for regulating FRT for the purposes of criminal proceedings is domestic legislation which prescribes the conditions and prerequisites for initiating and conducting criminal proceedings (i.e., criminal procedure code), legislation that regulates the organization and scope of authority of various bodies participating in criminal proceedings (i.e. the police), special laws that regulate the procedure for certain groups of the most serious criminal offenses (i.e. organized crime). However, the legal foundation for the application of FRT in criminal proceedings is not sufficient in itself. It is necessary for the domestic regulation to be clear, precise and concrete in order to avoid complaints of excessively broad discretionary powers of the police in the application of the FRT for the purposes of initiating and conducting criminal proceedings.[43]

2.3.2. Fair

Ensuring the principle of fairly conducted procedure refers to the ubiquitous tendency to limit the excessive repression of state bodies by prescribing guarantee forms and minimum rights of defence in various stages of the criminal procedure.[44] Therefore, it can be claimed that the fairness of the procedure primarily refers to contriving the right balance between powers of state criminal justice bodies (state attorney's office and police) and procedural rights of suspects or defendants in criminal proceedings. In the context of the application of the FRT for the purpose of initiating and conducting criminal proceedings, it is crucial that the suspect or defendant be informed in a timely, clear and comprehensible manner about the results of the FRT actions carried out in this way. That moment coincides with the moment when the suspect acquires the procedural position in accordance with Art. 2(1) of the Directive on the right of access to a lawyer in criminal proceedings in accordance with procedural solutions after the transposition of the Directive (hereinafter: Directive 2013/48/EU). At that moment, the suspect realizes

---

42 Neroni Rezende, I., *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, New Journal of European Criminal Law, Vol. 11, Issue 3, p. 387, [https://doi.org/10.1177/2032284420948161].

43 Madiega; Mildebrath, *op. cit.* note 32, pp. 18-21.

44 De Hert, P.; Sajfert, J, *The Role of the Data Protection Authorities in Supervising Police and Criminal Justice Authorities Processing Personal Data*. In: Brière C, Weyembergh A (eds) The Needed Balances in EU Criminal Law, Hart, Oxford and Portland, Oregon, 2018, pp. 243-257; Hacker, P., *Teaching fairness to artificial intelligence*, Common Market Law Review Vol. 55, Issue 4, 2018, pp. 1143 – 1185, [https://doi.org/10.54648/cola2018095].

the right to be informed about the criminal offense he is charged with, as well as the reasons from which arose the grounds for suspicion that he has committed a criminal offense.[45] Thereby, the suspect acquires the procedural rights of defence and the possibility to contradict the implemented actions based on the FRT as well as to use other procedural rights to contest the possible illegality of its results. Although the real implementation of FRT technology is still rudimental in most countries, the principle of procedural fairness must be a fundamental binding factor that must be followed in order to prevent any abuse of FRT to the detriment of the procedural rights of the defence.

2.3.3. Transparent

The question of the transparency of the criminal justice system is reflected in the quest for an ideal balance between the aspiration for the efficiency of the criminal proceedings and the aspiration for the protection of fundamental rights and freedoms of the individual.[46] Namely, excessive tightness and secrecy of law enforcement agencies' actions opens the door to arbitrary and malicious treatment. On the other hand, the excessive openness of the judiciary and the disclosure of all information in the earliest stages of criminal proceedings calls into question the possibility and ability of the state to successfully fight against various forms of criminal offences.[47] The FRT is primarily applied within the framework of the police's research and investigative activities. In the earliest phases of criminal proceedings, which are by nature secret, any unilateral insisting on the disclosure of all information about the type and nature of police actions and measures would lead to the paralysis of the justice system. Therefore, the provision of Art. 13. LED that imposes an obligation on the controller to inform in advance the data subject is meaningful and applicable in the situation when FRT is used in public places (streets, squares, stadiums, etc.) where a large fluctuation of people is expected. FRT is used in these cases primarily as a means of deterring the commission of criminal offenses or as an aid in the subsequent detection of perpetrators of criminal offenses.[48] Therefore, the request for ex ante information is acceptable,

---

45 Novokmet, A., *The Europeanization of the Criminal Proceedings in the Republic of Croatia through the Implementation of the Directive 2013/48/EU*. European Journal Crime Criminal Law and Criminal Justice, Vol. 27, No. 2., pp. 112-115, [https://doi.org/10.1163/15718174-02702002].

46 Bibas, S., *Transparency and Participation in Criminal Procedure*. New York University Law Review, Vol. 81, No. 3, 2006, pp. 911-966.

47 De Hert, P.; Papakonstantinou, V., *The New Police and Criminal Justice Data Protection Directive, A first analysis*. New Journal of European Criminal Law Vol. 7, Issue 1, 2016, pp. 7-19., [https://doi.org/10.1177/203228441600700102].

48 Kotsoglou KN.; Oswald M., *The long arm of the algorithm? Automated Facial Recognition as evidence and trigger for police intervention*, Forensic Science International: Synergy, Vol. 2, pp. 86-89. [https://

and citizens should be aware that video surveillance is being carried out in certain public spaces, which can later be used for automatic data processing in accordance with Art. 13 (1) (2) LED. On the other hand, in a situation where the police, in the process of investigating criminal offenses, use photographs or recordings obtained from the surveillance system to identify perpetrators of criminal offenses by comparing the obtained photograph/recording with police databases in order to identify a specific person as a possible perpetrator of a criminal offense, such prior notification is not possible and falls under the regime of Art. 13 (3) (b) LED in which situation it is possible to delay, restrict or omit the information to the data subject to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offenses or the execution of criminal penalties. However, in such a situation, it is absolutely necessary to ensure that the aforementioned delay in the notification of rights is carried out only as a necessary and proportionate measure with due regard for the fundamental rights and the legitimate interests of the natural person concerned (Art. 13 (3) LED). In these cases, notification may follow ex post at the moment when a person acquires the position of a suspect in criminal proceedings in accordance with Art. 2 (1) of Directive 2013/48/EU on the right of access to a lawyer in criminal proceedings. In any case, subsequent notification entails the necessity of establishing an adequate ex post control mechanism of the legality of the implemented measures and the need to ensure the right to an effective legal remedy in order to respect the fundamental rights of defence.

2.3.4. Specific, explicit and legitimate purpose

One of the key standards for the validity and legal use of FRT for the purposes of criminal proceedings is strict compliance with the principle of legality (*nullus actus sine lege*). It specifically prescribes the requirement that any interference by state authorities in the rights and freedoms of individuals must be based on the norm of legal rank.[49] Therefore, this principle prohibits the introduction of new restrictions on the fundamental rights and freedoms of citizens in criminal proceedings by referring to "necessity", "purposefulness", etc. However, it is not enough to prescribe the possibility of using some FRT measure for the purposes of criminal proceedings only by a norm of legal rank. It is absolutely necessary that the legal provision determines, with a sufficient degree of precision, the scope and manner of exercising the authority of state bodies while respecting the legitimacy of the goal that is to be achieved.[50] Therefore, the provision of Art. 4(1) b LED that data collected with the help of FRT can only be collected if they are collected for

doi.org/10.1016/j.fsisyn.2020.01.002].

49 Krapac *op. cit.* note 36, p. 306.

50 Madiega; Mildebrath, *op. cit.* note 32, p. 33.

specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes should be interpreted in such a way that the domestic legal order must more precisely determine not only the prerequisites for the application of FRT, but also its content and scope of application. This is the only way to avoid discrimination on any basis, ensure the equality of all citizens before the law, and simultaneously ensure that the person to whom the application of the FRT measure applies can foresee with a sufficient degree of certainty the purpose for which his data is being processed.[51]

2.3.5. Adequate, accurate, time-limited, data security and accountability

The LED directive in Art. 4(1)c prescribes an important requirement that the data collected is adequate, relevant and not excessive in relation to the purposes for which they are processed. In other words, emphasis was placed on the sufficiency of data collection in a manner that only those data which are relevant are collected, taking into account the purpose that will be achieved in collecting data. This specifically means, when it comes to a photo or video images, that for the purposes of criminal proceedings, only the part of the recording that is absolutely necessary should be used, and everything that is not useful should be blurred or anonymized in a way such as to prevent the subsequent use of that data.[52]

Like any other technology developed and operated by humans, FRT can produce reliable and accurate results only to the extent that the input data on which FRT performs its activity is accurate and reliable.[53] Therefore, the directive in Art. 4(1) d sets an important requirement that data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. This is particularly significant in the context of criminal proceedings since the FRT, based on wrong or incorrectly entered data, could discriminate against certain persons with regard to race, skin color, gender, age, etc.[54] It should not be forgotten that FRT does not always produce a 100% accurate result but operates on the basis of a certain degree of probability that, for example, the face from the photo and the face in the police database would

---

51 *Ibid.*

52 *Ibid.*

53 Hill, D.; O'Connor, CD.; Slane, A., *Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making*, International Journal of Police science & management, Vol. 24, Issue 3., pp. 327-331, [https://doi.org/10.1177/14613557221089558].

54 Dessimoz, D.; Champod, C., *A dedicated framework for weak biometrics in forensic science for investigation and intelligence purposes: The case of facial information*. Security Journal, Vol. 29, 2016, pp. 603–617. [https://doi.org/10.1057/sj.2015.32].

correspond to the same person. Therefore, it is necessary to ensure ex post human supervision in order to eliminate the danger of possible bias in the treatment based on the results produced by the FRT.

The directive also contains an important provision on the time limit for data storage and stipulates that collected data must not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which they are processed (Art. 4(1)e). In this way, the directive introduces a kind of proportionality in the time retention of personal data and sets a requirement to establish a system of weighing the interests of data retention for the purposes of criminal proceedings and the interest of a person that his/her data is not affected by the data retention measure more than is absolutely necessary. In practice, for example, time limits for data retention have already been established at the level of recommendations, so it is emphasized that a period of three days, or 72 hours, is sufficient to reach a conclusion on whether the collected data should be retained for a longer period of time.[55] On the other hand, it is legitimate and quite understandable that in the case of more serious criminal offences that threaten organized life in society (human trafficking, drug smuggling), the retention of data may be prolonged, taking into account the need to implement special investigative techniques (secret monitoring, wiretapping etc.) in the detection of the criminal offence and the perpetrator.

One of the most sensitive challenges that needs to be resolved in order to ensure the credibility of the results obtained using FRT for the purposes of criminal proceedings is certainly the proper level of data processing security. Namely, it is necessary to ensure that the data is processed in a manner that ensures the appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (Art. 4(1)f LED). This request can only be met by a concrete procedural norm that will determine the persons authorized to act and deal with the collected data as well as the legal consequences of their disclosure to unauthorized persons. Certainly, it is necessary to take into account that any previous or subsequent manipulation of the data obtained through FRT technology entails the invalidity of the evidence collected in this way, and as a result, exclusionary rule on illegally obtained evidence is applied; such results cannot be used as evidence in criminal proceedings. Therefore, it is necessary to provide sufficient guarantees during the entire data processing that the collection, transfer and processing of data is protected from any external influences that could

[55] Madiega; Mildebrath, *op. cit.* note 32, p. 15.

compromise these data, which would result in the impossibility of using it as evidence in criminal proceedings.[56]

The last but not least important standard is the question of the responsibility of the data controller for compliance with the basic principles for the processing of personal data. The directive thus expressly prescribes the obligation to implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this directive (Art. 19(1) LED). In doing so, it is necessary to place special emphasis on the assessment of the impact on the protection of personal data when it comes to systems that represent a high risk for the rights and freedoms of individuals. There is no doubt that such a high risk is indeed represented by FRT systems developed for the purposes of criminal proceedings, because not only does their application represent a significant encroachment that limits fundamental human rights and freedoms, but also, the results of such actions can be used as evidence in criminal proceedings[57], before the implementation of the FRT itself, for the purposes of criminal proceedings, it is necessary to carry out a targeted risk assessment for the rights and freedoms of the respondents, foreseen risk measures, protective and security measures, and mechanisms to ensure the protection of personal data and proof of compliance with this directive (Art. 27(2) LED).

3. CONTEMPORARY FRT SYSTEMS IN EUROPE – RECENT DEVELOPMENTS

The presence, testing, and use of FRT is not new in Europe. Many countries have been using this technology for many years, primarily applied in the area of criminal law, but examples of the use of FRT in other areas of everyday life such as education and transport are becoming more and more common.[58] However, some countries are leading the way in terms of the use of new technologies, both in quality and quantity. One of the indicators is certainly the use of mass surveillance systems that can easily apply FRT. China and the USA continue to dominate in terms of the presence and use of mass surveillance and FRT, but European countries, following the trends of global leaders, have significantly increased the presence of the aforementioned technologies.[59]

---

56 *Ibid.*

57 *Ibid.*

58 Gentzel, M., *Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy*, Philosophy & Technology, Vol. 34, 2021, p. 1639.

59 See: Bischoff, P., *Facial Recognition Technology (FRT): 100 countries analyzed*, available at: [https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/], Accessed 15 July 2022.

3.1. Wales

The UK is one of the countries with the largest number of CCTV cameras in relation to the number of inhabitants in the world; London is one of the most surveilled cities in the world and one of the first that connected CCTV cameras to facial recognition software.[60] Therefore, it is not surprising that Wales and other countries of the UK followed the aforementioned trends and tested FRT. South Wales Police is the leading UK national authority in testing and conducting trials of automated facial recognition (hereinafter: AFR), and after the procurement process and tender, AFR software developed by NEC, called NeoFace Watch software, was chosen based on quality and money-for-value criterion.[61] AFR Locate software is a type of FRT used by the South Wales police that attracted a lot of public attention and ultimately led to a court epilogue. Deployment of AFR Locate includes usage of CCTV cameras that police mount on vehicles (mostly vans), poles, or posts that are suitable for capturing images of faces of people that are passing within range of the mounted cameras. Those digital pictures are processed in real-time to extract facial biometric information and compare it with facial biometrics of persons that are placed on a watchlist that is specifically composed for every deployment *in concreto*.[62] According to South Wales Police official reports, the AFR locate system was deployed and applied 70 times in the period from 2017-2019, resulting in several hundred thousand scanned faces and 59 arrests based on the results of the AFR Locate and NeoFace Watch software.[63]

---

60 Zalnieriute, M., *Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State*, The Columbia Science & Technology Law Review, Vol. 22, No. 2, 2021, pp. 286-287; see also, Brandl, R., *The world´s most surveilled citizens*, 3 February 2021, available at: [https://www.tooltester.com/en/blog/the-worlds-most-surveilled-countries/], Accessed 3 July 2022, Bischoff, P., Surveillance camera statistics: which cities have the most CCTV cameras?, 17 May 2021 available at: [https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/], Accessed 3 July 2022.

61 Davies, B.; Innes, M.; Dawson, A., *An Evaluation of South Wales Police's Use Of Automated Facial Recognition. Universities',* Police Science Institute Crime & Security Research Institute, pp 1-45, available at: [https://static1.squarespace.com/static/51b06364e4b02de2f57fd72e/t/5bfd4fbc21c67c2cdd692fa8/1543327693640/AFR+Report+%5BDigital%5D.pdf.] Accessed 15 July 2022; *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police,* [2020] EWCA Civ 1058, §10.

62 For more details on how AFR locate is functioning see: Kotsoglou; Kyriakos, *op. cit.* note 48, p. 87; South Wales Police, Facial Recognition Technology, available at: [https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/], Accessed 4 July 2022; *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police,* [2020] EWCA Civ 1058, §12.

63 South Wales Police, *Facial Recognition Technology*, 2020, available at: [https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial recognition-technology/], Accessed 4 July 2022.

The substantial criticism of the use of such systems comes from NGOs, whose objections can be divided into general and specific categories, the latter of which relates to individual systems, their specific use, and specific events. The lack of systematic legal regulation and the inadequacy of the same in the UK are some of the most serious objections of a general nature, with the emphasis on the problem of the lack of adequate supervision outside the police system over the use of such systems as well as the lack of a strategic approach to the usage and development of facial recognition systems as pointed at by Big Brother Watch.[64] The use of facial recognition systems has direct implications for the realization of the rights to privacy, family life, and freedom of expression, but it also has an impact on the issue of equality for all, i.e., discrimination.[65] One of the more specific objections to the AFR Locate system regards the large number of incorrectly identified innocent persons, which amounts to about 91% in the period from 27 May 2017 to 27 March 2018, calling into question the precision of this technology.[66] Another specific objection relates to the usefulness of such systems considering that in the same period, based on the use of the AFR Locate and NeoFace Watch software, a total of 15 people were arrested, which is about 0.005% of the total number of people covered by the work of the previously mentioned systems according to the data provided by Big Brother Watch and South Wales Police.[67]

Many of these objections were addressed first by the High Court and then by the Court of Appeal in the landmark case of Edward Bridges.[68] In the *case of Edward Bridges v. The Chief Constable of South Wales Police* (2019) EWHC 2341, Mr. Bridges first tried to challenge, before the High Court, the use of the AFR Locate system on two occasions, namely, on 21 December 2017 at Queen Street, a busy shopping area in Cardiff; and on 27 March 2018 at the protest in front Defense

---

64 Big Brother Watch, *Face off: The lawless growth of facial recognition in the UK policing*, May 2018, pp. 9-10, available at: [https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf], Accessed 5 July 2022.

65 *Ibid.*, pp. 13-19; see also Gentzel, M., *op. cit.* note 58, p. 1645 *et seq*.

66 Purshouse, J.; Campbell, L., *Privacy, Crime Control and Police Use of Automated Facial Recognition Technology,* Criminal Law Review, Vol. 2019, Issue 3, 2019, pp. 191-192.

67 Big Brother Watch, *op. cit.* note 7, p. 4. For comparison of listed figures, that are in accordance with further available data on the use of the AFR locate the system in the period from 2017 to 2019 and even in 2022 see also South Wales Police, Smarter Recognition, Safer Community, Deployments 2017-2019, available at: [https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/FRT deployments.pdf], Accessed 5 July 2022.

68 *Edward Bridges v The Chief Constable of South Wales Police* [2019] EWHC 2341, For a detailed analysis of the case see Gordon, BJ., *Automated Facial Recognition in Law Enforcement: The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police, Potchefstroom Electronic Law Journal,* Vol. 24., No. 1, pp. 4-15, [http://dx.doi.org/10.17159/1727-3781/2021/v24i0a8923].

Procurement, Research, Technology and Exportability Exhibition ("the Defense Exhibition"), which was held at the Motorpoint Arena. In its decision, the High Court did not accept the claims of Mr. Bridges that the use of AFR Locate on the two previously mentioned occasions violated his right to privacy and private life under Art. 8 of the European Convention on Human Rights and breached both the UK's data protection law and public sector equality duty.[69]

Mr. Bridges appealed against the decision of the High Court on five grounds of appeal, and the Court of Appeal, in the case of *R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police* EWCA Civ 1058, accepted three of those grounds and overturned the decision.[70] The Court of Appeal accepted the first ground of appeal in which it was stated that the existing legal framework governing the use of the AFR Locate system is insufficient. The two biggest objections of the Court of Appeal are that the legal framework did not define who can be put on the watchlist and where the AFR Locate system can be deployed. The latter issue is decided by the police on the basis of discretion, and the fact that there is a high degree of discretion is shown by the various types of events where the AFR Locate system was installed; Surveillance was carried out on various types of events from the Champion League Final, Antony Joshua's boxing match, various concerts, boat races and the Defense Exhibition.[71] The second accepted ground of the appeal refers to the issue of compliance with section 64 of the Data Protection and Freedom of Information (hereinafter: DPA) 2018; the Court of Appeal concluded that the "DPA failed properly to assess the risks to the rights and freedoms of data subjects and failed to address the measures envisaged to address the risks arising from the deficiencies they have found". Regarding the final ground of appeal, the Court held that the South Wales Police were deficient in fulfilling their public sector equality duty because they failed to recognize the risk that automatic facial recognition profiling could disproportionately impact women and minorities.[72]

Although this landmark case provided answers to certain questions about the use of FRT, it also opened up several other questions and issues that will certainly be the subjects of judicial decisions and interpretations in the foreseeable future. Firstly, although the Court of Appeal indicated that the legal framework govern-

---

69 Zalnieriute, M., *op. cit.* note 60, pp. 290-292.

70 *R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police,* [2020] EWCA Civ 1058, §129-130; see also *supra*, note 61.

71 South Wales Police, *Facial Recognition Technology*, 2021, available at: [https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/], Accessed 4 July 2022; Davies; Innes; Dawson *loc. cit.* note 60.

72 Zalnieriute, M., *op. cit.* note 60, p. 295-296.

ing the use of the AFR Locate system was insufficient, the same Court nevertheless concluded that the use of such a system was acceptable, proportionate, and in line with the legitimate aims that South Wales Police wanted to achieve. Such a point of view paves the way for increased use of the AFR Locate system when the conditions specified by the Court of Appeal are met by amendments to the existing legal framework. The second question of the impact of the use of the FRT on the realization of the rights to freedom of expression, assembly, and association under Arts. 10 and 11 of the European Convention on Human Rights remained unanswered because it was withdrawn before the first instance of court.[73] The use of FRT certainly affects the realization of the previously mentioned convention rights, and the concept of positive and negative obligations of the state will have to be adapted to new technologies. Thirdly, the court pointed to the problem of the relationship of safeguards that are required, which significantly complicates the assessment of the results of using FTR systems and their potential bias. The aforementioned issue will certainly be at the center of the future regulation of the use of FRT systems.

3.2. Netherlands

The Netherlands, known for securing the realization of individual rights and freedoms, is another European country experimenting the most with FRT as well as with other forms of using AI systems in police work and in relation to criminal prosecution.[74] CATCH is one of the many systems used by the Dutch police since 2016, which includes the use of FRT software. The main purpose of the CATCH system is to identify suspects or convicts by comparing the biometric data from the camera footage with a database containing persons who have been suspected or convicted of serious crimes since 2010 as well as persons who refused to identify themselves during arrests. According to data from 2019, the CATCH database contained 2.3 million pictures taken by the Dutch police.[75] Despite the deletion of 218,434 photos from the database in 2020, the total number of photos in the CATCH database in the same year grew to 2.653,038 photos, which indicates the trend of covering an increasing number of people with FRT.[76]

---

73 Gordon *loc. cit.* note 68.

74 For more see: Fair Trials, *Automating injustice: The use of artificial intelligence & automated decision-making systems in criminal justice in Europe*, pp. 8-14, 17-20, available at: [https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf], Accessed 13 July 2022-

75 Montag, L.; Mcleod, R.; De Mets, L.; Gauld, M.; Rodger, F; Pełka M., *EDRi report: The rise and rise of biometric mass surveillance in the EU: A legal analysis of biometric mass surveillance practices in Germany, The Netherlands, and Poland*, 2019, pp. 61-62.

76 See more: Politie, Centrale Automatische TeChnologie voor Herkenning (CATCH), Jaarcijfers 2020, available at:

In addition to the use of photos and footage obtained by recorded cameras for comparison with photos from the CATCH database, there are a number of other possibilities for the police to use the CATCH system on photos obtained from other sources. The CATCH system can be applied to photos and videos obtained through body cameras used by the police, videos sent by citizens, and videos and images obtained by private cameras installed and used by citizens.[77] The use of different ways to obtain images or recordings to which the CATCH system is applied is one of the fundamental objections to using such systems, especially in relation to photographs and recordings obtained by private cameras. In this regard, the project of the Dutch police called *Camera in Beeld* can be problematic. Through this project, the police invite private individuals and business entities to include the cameras they use in their private lives or business activities in their system; the registration is quite simple and straightforward, and the intention is that the recordings of these cameras are used only when it is necessary for added value to the investigation and detection of the perpetrators of criminal acts.[78] This way of expanding the police surveillance network to cameras of private entities circumvents the provisions of the Act on police data[79] and the LED Directive[80], which regulates biometric data as a special type of data, the processing of which imposes the standards of strict necessity and sufficient protection. Also, in accordance with the provisions of the GDPR, data collected by private cameras do not fall into the category of special data from Art. 9 but rather the processing of usual data from Art. 6.[81] Although, in the Netherlands, it is not allowed for the cameras of private entities to record public areas; however, it is possible that when it is necessary or cannot be avoided due to the specifics of the property, part of the public area

[https://www.politie.nl/binaries/content/assets/politie/onderwerpen/forensische-opsporing/catch-jaarcijfers-2020-hr-online.pdf], Accessed 13 July 2022.

77 Montag; Mcleod; De Mets; Gauld; Rodger; Pełka *loc. cit.* note 75.

78 Politie, Camera in Beeld, available at: [https://www.politie.nl/onderwerpen/camera-in-beeld.html], Accessed 13 July 2022.

79 Wet politiegegevens, Art. 5., available at: [https://wetten.overheid.nl/BWBR0022463/2020-01-01/0], Accessed 13 July 2022.

80 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2016], *OJ L 119,* Art. 10.

81 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] *OJ L 119,* Art. 6 and 9.

may be recorded.[82] Taking into account that the *Camera in Beeld* system in 2019 included 220,000 cameras and that 87% of them recorded parts of public areas, it can be considered a potentially large source of images and recordings for the police outside their own system of surveillance.[83] Considering the announcements that such a system may include over 1.5 million cameras[84], the issue of the legal regulation of the use of CATCH and other FRTs will be of imperative importance for the protection of the rights guaranteed by the Convention. With a slightly smaller reach, the same problems can occur regarding smart doorbell projects.[85]

The fundamental problem that appears with numerous FRT systems is the question of the proportionality of the success of such a system in relation to the goals that should be accomplished and the degree of violation of fundamental human rights and freedoms. CATCH is not an exception; according to available police data, in 2019, out of a total of 1,249 images, only 98 resulted in a positive match, which amounts to 8%. In 2020, out of a total of 1,142 images, only 96 resulted in a positive match, and that is a slight increase to 10% success.[86] Data on the actions of the police and criminal prosecution authorities on the actions taken in this 8% and 10% of positive matches are not known, nor is information regarding to what extent the recognition by the CATCH system contributed to the prosecutions and convictions. Taking into account the aforementioned percentages as well as the extremely small percentages of arrestees recognized by the AFR deployed by the South Wales Police (see section 3.1.), the question of the justification and effectiveness of using such a system in relation to the level of potential violations of individual rights naturally arises. This is supported by the jurisprudence of the Rechtbank Zeeland-West-Brabant in case No. 02-665274-18[87], in which the court concluded that the mere fact that the person was recognized by the CATCH system and that the identification was confirmed by two investigators as a human

---

82 Autoriteit Persoonsgegevens, Stappenplan camera bij huis, available at: [https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stappenplan_camera_bij_huis.pdf], Accessed 13 July 2022.

83 Dutch police can access 200,000 private security cameras, campaign for more, 2019, available at: [https://www.dutchnews.nl/news/2019/01/dutch-police-can-access-200000-private-security-cameras-campaign-for-more/], Accessed 13 July 2022; considering the announcements that such a system should include over 1.5 million cameras, the issue of legal regulation of the use of CATCHA and other FRTs will be of imperative importance for the protection of the rights guaranteed by the Convention.

84 *Ibid.*

85 Montag; Mcleod; De Mets; Gauld; Rodger; Pełka *op. cit.* note 75, pp. 72-74.

86 Politie, *Centrale Automatische TeChnologie voor Herkenning (CATCH)*, *loc. cit.* note 75, see also: Waarlo, N.; Verhagen, L., *De stand van gezichtsherkenining in Nederland, de Volkskrant*, available at: [https://www.volkskrant.nl/kijkverder/v/2020/de-stand-van-gezichtsherkenning-in-nederland~v91028/?referrer=https%3A%2F%2Fwww.google.com%2F], Accessed 14 July 2022.

87 *Rechtbank Zeeland-West-Brabant [2019] case No. 02-665274-18, ECLI:NL:RBZWB:2019:2191.*

factor in making a decision (i.e., a safeguard) is not sufficient to convict a person; that is, additional evidence is necessary.

3.3. Germany

Germany is not an exception to the growing trend of mass surveillance and the use of FRT systems in Europe. Such a trend has certainly been accelerated by contemporary and recent socio-political events. Taking into account that Germany is one of the leaders in the establishment of mass surveillance in Europe, both at local levels through the established systems in Bielefeld and Coesfeld in 2003, in Mönchengladbach in 2004, and Düsseldorf in 2009, as well as those established on the basis of national projects such as the mass surveillance of the Südkreuz train station in Berlin in 2017, it is not surprising that FRT systems are applied in Germany.[88] The vast majority of cameras that have been installed are ready for biometric identification, especially in the last-mentioned project; but even if they aren't capable of applying biometric identification in real-time, it is possible afterward. In the case of *Gaughran v. United Kingdom Application no. 45245/15*, the European Court of Human Rights warned that the storage of recordings and images that are not subject to the direct use of facial recognition software but can be subsequently placed in a database to which the aforementioned programs can be applied represents a direct interference with Art. 8(1) of the Convention.[89]

The application of FRT in Germany is not only potentially related to mass surveillance; there are a number of projects, events, and examples of direct use of such systems. The use of the facial recognition software Videmo 360, with a real-time facial recognition function, by the Hamburg police for the investigation of criminal offenses in connection with the G20 meeting that took place at the Hamburg summit, is one relatively recent example of the usage of FRT in Germany. For this purpose, a database was created containing 100 terabytes of recordings and images that were collected from various sources such as police video surveillance material, footage from the public transport and tram stations, material from the 'Boston infrastructure' portal of the Federal Criminal Police Office, private footage uploaded by citizens for the police, and video and image files taken from media sources.[90] Seventeen terabytes were used for facial recognition by Videmo 360, including

88 Montag; Mcleod; De Mets; Gauld; Rodger; Pełka *op. cit.* note 75, pp. 19-22.

89 The ECtHR warned that the storage of recordings and images that are not subject to the direct use of facial recognition software but can be subsequently placed in a database to which the aforementioned programs can be applied represents a direct interference with Article 8(1) of the Convention, see more: Judgment *Gaughran v The United Kingdom* (2020) EHRR, No. 45245/15, 13 February 2020, § 69-70.

90 Raab, T., *Video Surveillance and Face Recognition: Current Developments, Reports: Germany*, European Data Protection Law Review (EDPL), Vol. 5, Issue 4, 2019, p. 544.

around 15,171 videos and 16,480 images.[91] In this case, The Hamburg Commissioner for the DPA concluded that the police do not have the authority to make a decision on the application of biometric identification, especially taking into account the level of intrusion into human rights, and accordingly ordered the deletion of the aforementioned database. A number of objections were raised by the DPA, considering that the use of Videmo 360 was not selective and violated the rights of individuals who were never even suspected of committing a crime; the second part of the complaint referred to the fact that the persons were not aware or informed that the FRT technology was being applied to them and, accordingly, could not even file a complaint; one of the objections is the lack of a legal framework regulating the collection of data from different sources and the creation of a database for processing through FRT technology, which has proven to be a general problem in European countries that use FRT.[92]

The Hamburg Administrative Court, in *case no. 17 K 203/19*[93] concluded that the DPA did not have the authority to conduct a legal analysis and ordered the deletion of the database, which led to the annulment of the order issued by the DPA. Therefore, due to procedural and formal reasons and the lack of DPA authority, the Court did not consider the legality and validity of the use of Videmo 360; the Court stated that biometric data is a special type of data and that their processing must meet the condition of strict necessity.

The DPA appealed against the said decision; the appeal was allowed, and the case is pending. The Hamburg Police publicly announced that it had deleted the database from the G20 summit, considering that there was no longer a reason for the appeal. According to the DPA's point of view, considering the importance of legal regulation in the field of FRT and biometric identification and the use of these systems in the future, especially in the context of endangering a democratic society, it values further judicial interpretation and clarification.[94] Taking into ac-

---

91 *Ibid.*; See also: Monroy, M., *Security Architectures in EU: G20 in Hamburg: Data protection commisioner considers face recognition illegal*, 2018, available at: [https://digit.site36.net/2018/08/15/g20-in-hamburg-data-protection-commissioner-considers-face-recognition-illegal/], Accessed 15 July 2022.

92 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, *Einsatz der Gesichtserkennungssoftware „Videmo 360" durch die Polizei Hamburg zur Aufklärung von Straftaten im Zusammenhang mit dem in Hamburg stattgefundenen G20- Gipfel*, 2018, available at: [https://datenschutz-hamburg.de/assets/pdf/Anordnung_HmbBfDI_2018-12-18.pdf], Accessed 15 July 2022.

93 Verwaltungsgericht Hamburg, Urteil [2019] case no. 17 K 203/19.

94 See more: The Hamburg Commissioner for Data Protection and Freedom of Information, *PRESS RELEASE, Hamburg Police deletes the biometric database for facial recognition created in the course of the G20 investigations*, 28 May 2022, available at:

count the recent jurisprudence regarding the surveillance of Breslauer Platz and its side streets in Cologne in the cases *VG Köln 20 L 2340/19*[95] and *OVG Nordrhein-Westfalen 5 B 137/21*[96], as well as recent research that shows that the approval rate regarding the FRT system in Germany is lower than in the UK, USA, and China and that the opposition rate is the highest concerning the citizens of the aforementioned countries[97] the court's interpretation regarding the aforementioned issues will be significant not only for legal regulation but for society in general.

4. CHALLENGES AND DOUBTS FOR THE IMPLEMENTATION OF FRT IN EUROPE – BETWEEN UNQUESTIONABLE PRINCIPLES OF CRIMINAL PROCEDURAL LAW AND THE RENAISSANCE OF MODERN TECHNOLOGY

The great potential for the application of facial recognition technology (FRT) for criminal proceedings is primarily demonstrated in the facilitation and acceleration of activities that the police carry out. The use of FRT can facilitate the clarification of a criminal offense and the preventive actions of police officers. In particular, the improvement and acceleration of the process of identifying individuals enable the police to respond in real time, immediately, whether it is a matter of stopping and arresting someone or taking preventive action to increase the readiness of police officers in a particular area due to the presence of suspicious individuals. In addition to ordinary face-to-face matching, or discovering a specific face among a crowd of people on recordings or live cameras, FRT can also be used for the detection of certain emotions and affections. In this sense, FRT can be used to detect "strange behavior", which can also be a trigger for stopping someone and directing further proceedings toward them.

In addition to the above, the result of FRT processing has a certain potential for use in the evidentiary context.[98] The result or "output" of FR processing is only a data point that shows a certain percentage or probability of the existence or non-existence of a certain fact, or the making or not making of a certain decision. It is not difficult to imagine that an FR tool could be used to verify the results of iden-

[https://datenschutz-hamburg.de/assets/pdf/2020-05-28-Press-Release_Biometric_Database.pdf], Accessed 15 July 2022.

95 VG Köln [2020] 20 L 2340/19.

96 OVG Nordrhein-Westfalen [2022] 5 B 137/21.

97 Kostka, G.; Steinacker, L.; Meckel, M., *Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States*, Public Understanding of Science 2021, Vol. 30, No. 6, pp. 671–690.

98 Kotsoglou; Oswald, *loc. cit.* note 48.

tification as a procedural action, in which the tool would confirm or question the recognition result. Any data that affect the assessment of the level of suspicion that a particular person has committed a criminal offense can be of crucial importance in deciding on the formal initiation of criminal proceedings, ordering some evidentiary actions, or adjudicating on pre-trial detention or bail. In this context, the question also arises as to whether and to what extent FRT should be used to assess the credibility of statements, e.g., from witnesses or defendants. It is increasingly common practice for the statements of individuals at different stages of the proceedings to be recorded and therefore become suitable for subsequent FR analysis. The credibility of the statement of an individual is of crucial importance, and such an assessment is made by law enforcement authorities based on direct observation, life experience, and logical conclusion.[99] How credible, advisable, or acceptable it would be to use FRT to supplement or even replace human judgment in the assessment of credibility is a complex and multifaceted issue that raises numerous legal, ethical, and social questions.[100] It is not easy to answer the aforementioned questions; the response depends primarily on the stage of the criminal process and the nature of the decision being made. It is not an equal situation if it is about an early stage of the proceedings and the decision is made in favor of the suspect or if the procedure is already in the trial phase and such an assessment becomes a basis for a verdict on the defendant's guilt.

Although potentially useful, the employment of AI for the purposes of deciding on criminal prosecution can lead to numerous unwanted phenomena. The same can be applied to FRT, which can result in incorrect facial matching or identification. The rights at stake include the rights to dignity, privacy, protection of personal data, non-discrimination, freedom of assembly, effective legal remedy, and the right to a fair trial.[101] Therefore, it is appropriate to consider AI systems in the context of their use in criminal proceedings as high-risk systems, as classified by the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)

---

99 Krapac *op. cit.* note 36, p. 102.

100 The complexity of utilizing Facial Recognition Technology and exploring its potential positive applications necessitates a comprehensive and balanced approach. By addressing technical challenges, privacy concerns, and ethical considerations, we can strive towards leveraging FRT's capabilities while upholding individual rights and societal well-being. See more in: Roksandić S; Protrka N.; Engelhart M., *Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?*, 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2022, pp. 1227-1229, doi: [10.23919/MIPRO55190.2022.9803606].

101 Kritikos, M., *Artificial Intelligence ante portas: Legal & ethical reflections*, European Parliamentary Research Service, Scientific Foresight Unit (STOA), pp. 4-5, available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634427/EPRS_BRI(2019)634427_EN.pdf], Accessed 13 July 2023.

and amending certain union legislative acts (hereinafter: Proposal).[102] This applies in particular to AI systems for remote biometric identification as well as those used for individual risk assessments, assessment of the reliability of evidence in criminal proceedings, polygraphs, or other similar tools for determining an individual's emotional state, and predicting the occurrence or reoccurrence of a criminal offense based on the creation of an individual profile. All of the above also applies or may apply to FRT.

Technical errors, discrimination, violation of freedom of assembly, protection of personal data, and impact on dignity and privacy have already been discussed extensively.[103] Therefore, this chapter focuses on issues related to the use of FRT for the purposes of criminal proceedings, such as the impact on the rights to a fair trial and fair legal procedure and, above all, on the presumption of innocence.

Considering many forms of the use of FRT for the purposes of criminal proceedings, it is necessary to first establish criteria or parameters for analyzing each specific situation of FRT use in order to detect potential problems and points that need to be carefully legally regulated.

Through regulation, it is necessary to differentiate preventive and investigative activities of law enforcement authorities, especially its evidentiary activities. Furthermore, the judicial bodies and stages of the proceedings at which FRT is applied vary widely. Attention must be directed to the potential bias of the court or decision-maker, the right to a legal remedy against the decision, and the duty to inform the individual that FRT has been applied.

4.1. FRT and the Presumption of Innocence

FRT can be applied to a specific person with or without suspicion that he/she has committed a specific criminal offense. It is important to consider a situation in which there is a suspicion that a specific person has committed a criminal offense. It should be noted here that there is a difference between the use of FRT in relation to criminal proceedings regarding the crime for which the person is suspected and the preventive use of FRT on that person in order to prevent other criminal offenses. While the use of FRT in the first case is almost self-evident, in the second situation, it may be quite questionable. Such preventive use should be accompanied by the fulfillment of certain additional conditions with a limited scope of interference with rights and freedoms. Moreover, the fact that someone

[102] The use of biometric data is also prescribed as risky by the Law Enforcement Directive (Recital 51).

[103] Leslie, D., *Understanding bias in facial recognition technologies: and explainer*, The Alan Turing Institute, 2020., pp. 1-50., [https://doi.org/10.5281/zenodo.4050457].

is suspected of committing a certain criminal offense must not affect his/her private everyday life as if they had already been definitively convicted of the specific criminal offense. They must be able to continue to live normally and enjoy all their rights and freedoms like any other person. The aforementioned regards the effects of the presumption of innocence which do not concern the criminal proceedings against the accused but rather his everyday functioning in society. This should be kept in mind when deciding whether and to what extent FRT should be applied against certain individuals.[104]

The implications of the presumption of innocence on the use of FRT for the purposes of specific criminal proceedings can be multiple. On the one hand, it can affect the admissibility of the use of FRT with regard to a specific person, while on the other hand, it can be relevant to the legality of the results obtained. Above all, it is necessary to distinguish investigative activity from evidentiary activity, and then the question of the legality of the obtained results arises in each of the previously mentioned activities.

For the analysis of these issues, the nature of the results obtained through the use of FRT is of key importance. In fact, the result of the application of FR tools is a certain percentage or probability.[105] However, the language of probability is only a language of speculation and, as such, is not applicable in those stages or phases of criminal proceedings in which the *in dubio pro reo* principle is a key component (or, more accurately, a consequence) of the presumption of innocence.[106] A clearly expressed percentage probability of the existence of a certain phenomenon or fact also provides a clearly expressed percentage probability of the non-existence of the same phenomenon or fact. In this way, the accused is provided with a strong argument to challenge a decision that is not in his or her favor, and it highlights the fact that the decision-maker is not completely certain in their decision and that the decision being made is objectively problematic.[107]

Special problems are situations in which we encounter borderline cases determined by a few percentile points, which could be the boundary between the status of a citizen and the status of a suspect, and even positive or negative decisions on, for example, initiating a criminal procedure, determining pre-trial detention,

---

104 Identifying or locating a potentially dangerous person in a certain space does not necessarily have to trigger an arrest but can be a reason for raising the operational readiness of police forces.

105 Kotsoglou; Oswald, *loc. cit.* note 48.

106 The presumption of innocence in criminal proceedings is expressed through the principle *in dubio pro reo* and the rule that the burden of proof is on the prosecutor.

107 Damaška M, *Dokazno pravo u kaznenom postupku: oris novih tendencija*, Pravni fakultet u Zagrebu, Zagreb, 2001, pp. 32-33.

deciding on the discontinuation of proceedings or even deciding on one's guilt or innocence. However, these situations are not equal. These decisions are made by different subjects at different stages of the procedure, and the consequences of the above errors are not equally severe.

In the early stage of discovering and clarifying a criminal offense, the stage of the investigation, and even in the filing of the indictment, the principle *in dubio pro reo* does not apply, and the presumption of innocence does not directly hinder the use of FRT or the use of AI in general.[108] The percentages of the probability for the existence of a certain fact are extremely valuable and applicable in the work of the police in the stage of detecting a suspect, as well as for the prosecutor when deciding on the undertaking of certain investigative actions or on moving forward with an investigation against a certain person. In this stage of criminal proceedings, the activity of the law enforcement authorities is reduced to weighing the probabilities, or whether there are grounds for reasonable suspicion that the criminal offense has been committed or there is already probable cause that a specific person has committed a criminal offense. In this sense, the application of FR tools and AI tools, in general, seems more than justified for the activities of the police. It can lead to the identification and arrest of the suspect and help in deciding on the need to take some other investigative or evidentiary action. Any error in the application of FR tools could be compensated for by activating additional guarantees and rights of the accused, thereby eliminating the error (in recognition) quickly.

There is a slightly more complex situation with the application of FR tools in the work of the prosecutor. As mentioned, the part related to the inquiry of criminal offenses and deciding on the undertaking of (urgent) investigative and evidentiary actions is actually the same as in the work of the police. However, caution should be exercised in decisions on the formal initiation of criminal proceedings, indictment, and determination of pre-trial detention and other coercive measures. Namely, the undertaking of these actions leads to serious interference with the rights and freedoms of the individual, that is, the accused, all because of the probability jump caused by the application of AI or FRT tools. The situation is particularly sensitive if the prosecutor, using FRT tools, is to come to the result that there is a 51% probability that someone is the perpetrator of a criminal offense, which would actually activate his obligation to initiate criminal proceedings in accordance with the principle of legality (mandatory) prosecution; at this percentage, it is considered that there is probable cause that a specific person has committed a

[108] Novokmet, A., Tomičić, Z., Vinković, Z., *Pretrial risk assessment instruments in the US criminal justice system—what lessons can be learned for the European Union*, International Journal of Law and Information Technology, Vol. 30, Issue 1, 2022, pp. 1–22, [https://doi.org/10.1093/ijlit/eaac006].

criminal offense. Namely, the prosecutor should not initiate criminal proceedings under the same principle of legality if the percentage is lower than 51%.[109] Therefore, from the aspect of the presumption of innocence, there is no direct obstacle to the application of FRT here. At this stage of the proceedings, the principle *in dubio pro reo* does not yet apply. The application of FRT is undoubtedly for the purposes of criminal proceedings because there is suspicion of the commission of a criminal offense by the person in relation to whom the FRT is applied. The question is only the context in which FRT is applied and how the result of its application contributes to the overall assessment of the prosecutor about the probability of committing a criminal offense. This could be a question of the identity of the person recorded[110] or the assessment of the credibility of a particular piece of evidence or personal statement.

The question of evaluating the reliability of a particular piece of evidence using FRT is a slippery slope. This question can be encountered by both the prosecutor and the court. Using FRT, for example, one could check the result of the identification against the results of recognition by the witness. Their results could match or differ significantly. It goes without saying that the result of such an action could be important for the prosecutor or court's decision on further proceedings. Furthermore, the development of technology has led to the frequent, and sometimes mandatory, audio-video recording of certain evidentiary actions, i.e., interrogations of suspects. Such recordings are used by the court and the prosecutor for evidentiary purposes, and by reviewing them, they are becoming familiar with their content, but they are also assessing the reliability of the statements themselves. For example, such could include recorded statements of witnesses and defendants as well as the evidentiary action of confrontation that is carried out. The question arises as to whether the prosecutor or the court can subject such a recording to FRT and obtain the relevant data on the probability that the statement of a particular person is reliable or not. The fact is that the judicial bodies are not bound by specific formal evidentiary rules regarding the proven or unproven nature of a fact and that they evaluate the evidence based on the principle of free evaluation of evidence. In other words, the judiciary carries out this evaluation following their legal knowledge and life experience, logical conclusions, and analysis of all the evidence individually and in connection with any other evidence.[111] One can

---

109 *Ibid.*

110 We can imagine a hypothetical example in which we have evidence that person A has committed a criminal offense, but after the arrest and the expiration of the maximum detention period, we cannot with 100% certainty determine that the arrested person is indeed person A. By applying the FRT tool, we get the result that there is a 75% probability that it is indeed person A. Can we impose investigative detention on the arrested person? The answer is addressed below.

111 Krapac *op. cit. note* 36, pp. 102, 124-127.

ask whether judicial bodies carry out the analysis of a particular piece of evidence in such a way that FRT points out to them some signal or gesture that the judge or prosecutor did not notice in their observation, but which would indicate the statement of a person as true or false. Such verification of reliability comes with numerous challenges.

The consideration of verifying the reliability of a person's statement using FR tools has certain similarities with polygraph testing. The results of polygraph testing are not recognized by almost any legal system as evidence in criminal proceedings but are only applicable informally, in the cognitive sense, in the preliminary proceedings.[112] The next important circumstance is that it is necessary to obtain the consent of the examinee for polygraph testing. Since there is no request for consent for the use of FR, logic dictates that FR should not be used in a wider scope than a polygraph. Therefore, the use of FR for the purposes of verifying the reliability of a person's statement should definitely remain outside the scope of verifying the reliability of the evidence on which the final verdict is based, or outside the trial stage in which the principle *in dubio pro reo* also applies. Namely, in order to deliver a guilty verdict, the court must be certain of the defendant's guilt, that is, the guilt must be fully proven. It must be certain that the defendant is guilty, that is, proven beyond any reasonable doubt. These formulated highest standards of proof do not tolerate any numerical expression in percentages, nor any eventual grading. It is difficult to imagine that FR would ever provide a result that would with 100% certainty declare a certain piece of evidence reliable or unreliable, and any other number, even if it were 90% or more, would lead to doubt or the application of the principle *in dubio pro reo.*[113] Clearly expressing a percentage in the reasoning of the judgment would provide the defense with a strong argument for contesting the judgment through legal remedies.

Taking technical problems into account, such as the accuracy of the FR tool itself and the possibility of evaluating the credibility of the whole statement, the conclusion is that the verification of the credibility of evidence through the FR tool in the trial stage should be explicitly prohibited. The explicit prohibition should eliminate any surreptitious use of the FR tool by the court. It is possible to imagine the court using the FR tool without the knowledge of the parties in the proceedings and not mentioning such use anywhere in the reasoning of the judgment despite its significant effects on the formation of its position on the credibility of certain evidence.

---

112 Novokmet; Tomičić; Vinković, *op. cit.* note 108, p. 18.

113 Damaška *op. cit.* note 107, p. 33.

4.2. FRT and other elements of the right to a fair trial

The application of FRT in criminal proceedings, as well as AI tools in general, can also significantly affect some other aspects of a right to a fair trial. Below, we present those that we considered most important for the assessment of the admissibility of the use of FRT for the purposes of criminal proceedings.

The use of FR tools in the decision-making process could significantly affect the objectivity of the court, as well as any other authority making the decision in criminal proceedings. There is a justified fear that decision-makers might excessively and uncritically rely on the results of FRT and AI tools in general and that, ultimately, the results of such processing would become the deciding factor in the decision-making process.[114] Even the very impression from the objective and impartial side that decisions are actually made by someone else, rather than the body responsible for decision-making, can significantly damage the perception of the criminal proceedings as fair. Due to the danger that such evidence will be predominant, care must be taken in what purposes for which it can be allowed to use FRT.

Transparency and reliability of the functioning of FR tools can represent a significant problem in terms of ensuring the fairness of proceedings in relation to the accused. Namely, the accused has the right for the decision to be minutely and clearly reasoned so that he can challenge it with legal remedies and request its review by a competent court. Similarly, the accused must be allowed to challenge the results of FRT processing during criminal proceedings, similar to the right of confrontation as one of the minimum rights of defense. If the mechanism of functioning of the FR tool is too complex, it is not possible to adequately meet these minimum standards of fairness of proceedings. Therefore, not only should the accused be aware that FRT has been applied for the purposes of the criminal proceedings in order to be able to challenge the decision with legal remedies in that direction, but he should also be familiar with the technical fundamentals of the functioning of the FR tool and the way in which the results of FR processing are created. The use of a tool whose functioning is a mystery represents an unacceptable lack of transparency and certainly does not meet the standards of fair proceedings.

The prohibition of the use of illegally obtained evidence is an essential standard that arises from the requirement for fair proceedings and must therefore be represented in the use of FRT. In this sense, it is necessary to clearly specify in which cases the use of FR tools is not allowed. For example, the face represents biometric data or personal data that can be protected and considered data that must not be

[114] Kotsoglou; Oswald, *loc. cit.* note 48.

processed under certain conditions. As previously pointed out, it is important to prohibit the use of FRT in the trial phase of criminal proceedings.

Due to all of the above, it is necessary to seriously consider introducing mandatory defense for all cases in which FRT is applied. These are cases involving the use of high-risk new technologies. The rights of the accused may be seriously tested, and assistance from a defense lawyer should be provided even when the accused does not recognize such a need.

As stated in the previous chapter, not all of these rights are equally at risk throughout the entire process. The level of threat depends on the stage of the criminal proceedings, the purpose of using FRT, and the authority that uses it. Therefore, it is necessary to return to the question of the verification of the credibility of statements using FRT. As we already undoubtedly expressed a negative opinion on the use of FRT in a trial phase due to the application of the principle of *in dubio pro reo*, the focus won't be on problematizing the use in a trial from the perspective of the other elements of the right to a fair trial. However, when it comes to the decisions of the prosecutor and the court with regard to initiating criminal proceedings or deciding on, for example, pre-trial detention, the application of the principle of *in dubio pro reo* is not directly affected. On the other side, the use of FR tools for the purpose of verifying the credibility of statements would be questionable.[115] Namely, these are decisions that heavily affect the accused. His status is significantly changed, he is deprived of freedom or formally has a criminal procedure against him, and the decision is founded on the FR tool calculation whose results are questionable from the standpoint of the fair trial principle. Here, we primarily have in mind the previously ascertained insufficient transparency and reliability of the use of FRT for the purpose of verifying the credibility of statements but also its potential predominance and possibility of being uncritically relied upon by the decision maker. It is not equal to applying an FR tool for the identification of a person, which is relatively safe, transparent, and easily verifiable by the decision maker, as it is to apply an FR tool for the assessment of the credibility of statements. If such use should be allowed, it would require clearly specified additional guarantees such as the obligation of a competent authority to the accused that FRT is used for the stated purpose in the specific case. Furthermore, the accused should be informed about the basic principles of the functioning of the FRT, and a regulation on obtaining the accused's consent as a prerequisite for use of FRT, similar to polygraph testing, should be considered.

Given the identified problems, the proposal for the utilization of FRT for the purpose of verifying the credibility of statements could be regulated in the direction

[115] Novokmet; Tomičić; Vinković, *op. cit.* note 108, pp. 16-18.

of allowing such use in earlier stages of the criminal proceedings, but only if the result would be in favor of the accused. There is nothing preventing the prosecutor, for example, from using an FR tool to verify the credibility of a statement given by a suspect to the police in a formal manner when reviewing the recording of the statement and ultimately explaining his decision to discontinue the criminal proceedings by stating that the accused's statement denying guilt is credible, whereas, for example, the statement of a witness accusing him is not credible. This analogy is drawn from the exceptional possibility of using even illegally obtained evidence if it is for the benefit of the accused.[116] Namely, if we have technology at our disposal that can be helpful, but its use is questionable for the protection of the rights of the accused or the fairness of proceedings, the interests of protecting justice require us to apply this technology in order to establish the truth in favor of the accused.

4.3. Critical points for regulating the use of certain types of FRT

The main problem with the use of FRT is the risk of incorrect recognition or obtaining false positive and false negative results. Such errors lead to further risks. The police will stop people for whom a certain level of matching has been obtained, and some of these people will be arrested or otherwise unjustly treated, leading to potential tensions and discomfort, not to mention violations of the rights and freedoms of innocent citizens. Avoiding and reducing these risks is the primary task of both the legislator and the authorities that carry out specific actions. Besides the possible technical sources of errors, discrimination, restriction of freedom of assembly, protection of personal data, and impact on dignity and privacy, here are highlighted some key critical points that legislators should consider when regulating this issue. Firstly, as already stated, it is not acceptable to equate preventive and investigative activities of law enforcement officials, and it is especially necessary to distinguish preliminary investigation from formal investigation.

When speaking about the risks of using FRT for identification purposes, it is acceptable to bear a greater risk for serious criminal offenses that need to be clarified or prevented. Similarly, in general, it is more acceptable to bear a higher risk when it is necessary to immediately identify and arrest the perpetrator of a specific criminal offense as opposed to a situation where we only act preventively to deter the perpetrator from committing a crime. Eventually, it is certainly necessary to emphasize that the risks in the use of FRT are much higher when identification using FRT is carried out live, in real-time, and an immediate reaction by police

[116] Krapac *op. cit.* note 36, pp. 102, 457-463.

officers follows rather than when such identification and reaction are delayed. Namely, real-time identification is much more prone to incorrect identification. The quality of the recording is much poorer than when identification is carried out under controlled conditions based on better-quality recordings or photographs. The police officer has much less time to check the results, and there is a greater risk that he will react to the identified person only based on the results of the FR tool, which puts us at risk of having the decision on the reaction not made by a person, an authorized officer, but by the FR tool.

Every legal system recognizes the situation in which the police verify and determine the identity of a certain person suspected of committing a criminal offense whose identity is unknown. This type of identification is the least controversial. General databases can be used in this situation, and the identity of the person will be quickly determined by comparing face images one on one. This type of identification is carried out with better-quality photographs, and the possibility of incorrect pairing is minimal. In this case, FRT can significantly shorten the time needed for identification, which is of great help here, as otherwise, the deadlines, i.e. for the detention of the arrested person, could expire. With the use of FRT, such a situation is possible but still harder to imagine.[117]

FRT can further significantly contribute to the quickness of clarification of the criminal offense and to finding the perpetrator in cases of identification of people from footage obtained after the commission of the criminal offense.[118] It can involve the identification of people recorded at the place of commission or in the vicinity, as well as the pairing of faces that are on footage taken at critical times at locations where the perpetrator could be found. It should be possible to use all available databases in this case as well, regardless of potential limitations imposed by the requirement to protect personal data. Reducing the time it takes to find and identify the perpetrator is of enormous importance for the final outcome of the criminal investigation, as expressed through the old criminalistic saying that 'time passing is truth running away'.

---

[117] Can pre-trial detention be determined against a person for whom all conditions are fulfilled, but there is not 100% assurance of their identity? For example, FRT says there is a 75% chance that this is person A., but there is still a 25% chance that it is not that person. This shows the fact that FRT assessment is just data that the decision maker needs to verify and put in relation to other data to make a decision. There is a trap of the predominance of such data or "evidence", which will be of great practical influence on the decision maker. In any case, we consider it justified to insist on the obligation to inform the person of the fact that they have been recognized by FRT and on the right to a lawyer and legal remedy against the decision on pre-trial detention. In the specific case, the weight of the criminal offense being charged would certainly be of significance, and the determination of pre-trial detention would only be possible for the most serious criminal offenses.

[118] Kotsoglou; Oswald, *loc. cit.* note 48.

There are no special barriers to the use of the FRT in the case of the enforcement of criminal sanctions against convicted perpetrators. This refers to convicts for criminal offenses whose freedom of movement is restricted by a court decision. As such, they are included in tracking and identification databases by FRT at locations where, according to a final judgment, they should not be. They are not protected by the presumption of innocence, and on top of that, they knowingly and directly violate legally imposed prohibitions. The only thing to be careful of is the high level of recognition by the FR tool and the need for the police officer to personally verify such a result and make a specific decision on an appropriate response.

Definitely, the most controversial case is live identification, that is, real-time identification.[119] The Proposal specifically draws attention to this type of recognition and calls it the use of AI systems for the remote biometric identification of individuals in real-time in public places for the purposes of criminal prosecution. As such, it considers it a significant violation of the rights and freedoms of the involved individuals to the extent that it can affect the private life of a large part of the population, create a feeling of constant surveillance, and indirectly deter the exercise of the freedom of assembly and other fundamental rights.[120]

It is particularly controversial when such identification is carried out for preventive purposes. However, it should also be emphasized that the reaction of the police officers to recognition does not necessarily have to be a stop and arrest or a search of the person. Other preventive reactions in the form of determining and carrying out certain secret preliminary investigations, and potentially certain secret surveillance measures, are also possible. The key problem with this type of identification is actually the database on which the identification or recognition is based. Namely, there must be a clear reason and legal basis to justify why a certain person is on the surveillance list. Who will be on such a list must be accurately determined by the legislator. Questions also arise as to whether the person on such a list is aware of this fact and whether and under what conditions he/she could request removal from the list.

Due to the high risks it poses, the use of live FRT should be subject to judicial review, i.e., each user should be pre-approved by a court in a strictly limited area

---

119 Leslie *loc. cit.* note 103.

120 The European Commission (2021) Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial intelligence act) and amending certain Union legislative acts COM(2021) 206 final, available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.], Accessed 6 July 2022, Recital 18.

for specifically defined purposes. The content of the database or surveillance list should also be determined for each specific case.[121] The Proposal explicitly advocates for the prohibition of the use of these systems for criminal prosecution, except in the three thoroughly mentioned and narrowly defined situations in which such use is necessary to achieve a significant public interest, the importance of which outweighs the risks. These situations include the search for potential victims of criminal offenses, including missing children, certain threats to the life or physical safety of natural persons, threats of terrorist attack, and the detection, location, identification, or prosecution of perpetrators or suspects of criminal offenses or offenses referred to in Council Framework Decision 2002/584/JHA38 if those offenses are punishable in the Member State by a maximum sentence of imprisonment or detention of at least three years.[122]

5. CONCLUSION

Various state-of-the-art artificial intelligence systems are increasingly fortifying their place in contemporary criminal justice. Regardless of the seriously expressed scepticism due to the fear that such modern tools represent threats to the finely balanced system of protection of fundamental human rights and freedoms, it is not to be expected that criminal law will remain immune to the multiple benefits that artificial intelligence offers in the fight against modern forms of crime. Although criminal law slowly and relatively passively adapts to new social circumstances and technological development, there is no doubt that the number and variety of different forms of criminal offences, and especially the technologically equipped perpetrators, greatly exceeds the current capabilities of law enforcement agencies. Thus, it is reasonable to expect that society must have at its disposal certain means that will be able to respond to all the challenges of modern criminality. Since various advanced algorithmic systems have already infiltrated all spheres of social life for the purpose of efficient and quick action by law enforcement agencies in the revealing of criminal offenses and detecting perpetrators, it will be necessary to adopt advanced AI systems that will support the technological (r) evolution of criminal law.

One of these advanced AI tools is facial recognition technology. Facial recognition is a well-known technique for determining the identity of a person using their

---

121 Kotsoglou; Oswald, *loc. cit.* note 48.

122 The European Commission (2021) Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial intelligence act) and amending certain Union legislative acts. COM(2021) 206 final, available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.], Accessed 6 July 2022, Recital 19.

face. However, modern tools that use specially developed algorithms for fast facial recognition in a predefined database, even when it comes to recognition in difficult conditions (e.g. a darkened or concealed face), show all the benefits of using advanced technologies in the daily operation of law enforcement agencies. Those tools show their advantages not only in the proactive phase of the procedure, when it is necessary to discover and identify the perpetrator of a criminal offense in the shortest time, but also in the preventive reaction which aims to prevent the commission of a criminal offense and save human lives from direct loss by noticing and recognizing possible excessive situations in a timely manner.

However, despite the aforementioned benefits, facial recognition technology has recently been subjected to serious criticism that due to the risk of incorrect results (false positive or false negative) and possible discrimination, violations of the right to privacy and personal data, the unquestionable fundamental values that are the core of human dignity could be jeopardized. Contemporary European criminal procedural law truly inherits the general and specific fair trial guarantees (Art. 6. ECHR) that are the cornerstone of modern criminal justice. Among them, the presumption of innocence, the *in dubio pro reo* rule (Art. 6 (2) ECHR), and minimal rights of the defence (Art. 6 (3) ECHR) represent the European minimum standards for the protection of the defendant against the excessive power of state bodies in criminal proceedings. This minimum threshold of fundamental rights is a "litmus test" for every bold attempt directed to the incorporation of modern solutions that are intended to infringe upon human rights and freedoms, and facial recognition technology must not be an exception.

This paper discusses some critical aspects that European legislators must take into account when implementing FR tools based on the use of advanced and modern AI technology. Those aspects not only include defining the conditions for their application, form of action, scope of application and bodies authorized to use them, they also presuppose the correct positioning of judicial review as a key guarantor of the legality and proportionality of the application of facial recognition technology. Only properly established protective mechanisms through preventive and/or subsequent judicial review for the justification of the application of the FRT for the purposes of criminal proceedings can create legitimate preconditions for a well-balanced framework between the aspiration for the fast, modern and efficient investigation of criminal offenses and the aspiration for the protection of fundamental human rights and freedoms, which, as a civilizational achievement of modern society, reflects the basic orientational criteria of the rule of law and represents a barrier to arbitrary and malicious actions of state bodies.

This paper went into a detailed analysis of the risks involved in the application of FR technology for the purposes of criminal proceedings. Attention is drawn to

the fact that, when regulating FR, it is important to distinguish activities aimed at prevention and detection as well as probative activities of law enforcement agencies. In principle, we can say that we are ready to bear greater risk according to the seriousness of the crime that we want to detect or prevent. Likewise, we are willing to bear a greater risk when it is necessary to immediately identify and arrest the perpetrator of the specific criminal offense that we are trying to solve than when we only want to act preventively. It should certainly be pointed out that the risks in the application of FRT are far greater when identification using FRT is performed live in real time and the reaction of police officers immediately follows than when such identification and reaction are undertaken with a delay once the criminal offences have been committed.

Special attention is paid to the potential of FR technology to provide law enforcement authorities with evidence to support the credibility of a person's statements since FRT could be useful in the detection of emotions and affects. This kind of application encroaches on the unquestionable principles of criminal procedural law, such as the principle of free evaluation of evidence and the right to a fair procedure, and the paper calls for increased caution when standardizing this issue. The reliability of the results is still not at a satisfactory level, and even when it reaches such a level, there are still significant barriers regarding its application in criminal proceedings. The use of the FR tool for the purposes of verifying the credibility of statements by persons should definitely remain outside the sphere of verifying the credibility of the evidence on which the final verdict is based, that is, outside of the trial in which the *in dubio pro reo* rule applies. Namely, in order to pass a guilty verdict, we need to be sure of the defendant's guilt, guilt must be fully proven beyond reasonable doubt. Formulated in this way, the highest standards of evidence do not tolerate any numerical expression in percentages, nor any possible gradation. Therefore, it is necessary to insist on the consistent application of traditional and firmly rooted European legal standards, which must play a key role in shaping modern tools aimed at coping with contemporary criminal offenses, in order to protect the painstakingly built system of human rights from collapse under the guise of strengthening the efficiency of criminal proceedings.

REFERENCES

BOOKS

1. Damaška, M., *Dokazno pravo u kaznenom postupku: oris novih tendencija*. Pravni fakultet u Zagrebu, Zagreb, 2001
2. Krapac, D., *Kazneno procesno pravo*. Narodne novine, Zagreb, 2015

BOOK CHAPTERS

1. De Hert, P., Sajfert, J., *The Role of the Data Protection Authorities in Supervising Police and Criminal Justice Authorities Processing Personal Data*, in: Brière C, Weyembergh A (eds) The Needed Balances in EU Criminal Law. Hart, Oxford and Portland, Oregon, 2018, pp. 243-257

JOURNAL ARTICLES

1. Bacchini, F., Lorusso, L., *Race, again: how face recognition technology reinforces racial discrimination*, J Inf Commun Ethics Soc 17:321-335, 2019 [http://dx.doi.org/10.1108/JICES-05-2018-0050]
2. Bibas, S., *Transparency and Participation in Criminal Procedure*, N. Y. Univ. Law Rev. 81:911-966, 2006
3. Callananm G., *Does the Right to Privacy Apply to Facial Biometrics? Specifically, When Analyzed Under the European Convention on Human Rights*, Ga. J. Int'l & Comp. L. 49:351-369, 2021
4. De Hert, P., Papakonstantinou, V., *The New Police and Criminal Justice Data Protection Directive, A first analysis,* New J. Eur. Crim. Law 7:7-19, 2016, [https://doi.org/10.1177/203228441600700102]
5. Dessimoz, D., Champod, C., *A dedicated framework for weak biometrics in forensic science for investigation and intelligence purposes: The case of facial information*, Secur. J. 29:603–617, 2016, [https://doi.org/10.1057/sj.2015.32]
6. Gentzel, M., *Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy*, *Philos. Technol.* 34:1639–1663, 2021, [https://doi.org/10.1007/s13347-021-00478-z]
7. Gordon, BJ., *Automated Facial Recognition in Law Enforcement: The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police*, Potchefstroom Electronic Law Journal, 24:1–29, 2021, [https://doi.org/10.17159/1727-3781/2021/v24i0a8923]
8. Hacker, P., *Teaching fairness to artificial intelligence*, Common Mark. Law Rev. 55:1143 – 1185, 2018, [https://doi.org/10.54648/cola2018095]
9. Hill, D., O'Connor, CD., Slane, A., *Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making*, Int. j. police sci. manag. 24: 325-335, 2022, [https://doi.org/10.1177/14613557221089558]
10. Kostka, G., Steinacker, L., Meckel, M., *Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States*, Public Understanding of Science 30:671–690, 2021, [https://doi.org/10.1177/09636625211001555]
11. Kotsoglou, KN., Oswald, M., *The long arm of the algorithm? Automated Facial Recognition as evidence and trigger for police intervention*, Forensic Sci. Int.: Synergy. 2:86-89, 2022, [https://doi.org/10.1016/j.fsisyn.2020.01.002]
12. Leiser, MR., Custers, BHM., *The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680*, Eur. Data Prot. Law Rev. 5:367-378, 2019, [https://doi.org/10.21552/edpl/2019/3/10]

13. Leslie, D., *Understanding bias in facial recognition technologies: and explainer*, The Alan Turing Institute. 1-50, 2020, [https://doi.org/10.5281/zenodo.4050457]
14. Neroni Rezende, I., *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, New J. Eur. Crim. Law. 11:375-389, 2020, [https://doi.org/10.1177/2032284420948161]
15. Nesterova, I., *Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world, The 19th International Scientific Conference Globalization and its Socio-Economic Consequences 2019 – Sustainability in the Global-Knowledge Economy*, SHS Web Conf 74:1-8, 2020, [https://doi.org/10.1051/shsconf/20207403006]
16. Novokmet, A., *The Europeanization of the Criminal Proceedings in the Republic of Croatia through the Implementation of the Directive 2013/48/EU*, Eur. J. Crime Crim. Law Crim. Justice. 27:97-125, 2019, [https://doi.org/10.1163/15718174-02702002]
17. Novokmet, A., Tomičić, Z., Vinković, Z., *Pretrial risk assessment instruments in the US criminal justice system—what lessons can be learned for the European Union. International* Journal of Law and Information Technology, 30: 1–22, 2022, [https://doi.org/10.1093/ijlit/eaac006]
18. O'Flaherty, M., *Facial Recognition Technology and Fundamental Rights*, Eur. Data. Prot. Law. Rev. 6:170-173 2020, [https://doi.org/10.21552/edpl/2020/2/4]
19. Park, SJ., Kim, BG., Chilamkurti, N., *A Robust Facial Expression Recognition Algorithm Based on a Multi-Rate Feature Fusion Scheme*, Sensors 21:1-26, 2021, [https://doi.org/10.3390/s21216954]
20. Purshouse, J., Campbell, L., *Privacy, Crime Control and Police Use of Automated Facial Recognition Technology*, Criminal Law Review 3:188-204, 2019, [ISSN 0011-135X]
21. Raab, T., *Germany Video Surveillance and Face Recognition: Current Developments*, Eur. Data. Prot. Law. Rev. 5:544-547, 2019, [https://doi.org/10.21552/edpl/2019/4/14]
22. Raposo, VL., *The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal*, Eur J Crim Pol Res, 2022, [https://doi.org/10.1007/s10610-022-09512-y]
23. Ritchie, KL., Cartledge, C., Growns, B., Yan, A., Wang, Y., *et al.*, *Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world*, PLOS ONE 16:1-28, 2021, [https://doi.org/10.1371/journal.pone.0258241]
24. Roksandić, S., Protrka, N., Engelhart, M., *Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?*, 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, pp. 1227-1229, 2022, [doi: 10.23919/MIPRO55190.2022.9803606]
25. Rowe, EA., *Regulating Facial Recognition Technology in the Private Sector*, Stan. Tech. L. 24:1-54, 2020
26. Sarabdeen, J., *Protection of the rights of the individual when using facial recognition technology*, Heliyon, 2022, [https://doi.org/10.1016/j.heliyon.2022.e09086]
27. Stoykova, R., *Digital evidence: Unaddressed threats to fairness and the presumption of innocence*, Comput Law Secur Rev 42:1-20, 2021, [https://doi.org/10.1016/j.clsr.2021.105575]
28. Yassin, K., Jridi, M., Al Falou, A., Atri, M., *Face Recognition Systems: A Survey*, Sensors 20:1-36, 2020, [https://doi.org/10.3390/s20020342]

29. Zalnieriute, M., (2021) *Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State*, Science and Technology Law Review, 22:284–307, 2021, [https://doi.org/10.52214/stlr.v22i2.8666]

ONLINE DOCUMENTS

1. Autoriteit Persoonsgegevens, *Stappenplan camera bij huis*, 2020, available at: [https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stappenplan_camera_bij_huis.pdf], Accessed 13 July 2022
2. Big Brother Watch, *Face off: The lawless growth of facial recognition in the UK policing*, pp 1-51, 2018, available at: [https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf], Accessed 5 July 2022
3. Big Brother Watch, *Stop Facial Recognition*, 2022, available at: [https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/#breadcrumb], Accessed 15 June 2022
4. Bischoff, P., *Facial Recognition Technology (FRT): 100 countries analyzed*, 2021, available at: [https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/], Accessed 15 July 2022
5. Bischoff, P., *Surveillance camera statistics: which cities have the most CCTV cameras?*, 2021, available at: [https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/], Accessed 3 July 2022
6. Brandl, R., *The world´s most surveilled citizens*, 2021, available at: [https://www.tooltester.com/en/blog/the-worlds-most-surveilled-countries/], Accessed 3 July 2022
7. Buolamwini, J., Ordóñez, V., Morgenstern, J., Learned-Miller, E., *Facial Recognition Technologies: A Primer*, Algorithmic Justice League. pp 2-16, 2020, available at: [https://assets.websitefiles.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf], Accessed 28 July 2022
8. Davies, B., Innes, M., Dawson, A., *An Evaluation of South Wales Police's Use Of Automated Facial Recognition*, Universities' Police Science Institute Crime & Security Research Institute, pp 1-45, 2018, available at: [https://static1.squarespace.com/static/51b06364e4b02de2f57fd72e/t/5bfd4fbc21c67c2cdd692fa8/1543327693640/AFR+Report+%5BDigital%5D.pdf], Accessed 15 July 2022
9. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, *Einsatz der Gesichtserkennungssoftware „Videmo 360" durch die Polizei Hamburg zur Aufklärung von Straftaten im Zusammenhang mit dem in Hamburg stattgefundenen G20-Gipfel*, 2018, available at: [https://datenschutz-hamburg.de/assets/pdf/Anordnung_HmbBfDI_2018-12-18.pdf], Accessed 15 July 2022
10. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, available at:

[https://eurlex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:32016L0680&from=HR], Accessed 18 June 2022

11. Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, available at:
[https://eurlex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:32013L0048&from=HR], Accessed 17 June 2022
12. Dushi, D., *The use of facial recognition technology in EU law enforcement: Fundamental rights implications*, Policy Briefs 2020, available at:
[https://tinyurl.com/3dnc69j3], Accessed 28 July 2022
13. DutchNews.Nl, *Dutch police can access 200,000 private security cameras, campaign for more*, 2019, available at:
[https://www.dutchnews.nl/news/2019/01/dutch-police-can-access-200000-private-security-cameras-campaign-for-more/], Accessed 13 July 2022
14. European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence*, 2021, available at: [https://www.echr.coe.int/documents/guide_art_8_eng.pdf], Accessed 15 June 2022
15. European Court of Human Rights, *Guide to the Case-Law of the European Court of Human Rights – Data protection*, 2022, available at: [https://echr.coe.int/Documents/Guide_Data_protection_ENG.pdf], Accessed 20 June 2022
16. European data protection board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, 2022, available at:
[https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf], Accessed 20 June 2022
17. European Parliament, *Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters 2020/2016(INI)*, 2021, available at: [https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html], Accessed 18 June 2022
18. Fair Trials, *Automating injustice: The use of artificial intelligence & automated decision-making systems in criminal justice in Europe*, pp. 1-47, 2021, available at:
[https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf], Accessed 13 July 2022
19. Kak, A., *The State of Play and Open Questions for the Future*, in: Kak A (ed) Regulating Biometrics: Global Approaches and Urgent Questions, AI now Institute, pp. 16-43, 2020, available at:
[https://ainowinstitute.org/regulatingbiometrics.html], Accessed 20 June 2022
20. Kayser-Bril, N., *At least 11 police forces use face recognition in the EU*, AlgorithmWatch, 2020, available at:
[https://algorithmwatch.org/en/face-recognition-police-europe/], Accessed 15 July 2022
21. Kritikos, M., *Artificial Intelligence ante portas: Legal & ethical reflections*, European Parliamentary Research Service, Scientific Foresight Unit (STOA), available at: [https://www.europarl.

europa.eu/RegData/etudes/BRIE/2019/634427/EPRS_BRI(2019)634427_EN.pdf], accessed 13 July 2023

22. Madiega, T., Mildebrath, H., *Regulating facial recognition in the EU*. European Parliamentary Research Service, 2021, available at: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf], Accessed 15 August 2022
23. Monroy, M., *Security Architectures in EU: G20 in Hamburg: Data protection commissioner considers face recognition illegal*, 2018, available at: [https://digit.site36.net/2018/08/15/g20-in-hamburg-data-protection-commissioner-considers-face-recognition-illegal/], Accessed 15 July 2022
24. Montag, L., Mcleod, R., De Mets, L., Gauld, M., Rodger, F., Pełka, M., *The rise and rise of biometric mass surveillance in the EU: A legal analysis of biometric mass surveillance practices in Germany, The Netherlands, and Poland*, pp. 1-158, 2019, available at: [https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf], Accessed 3 July 2022
25. Politie, *Centrale Automatische TeChnologie voor Herkenning (CATCH)*, Jaarcijfers, 2020 available at: [https://www.politie.nl/binaries/content/assets/politie/onderwerpen/forensische-opsporing/catch-jaarcijfers-2020-hr-online.pdf], Accessed 13 July 2022
26. Politie, *Camera in Beeld*, 2022, available at: [https://www.politie.nl/onderwerpen/camera-in-beeld.html], Accessed 13 July 2022
27. South Wales Police, *Facial Recognition Technology*, 2020, available at: [https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/], Accessed 4 July 2022
28. The European Commission (2021) Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial intelligence act) and amending certain Union legislative acts. COM(2021) 206 final, available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206], Accessed 6 July 2022
29. The European Parliament and the Council (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, available at: [https://eur-lex.europa.eu/eli/reg/2016/679/oj], Accessed 6 July 2022
30. Waarlo, N., Verhagen, L., *De stand van gezichtsherkenining in Nederland, de Volkskrant*, 2020, available at: [https://www.volkskrant.nl/kijkverder/v/2020/de-stand-van-gezichtsherkenning-in-nederland~v91028/?referrer=https%3A%2F%2Fwww.google.com%2F], Accessed 14 July 2022
31. Wet politiegegevens, *BWBR0022463*, 2020, available at: [https://wetten.overheid.nl/BWBR0022463/2020-01-01/0], Accessed 13 July 2022
32. Wired, *Europe Is Building a Huge International Facial Recognition System*, 2022, available at: [https://www.wired.com/story/europe-police-facial-recognition-prum/], Accessed 16 June 2022

CASE LAW

1. High Court of Justice (Queen's Bench Divison) Division Court (2019) Edward Bridges v The Chief Constable of South Wales Police. Case No: CO/4085/2018. EWHC 2341, available at: [https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf], Accessed 6 July 2022
2. Judgment *Gaughran v The United Kingdom* (2020) EHRR, No. 45245/15, 13 February 2020, available at: [https://hudoc.echr.coe.int/fre?i=001-200817], Accessed 17 June 2022
3. Judgment *P. N. v Germany*, (2020) EHRR, No. 74440/17, 11 June 2020, available at: [https://hudoc.echr.coe.int/rus?i=001-202758], Accessed 17 June 2022
4. Judgment *Peck v. United Kingdom* (2003) EHRR, No. 44647/98, 28 January 2023
5. Judgment *Reklos and Davourlis v Greece* (2009) EHRR, No. 1234/05, 15 January 2009, available at: [https://hudoc.echr.coe.int/eng?i=001-90617], Accessed 17 June 2022
6. Judgment *S. and Marper v. the United Kingdom* (2008) EHRR, No. 30562/04 and 30566/04, 4 December 2008, available at: [https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-1784%22]}], Accessed 17 June 2022
7. OVG Nordrhein-Westfalen (2022) 5 B 137/21, available at: [https://www.justiz.nrw.de/nrwe/ovgs/ovg_nrw/j2022/5_B_137_21_Beschluss_20220516.html], Accessed 5 July 2022
8. Rechtbank Zeeland-West-Brabant (2019) case No. 02-665274-18. ECLI:NL:RBZWB:2019:2191, available at: [https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBZWB:2019:2191], Accessed 8 July 2022
9. The Court Of Appeal (Civil Division) (2020) R (on the application of Edward Bridges) v The Chief Constable of South Wales Police. Case No: C1/2019/2670. EWCA Civ 1058, available at: [https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf], Accessed 6 July 2022
10. Verwaltungsgericht Hamburg (2019) Urteil. case no. 17 K 203/19, available at: [http://justiz.hamburg.de/contentblob/13535554/cc5a1e8c70c95088220147f57921d22d/data/17-k-203-19.pdf], Accessed 5 July 2022
11. VG Köln (2020) 20 L 2340/19, available at: [http://www.justiz.nrw.de/nrwe/ovgs/vg_koeln/j2020/20_L_2340_19_Beschluss_20201210.html], Accessed 5 July 2022