ARTICLES

SCHENGEN AND EUROPEAN BORDERS
*edited by* Iris Goldner Lang

# BIOMETRIC BORDERS ENVISAGED BY FRONTEX: FUNDAMENTAL RIGHTS IN THE BACKSEAT

MATIJA KONTAK*



ABSTRACT: This *Article* provides an assessment of the biometric policy of the European Border and Coast Guard Agency (Frontex) and its consequences for the fundamental rights of migrants. It provides an overview of the technological aspects of biometrics, their application, and the legal framework in the context of the Area of Freedom, Security and Justice. This sets the background for an analysis of how and why Frontex uses biometrics to advance its goals. This *Article* analyses policy papers, legal provisions, and other sources, but particularly the Technology Foresight on Biometrics for the Future of Travel, a report on biometrics published by Frontex. This *Article* concludes that Frontex fails to account for the consequences of its biometric policy on fundamental rights when considering the effects of biometric technologies for the future.

KEYWORDS: Frontex – biometrics – biometric data – personal data – fundamental rights – privacy.

## I. INTRODUCTION

This *Article* aims to critically examine the policy of the European Border and Coast Guard Agency (Frontex) on biometric technologies used in the EU and its impact on the protection of fundamental rights. In particular, this *Article* argues that Frontex fails in its legal obligation to respect fundamental rights in relation to its biometric policy.[1]

* Research Assistant, University of Zagreb, matija.kontak@pravo.unizg.hr. This *Article* is the result of the author's research within the framework of the project on "Algorithmic Fairness for Asylum Seekers and Refugees (AFAR)". More details about the project are available at www.hertie-school.org.

[1] EU law uses the terminology of fundamental rights instead of human rights. In this *Article*, the fundamental rights concept is mostly used, even though in international law and in the European Convention on Human Rights (ECHR) the term is human rights.


www.europeanpapers.eu
ISSN 2499-8249
doi: 10.15166/2499-8249/773

This *Article* consists of two main parts. The first explains how biometric technologies work, where they are used and what the applicable legal framework is in the EU. The second part explains the role of Frontex concerning biometric technologies in the EU, especially in the light of the report which Frontex published on the future of biometrics in border management.[2] This *Article* argues that considerations of fundamental rights, particularly privacy and data protection, are lacking in Frontex's approach to the future of biometrics.

## II. Technological and legal aspects of biometrics

### II.1. Technological aspects and the application of biometrics in the EU

The terms "biometrics", "biometric technologies", and "biometric data" can be hard to distinguish, especially in the realm of law.[3] Biometrics mean automated recognition of individuals based on human characteristics.[4] Biometric technologies are a group of modern technologies that allow identification of persons.[5] For example, 3D facial recognition technology identifies a person by the geometry of their face. Other prominent biometric technologies include iris recognition (which can employ natural light, infrared light, or other means to scan the iris) and fingerprint recognition (with many modes of comparing fingerprints). However, biometric technologies differ in how developed a certain technology is, how accurate it is, how acceptable it is to the public, and how fast and how cheaply a biometric technology operates. Most importantly, biometric technologies have different impacts on privacy and other fundamental rights.

Biometrics can be used unimodally, meaning that only one mode or biometric technology is applied in a particular instance. However, biometrics are increasingly used multimodally, meaning that more than one biometric technology is applied. An example of a multimodal system is the upcoming Entry Exit System (EES), which will require both fingerprints and facial recognition as an identity check.[6] Using more biometric technologies increases the accuracy and security of the system, but further infringes the privacy of the

[2] Frontex, *Technology Foresight on Biometrics for the Future of Travel* (European Border and Coast Guard Agency, 2022) www.frontex.europa.eu.

[3] One paper that tackles the problematic terminology of biometrics is by C Jasserand, 'Avoiding Terminological Confusion between the Notions of "Biometrics" and "Biometric Data"' (2016) International Data Privacy Law 63.

[4] International Organization for Standardization, *ISO/IEC 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics* www.iso.org.

[5] A distinction is often made between identification and verification. Identification is understood as meaning establishing who a person is among many persons (one-to-many comparison), while verification means checking whether the person present is the same as the person in the document (one-to-one comparison).

[6] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) (EES Regulation), art. 17.

individual.[7] The question arises as to what exactly are the limits of multimodal biometrics: could three or five biometric technologies be applied in parallel if they further increase accuracy and reduce the risk of fraud?

Biometric technologies change the notion of identification; instead of presenting a travel document to another person, people present their own bodies to a machine as a means of identification. Individuals can benefit from biometrics. Biometrics can be used to identify unaccompanied children or missing persons who can be recognised by their physical features and connected with their families. Biometric technologies promise border checks without our stopping, with only an invisible radar tacitly scanning our (happy) faces as we walk through an "e-gate" corridor. An ideal case would be to utilize a biometric technology that does not disturb the migrant, that shortens the time to cross a border, and where biometric data are neither stored nor accessible for other purposes. However, once collected, biometric data may be used for many purposes.

Public authorities of the EU Member States rely on biometric technologies in their role concerning migration, asylum, and border management. For example, border guards use human presence detectors that look for hidden movements or heartbeats inside lorries crossing into the EU.[8] Aerial drones with image recognition and infrared cameras are used by Frontex as well as national authorities to "control" the vast maritime borders of the EU.[9] Most EU Member States today have databases of millions of fingerprints, facial recognition, or DNA profiles (or all of these) which can be searched by modern computer algorithms.[10] These national databases of biometric data are mostly for law enforcement purposes and may have different rules on what type of data is stored, for how long, or who can access it. Human rights issues raised by these national biometric databases represent the "biometric" case law before the European Court of Human Rights (ECtHR).[11]

There are EU information systems which are fundamental to the operation of the Area of Freedom, Security and Justice. The European Asylum Dactyloscopie Database (Eurodac) relies on fingerprint recognition as a means of identifying and allocating responsibility for asylum seekers among Member States.[12] EES will collect fingerprints and facial images of travellers to the EU who do not need a long-term visa, and Member States will be able to

[7] G González Fuster and M Nadolna Peeters, *Person Identification, Human Rights and Ethical Principles: Rethinking Biometrics in the Era of Artificial Intelligence* (European Parliamentary Research Service Scientific Foresight Unit, December 2021) www.europarl.europa.eu.

[8] Science for Humanity, Human Presence, Movement & Heartbeat Detection System (MDS) s4h.be.

[9] Frontex, presentation on large hybrid drones, available at www.frontex.europa.eu.

[10] At least eleven EU Member States have biometric databases with facial recognition. F Ragazzi, E Mendos Kuskonmaz, IZ Plájás, R Van de Ven, B Wagner, *Biometric & Behavioural Mass Surveillance in EU Member States* (Report for the Greens/EFA in the European Parliament, October 2021) extranet.greens-efa-service.eu 38.

[11] *Infra*, section II.2.*(a)*

[12] Regulation (EU) 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of "Eurodac" (Eurodac regulation), art. 1(1).

choose which of the two will be the main biometric identifier for identity verification.[13] Authorised staff of Frontex will have access to the biometric data collected by EES.[14] Frontex is involved in the future development of EES and its biometric aspects.[15] Another valuable information system is the Schengen Information System, upgraded in 2023 to include biometrics such as palm prints, fingerprints, as well as DNA records in the case of missing persons.[16] There are other EU information systems or information exchange frameworks which concern biometric data. Some of these systems will become interoperable, which will make it easier for public authorities to access personal and biometric data.[17]

### II.2. Biometric legal framework

In the EU, especially in relation to migration, asylum, and law enforcement, biometrics are regulated by primary law and by secondary legislation.[18] The first is the human rights framework of the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights (CFR). The other important legal framework concerning biometrics is the data protection framework of the EU, in particular the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED), and their provisions regarding biometric data protection.[19]

*a) Biometrics and fundamental rights*

The use of biometric technologies raises fundamental rights issues, in particular concerning privacy, non-discrimination, and human dignity. The CFR is applicable to institutions, bodies, offices, and agencies of the EU and to Member States when they are applying EU law.[20] The meaning and scope of rights in the CFR is the same as those same rights laid out in the ECHR.[21] The CFR has distinct rights to privacy (art. 7) and to data protection

[13] Regulation (EU) 2017/2226 cit. 20–82 (EES Regulation).

[14] *Ibid*. art. 63.

[15] Frontex, *Technology Foresight on Biometrics for the Future of Travel* cit. 106.

[16] Commission Implementing Decision (EU) 2023/201of 30 January 2023 setting the date on which operations of the Schengen Information System start pursuant to Regulation (EU) 2018/1861 of the European Parliament and of the Council and Regulation (EU) 2018/1862 of the European Parliament and of the Council.

[17] N Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill 2022).

[18] E Kindt, 'Biometric Data Processing: Is the Legislator Keeping Up or Just Keeping Up Appearances?' in G González Fuster, R Van Brakel and P De Hert (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar Publishing 2018) 389.

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 General Data Protection Regulation – GDPR; Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 Law Enforcement Directive – LED.

[20] Charter of Fundamental Rights of the European Union [2012] (CFR), art. 51.

[21] Arts 52(3) and 53 of the Charter.

(art. 8), while the ECHR in its right to privacy also encompasses the right to data protection.[22]

The ECtHR decides the impact of modern technologies (and biometrics in particular) on human rights through the lens of art. 8 ECHR which protects the right to private and family life. Art. 8(2) ECHR provides that interference by a public authority with the right to private life of an individual is justified if it is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[23] *S and Marper v UK* is the emblematic case, both for modern technologies in general and for biometric technologies in particular.[24] It concerns the collection and storage of fingerprints and DNA samples of persons who were acquitted but with the data being retained indefinitely by the police. The judgment in *S and Marper* is important because the Court established a framework for dealing with biometric technologies in the context of human rights, particularly the right to private life. Further, the Court distinguished between the taking of biometric samples, storing these samples, and processing the data as separate interferences with the right to private life.[25]

The concrete facts of each specific case are crucial for determining the fundamental rights implications. These facts include: what biometric technology is used (as DNA profiling infringes the right to privacy more than the taking of fingerprints), for how long the biometric or personal data are stored, who can access the data, which categories of persons must have their biometric data collected, what are the qualities of the law prescribing the use of biometric technology in terms of the possibility of review of a decision to store biometric data and effective oversight.[26] The mere collection of biometric data infringes privacy, regardless of if or for how long such data are stored.[27] To justify interference with a right, there must be a legitimate aim for the interference by public authorities with the fundamental right (in the case of the CFR) or a human right (in the case of the ECHR). Furthermore, the assessment of interference is conducted via a proportionality test, but the essence of a human (or fundamental) right must not be infringed.[28]

[22] ECtHR *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* App n. 931/13 [6 November 2017] GC para. 137.

[23] Art. 8(2) ECHR.

[24] ECtHR *S and Marper v UK* App n. 30562/04 and 30566/04 [4 December 2008] GC.

[25] *Ibid*. para. 120.

[26] *Ibid*.

[27] *Ibid*.

[28] Not adhering to basic principles of data protection infringes the core of the fundamental right to data protection: case C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238 para. 40. The essence, or the core, of the fundamental right in the context of data protection was also elaborated in the following judgments: case C-203/15 *Tele2 Sverige* ECLI:EU:C:2016:970 para. 101; joined cases C-511/18 *Quadrature du Net* ECLI:EU:C:2020:791.

Newer "biometric" case law follows the reasoning of *S and Marper v UK*. In *Gaughran v UK*, the ECtHR decided that the indefinite detention of the biometric data of convicted persons is contrary to the right to private life under art. 8 ECHR.[29] In *Glukhin v Russia*, the ECtHR ruled that facial recognition software used by public authorities against a peaceful sole protester conflict with the ideals and values of a democratic society and is therefore contrary to art. 8 ECHR.[30]

In the EU's fundamental rights framework, the CFR in many respects corresponds to the ECHR. This includes the right to private and family life under art. 7 CFR, which is almost identical to art. 8 ECHR. However, unlike the ECHR, the CFR has a separate explicit right to data protection contained in its art. 8. The CFR prescribes that a measure interfering with a fundamental right must genuinely meet the objectives of general interest recognised by the EU or the need to protect the rights of others, but additionally the "essence" of a fundamental right, privacy in this case, must be respected.[31]

The case law of the Court of Justice of the EU (CJEU) indicates that there is a justified interference with the right to privacy in having to provide two fingerprints to be stored on the chip of a biometric passport for the purpose of preventing identity fraud and illegal migration.[32] The *Willems* case adds that public authorities, considering again art. 7 CFR, do not have to guarantee that biometric data processed for passports will not be used for other purposes.[33] These judgments of the CJEU explicitly established that biometric technologies may be allowed in certain instances and that their use is assessed via arts 7 and 8 CFR, along with secondary legislation on data protection.

Besides privacy and data protection, other fundamental rights may come into consideration when applying biometrics. Primarily, human dignity[34] may be affected by the way in which a biometric technology operates or by the data it processes. In the case of fingerprinting, human dignity may be infringed by the coercive nature of the procedure, particularly in cases where certain categories of persons, such as irregular migrants or asylum seekers, are forced to choose between having their fingerprints taken or possible detention along with the loss of access to asylum. There is also an issue on how human dignity is affected if fingerprints are forcefully taken, and what it means to have fingerprints forcefully taken in the case where a person does not fully comprehend the procedure or their rights.[35]

[29] ECtHR *Gaughran v UK* App n. 45245/15 [13 June 2020].

[30] ECtHR *Glukhin v Russia* App n. 11519/20 [4 July 2023].

[31] Art. 52(1) of the Charter.

[32] Case C-291/12 *Schwarz* ECLI:EU:C:2013:670.

[33] Case C-446/12 *Willems* ECLI:EU:C:2015:238.

[34] Art. 1 of the Charter.

[35] EU Fundamental Rights Agency (FRA) notes that sometimes fingerprints are forcefully collected and advises that fingerprinting should not be forced: fra.europa.eu. FRA advises authorities to repeatedly give information on why fingerprints are taken in the context of Eurodac to "reduce the risk to resort to coercive measures" edps.europa.eu.

Human dignity may also be affected by facial recognition technology. As it is put in the EDPB Guidelines 05/2022 on the use of facial recognition technology in law enforcement: "[h]uman dignity requires that individuals are not treated as mere objects. FRT [facial recognition technology] calculates existential and highly personal characteristics, the facial features, into a machine-readable form with the purpose of using it as a human license plate or ID card, thereby objectifying the face".

Facial recognition raises issues of the fundamental right to non-discrimination. Facial recognition may not recognise equally well black as opposed to white faces, and female faces as opposed to male.[36] However, facial recognition algorithms are rapidly improving, and newer algorithms may no longer discriminate in a statistically significant manner.[37] Nevertheless, the right to be treated equally remains an important safeguard which must be accounted for in all stages of the deployment of a biometric technology. The biometric algorithm must perform well in tests, be trained on representative data, and at least perform better than a human border guard inspecting a photo in a travel document with their naked eye and inherent human prejudice.

*b) Biometrics and EU data protection legislation*

The use of biometric technologies which results in the processing of personal data is also regulated by secondary legislation on data protection, in tandem with primary legislation concerning fundamental rights. Broadly speaking, public authorities use biometric technologies for two purposes, with different data protection legal bases: for law enforcement and for migration, asylum, and border control purposes. The processing of personal data means performing any operation, automated or not, on information that relates to an identified or identifiable natural person. Biometric data are defined in the GDPR as "personal data resulting from specific technical processing [...] which allow or confirm the unique identification of that natural person [...]".[38] This definition is very narrow because it restricts the concept of biometric data only to those data that result from a technical process (*e.g.* machine reading a document) and only for the purpose of unique identification.[39]

[36] J Buolamwini and T Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) Proceedings of Machine Learning Research; P Grother, M Ngan and K Hanaoka, 'Face Recognition Vendor Test Part 3: Demographic Effects' (19 December 2019) NIST publication.

[37] "We consider demographics, and note that for the more accurate algorithms, error rates are so low that accuracy variations across sex and race are insignificant", in P Grother, A Hom, ML Ngan and K Hanaoka, 'Face Recognition Vendor Test (FRVT) Part 7: Identification for Paperless Travel and Immigration' (13 July 2021) NIST publication 8381.

[38] Art. 4(14) GDPR cit. Emphasis added.

[39] On the legal nature of biometric data, see C Jasserand, 'Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data' (2016) European Data Protection Law 297–311; G González Fuster and M Nadolna Peeters, *Person Identification, Human Rights and Ethical Principles: Rethinking Biometrics in the Era of Artificial Intelligence* (European Parliamentary Research Service Scientific Foresight Unit, December 2021) www.europarl.europa.eu.

The use of biometric technologies can be legally viewed as either the processing of personal data, in the case of biometric technologies which have the purpose of categorisation, or as the processing of biometric data, if it concerns processing by technical means for the purpose of unique identification. Biometrics can be used for purposes other than identification: to categorise people by their age, gender or by other attributes determined by biometrics. Biometrics can be used to ascertain whether a car driver is drowsy or whether a person in a public space is carrying something akin to a weapon. In these cases, persons are not necessarily uniquely identified by biometrics. Therefore, such (biometric) data processing may not fall in the ambit of biometric data processing as defined in EU law, but in the broader context of the processing of personal data. What is more, in some cases of biometric categorisation in which people are categorised on the basis of "special categories" of personal data (for example, by their ethnic origin, health status or sexual orientation), again the stricter rules of art. 9 GDPR, which establish conditions for the processing of special categories of personal data, such as biometric, health or ethnic data, apply. Finally, in limited circumstances (*e*.*g*. because of specific encryption methods), the processing of information by biometric technologies may not relate either to an identified or identifiable natural person. Such processing of anonymous information is not the processing of personal data and is therefore not regulated by the GDPR. Thus, we can conclude that biometric technologies in the context of migration, asylum, and law enforcement are used for the processing of biometric data, or, in the case of categorisation, the processing of personal data. However, in the context of the biometric technologies considered in this article, the purpose is precisely the unique identification of a natural person by technical means. Consequently, such processing of data can be labelled biometric data processing.

The principles of processing personal data, prescribed in art. 5 GDPR, pose limitations to the operating of biometric technologies. Biometric technologies are sophisticated and opaque in operation, which presents a challenge for the principle of fairness and transparency of data processing. Biometric technologies tend to result in an abundance of sensitive data on the subject, particularly in the case of DNA profiling, and this raises challenges for the principle of data minimisation. Biometric technologies are not error-proof, and some, such as facial recognition, must be especially considered in the light of the accuracy principle. Biometric data processing means transposing unique physical human characteristics into digital data (which can then easily be shared, stored, and copied). Thus, key issues concerning the use of biometric technologies are framed by the principles of storage limitation, purpose limitation, and the integrity and confidentiality of the data. This last issue of the security of personal and biometric data is related to "privacy by design" covered in art. 25(1) GDPR, which require that state-of-the-art technologies and techniques be used. Among the rights of data subjects stipulated by the GDPR, in the context of biometric technologies, the right not to be subject to a decision solely based

on automated decision-making is particularly important, but with a relevant exception in the case where the automated decision is based on law and "to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests".[40]

Art. 9(2)(g) GDPR is important as it provides the legal basis for the processing of biometric data by public authorities. The processing is allowed provided it is necessary for reasons of substantial public interest and based on a law proportionate to the aim pursued. Additionally, it needs to respect the essence of the right to data protection and provide safeguards for the fundamental rights of the data subject. These conditions overlap significantly with the conditions of art. 7 CFR and art. 8 ECHR, as these also contain a proportionality test. The GDPR, however, does not apply to all processing of biometric data. When personal data are processed for the purposes of law enforcement, the LED is applicable. In comparison to the GDPR, the LED is less stringent in allowing the processing of biometric data.[41]

The processing of personal or biometric data for law enforcement purposes is regulated by the Law Enforcement Directive as a *lex specialis*. Art. 3(13) LED defines biometric data in the same manner as art. 4(14) GDPR. The LED specifically requires that data controllers distinguish between distinct categories of data subjects, such as those convicted of a crime, those under suspicion, victims, and other parties such as witnesses. Processing must be necessary for the purpose of law enforcement and based on law which specifies the objective and purpose of the processing and the personal data to be processed. The GDPR in principle prohibits the processing of biometric data and then lists exceptions to this prohibition, including the processing of biometric data for reasons of substantial public interest. On the other hand, the LED allows the processing of special categories of personal data, including biometric data, where strictly necessary and authorised by law. Public authorities processing biometric data must also adhere to the principles of data processing under art. 4 LED.

Many of these issues related to biometric data processing were addressed by the CJEU in a recent judgment. In case C-205/21 *Ministerstvo na vatreshnite raboti*, the CJEU found that the processing of biometric (and genetic) data by police authorities is allowed for the purpose of law enforcement if based on a sufficiently clear and precise national law prescribing such processing even if this national law mistakenly refers to the GDPR instead of the LED.[42] The CJEU determined that the processing of biometric data under the LED is allowed only if strictly necessary, with required safeguards, while the processing of biometric data under the GDPR is prohibited, but with a list of exceptions. Thus, there must no ambiguity in the interpretation of national law about which one is the correct legal basis. If there is a conflict between national provisions that seem to allow and

[40] Art. 22(2)(b) GDPR cit.

[41] Compare art. 10 LED cit. 10 with art. 9(2) GDPR cit.

[42] Case C-205/21 *Ministerstvo na vatreshnite raboti* ECLI:EU:C:2023:49.

those that seem to preclude data processing, the solution of the conflict is to favour the interpretation that secures the effectiveness of the LED. The CJEU states that distinct categories of data subjects, such as those convicted as opposed to those only suspected of a crime, must be treated differently regarding interference with their fundamental rights. The CJEU concludes that art. 10 LED, which sets the conditions for the processing of special categories of data (including biometric data) read with the LED principles of lawfulness, fairness, legitimate purpose and data minimisation, prohibits national legislation which requires the systematic collection of biometric and genetic data of persons accused of an intentional offence if such national legislation does not provide that competent national authorities can verify that it is strictly necessary and that there are no other means available that cause less serious interference with the rights and freedoms of the data subject.

*c) Biometrics, Frontex and the Artificial Intelligence Act*

Artificial Intelligence Act (AI Act)[43] will greatly influence the legal framework for biometrics in the EU and it can be counted among the "basic" rules for application of biometrics along with GDPR and LED that Frontex will have to consider. However, the relationship between AI Act and biometrics is highly complex. Biometric-related terms are mentioned over a hundred times in AI Act.[44] This legislation also defines for the first time in EU law important biometric concepts, such as biometric categorisation.[45] A complete overview of biometric side of AI Act cannot be given here, but certain highlights that may affect biometric practices of Frontex can be made.

AI Act creates what can be called a risk pyramid of AI practices, from those that carry no obligations for providers or deployers to those AI practices that are prohibited. High-risk AI systems must satisfy requirements stipulated by the AI Act.[46] High-risk AI systems include the biometric information systems of the EU used in migration, asylum and border control.[47] Certain special exemptions or carve-outs for these systems are provided in the AI Act.[48] Biometrics are explicitly named as a high-risk AI practice (even though it could be argued that not all sorts of biometrics entail AI).[49]

At the pinnacle of the AI Act's risk pyramid are the prohibited AI practices. Many of those prohibited practices are of biometric nature. AI Act prohibits AI systems that create

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

[44] The term "biometric" is mentioned 122 times in various forms in the Artificial Intelligence Act.

[45] See Regulation (EU) 2024/1689 cit. recital 16 and 30, art. 3(40).

[46] Arts 8-28 Regulation (EU) 2024/1689 cit.

[47] Annex III, point 7 Regulation (EU) 2024/1689 cit.

[48] See Regulation (EU) 2024/1689 cit. art. 14(5) second paragraph; art. 78(3); recital 73 last sentence.

[49] Annex III, point 1 Regulation (EU) 2024/1689 cit.

facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.[50] This was the business model of Clearview AI, an American tech company that offered law enforcement bodies the possibility to identify persons from their public social network profiles and similar sources. Prohibited are also biometric categorisation systems that categorise natural persons based on their biometric data to discern their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation, but here law enforcement is exempted from this prohibition.[51] Among the prohibited AI practices listed in the AI Act, most space is devoted to so-called real time remote biometric identification. But instead of making it prohibited, AI Act in art. 5(1)(h) and 5(2) to 5(8) stipulates the conditions by which this practice can be used for the purpose of law enforcement.

This kind of biometric surveillance has strong negative effects for fundamental rights of any person subjected to it, which the AI Act itself recognizes.[52] The use of surveillance with facial recognition has been deemed to cause a *chilling effect* on human rights, a legal term denoting the idea that persons do not engage in legal behaviour such as gathering in public places or expressing their political opinions due to the fear of being subjected to repression.[53] Nevertheless, real time remote biometric identification is expressly allowed by the AI Act, in its art. 5(d) and further, subject to conditions stated there. What is more, these provisions act as *lex specialis* in relation to Law Enforcement Directive.[54] This means AI Act explicitly allows biometric surveillance even if by an interpretation of LED, it would have been illegal. All this naturally helps Frontex to keep its biometric options open in contemplating the future.

Finally, AI Act grants special status to large scale information systems of the EU by giving those systems an extra time to comply with the provisions of AI Act.[55] These include the biometric based systems of Eurodac, Schengen Information System, Visa Information System and other, in which Frontex has a certain role, as mentioned previously.

In conclusion, AI Act will be another factor that Frontex has to consider while conducting its biometric policy and practices. Unfortunately, in the opinion of this Author, AI Act will not provide an effective new means of control of Frontex in relation to biometrics and fundamental rights. This is obvious from the effort of the legislator to carve special status for EU's own biometric information systems, further from the special consideration of biometric (AI) systems used for migration, asylum and border control and finally from

[50] Art. 5(1)(e) Regulation (EU) 2024/1689 cit.

[51] Art. 5(1)(g) Regulation (EU) 2024/1689 cit.

[52] Recital 32 Regulation (EU) 2024/1689 cit. states that real-time remote biometric identification "may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights".

[53] *Glukhin v Russia* App. no. 11519/20 [4 July 2023].

[54] Recital 38 Regulation (EU) 2024/1689 cit.

[55] Art. 111 Regulation (EU) 2024/1689 cit.

the fact that some of the most notorious practices, such as real time remote biometric identification, have been given a green light by the AI Act.

On the brighter side for fundamental rights of individuals, AI Act brings a newer, deeper understanding of biometrics by introducing new concepts into EU law as well as by recognizing in its recitals the dangers for privacy, non-discrimination and human dignity raised by biometrics. Finally, unlike previous drafts, AI Act does not exclude EU large scale biometric systems, such as Eurodac, from its meagre obligation, but instead gives those systems merely a longer period to comply with AI Act's conditions. Frontex will have to at least notionally consider this additional set of basic rules (additional to GDPR and LED) when using biometric identification systems in its "supportive" roles in migration, asylum and border control roles as well as law enforcement.

## III. Frontex's Biometric Policy and Fundamental Rights

### III.1. Frontex's role and legal obligations concerning biometrics

Frontex is an essential element in the EU biometric network spanning Member States, multiple EU bodies, and information systems. It is an EU agency involved in border checks and border surveillance which coordinates, assists, and monitors how Member States control their borders if those are also the EU's external borders. It leads research and innovation regarding the application of modern technologies for border control.[56] Besides research and innovation, the importance of Frontex for biometrics is its role in assisting Member States at their borders, which includes the use of biometric technologies for identification and other purposes. This EU agency is an integral component of European integrated border management (EIBM).[57] EIBM's purpose is to help manage regular and irregular migration, at the same time upholding fundamental rights.[58] Frontex is particularly responsible for contributing to research and innovation related to EIBM and in helping Member States to develop their technological capacities.[59] The idea of EIBM is to incorporate all the elements needed for protection of the border: border checks, control and surveillance, search and rescue operations as well as using "state of the art technology" and "remaining abreast of the latest developments in technologies for border management".[60] The duties of Frontex are many but are often ancillary in character: it is obliged to "monitor", provide "support", "assist", "provide assistance" or "cooperate".[61]

[56] Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard (Frontex Regulation), art. 3(2).

[57] *Ibid*. art. 4.

[58] *Ibid*. Recital 1.

[59] *Ibid*. art. 66.

[60] Frontex, 'Technology Foresight on Biometrics for the Future of Travel' 3.

[61] Art. 10(1) Frontex Regulation cit.

Frontex has such a large and growing number of responsibilities that the Article remunerating the tasks assigned to Frontex runs out of letters of the alphabet.[62] Given the ancillary nature of its tasks, it is difficult to pin legal responsibility on Frontex directly.[63] However, since the changes made to its mandate in 2019, Frontex has evolved from a border control agency to a "powerful information hub" alongside Europol.[64] Frontex cooperates with other organisations, primarily Eurojust and Europol, but also national law enforcement bodies to facilitate the exchange of information.[65] The processing of personal data in the context of the Frontex regulation is governed by a tailor-made regulation concerning the processing of personal data by EU authorities, which combines the provisions of LED and GDPR.[66]

Frontex is obliged to respect fundamental rights in all its activities.[67] To drive home this message, "fundamental right(s)" are mentioned over 200 times in the Frontex regulation. Frontex Technology Foresight on Biometrics for the Future of Travel (Frontex Study or Study) states that "fundamental rights are a cross-cutting component" of EU border management.[68] Despite this, Frontex has been associated with scandals concerning fundamental rights, notably in a report by the European Anti-Fraud Office in 2022.[69] Frontex has repeatedly been accused of facilitating pushbacks.[70] In response to the perceived fundamental rights deficiencies, Frontex has been reformed more than once. Some of the newer developments for this purpose have been the creation of a consultative forum to advise Frontex on fundamental rights issues,[71] as well as the establishment of a Fundamental Rights Officer at Frontex.[72] There is also a complaints mechanism to address the perceived lack of effective remedy for the actions of Frontex.[73] Finally, Frontex

[62] S Hartwig, 'Frontex: From Coordinating Controls to Combating Crime' (2020) EUCRIM 134.

[63] M Gkliati, 'The Next Phase of The European Border and Coast Guard: Responsibility for Returns and Push-backs in Hungary and Greece' (2022) European Papers www.europeanpapers.eu.

[64] T Quintel, *Data Protection, Migration and Border Control The GDPR, the Law Enforcement Directive and Beyond* (Hart 2022) 24.

[65] *Ibid*. 175.

[66] *Ibid*.

[67] Art. 1(1) Frontex Regulation cit.

[68] Frontex, *Technology Foresight on Biometrics for the Future of Travel* cit. 16.

[69] OLAF, Final Report on Frontex OC/2021/0451/A1 (2021) fragdenstaat.de.

[70] M Gkliati, 'The Next Phase of the European Border and Coast Guard: Responsibility for Returns and Push-backs in Hungary and Greece' cit.; E Tsourdi and P De Bruycker, 'The Evolving EU Asylum and Migration Law' in E Tsourdi and P De Bruycker (eds), *Research Handbook on EU Migration and Asylum Law* (Elgar 2022) 177.

[71] Art. 108 Frontex Regulation cit.; C Loschi and P Slominski, 'Frontex's Consultative Forum and Fundamental Rights Protection: Enhancing Accountability Through Dialogue?' (2022) European Papers www.europeanpapers.eu.

[72] Art. 109 Frontex Regulation cit.; J Rijpma and M Fink, 'The Management of the European Union's External Borders' in E Tsourdi and P De Bruycker (eds), *Research Handbook on EU Migration and Asylum Law* cit.

[73] Recital 104 Frontex Regulation cit.

maintains a "fundamental rights strategy" and a fundamental rights Action Plan.[74] However, instead of tracking how Frontex impacts the fundamental rights of migrants at the external border of the EU,[75] this paper brings to light another aspect of Frontex's activity: its activities concerning biometric technologies and their consequences for fundamental rights.

Frontex's activities relating to biometrics have multiple aspects. Frontex has been meeting with companies which develop biometric technologies, allegedly in secret, as a result of which human rights organisations have been accusing Frontex of promoting "militarisation" and the "border-industrial complex".[76] Frontex has since tried to explain its role concerning biometrics in terms of it being the "driving force in providing support and expertise to both Member States and the European Commission on the topic biometrics".[77] Related to the secretiveness of its activities, scholars have found that Frontex's public access to documents regime is restrictive and sometimes amounts to outright obstruction.[78]

Another activity of Frontex concerning biometrics was the Processing personal data for risk analysis (PeDRa) programme, by which sensitive personal data of migrants was processed, including genetic data, and exchanged between Frontex and Europol. The problem raised by the media and researchers was that Frontex tried to exclude EU data protection watchdogs from giving their input on PeDRa, even side-lining the critique stated by Frontex's own Data Protection Officer.[79] EDPS nevertheless issued a report on PeDRa and Frontex, in which it drew several conclusions: that privacy and data protection, stipulated in arts 7 and 8 CFR, are the cornerstones of a democratic society and that the rights extend to migrants and asylum seekers, not only to EU citizens. EDPS further stated that Frontex has grown exponentially in staff and resources, and so has its role

[74] *Ibid*. art. 80.

[75] S Tas, 'Fundamental Rights Violations in the Hotspots: Who Is Watching over Them?' (2022) European Papers www.europeanpapers.eu.

[76] The border–industrial complex is a name tag to explain the idea by which there is a flourishing industry which produces technologies for border control, and then uses resources and influence to push for greater implementation of the "security" solutions it has produced. In essence, the wider the public perception of security issues, the greater is the profit of the "border-industrial complex". Similar and more established is the well-known "military-industrial complex" in the US, which profits from the wars the US engages in. For the notion of the "border-industrial complex" in the context of Frontex, see M Douo, L Izuzquiza and M Silva Collis, 'Lobbying Fortress Europe: The Making of a Border-Industrial Complex' (5 February 2021) Corporate Europe Observatory corporateeurope.org.

[77] FragDenStaat*, Concept Note by Frontex, International Conference on Biometrics for Borders 2019: Morphing and Morphing Attack Detection Method* fragdenstaat.de.

[78] M Fink and M Hillebrandt, 'Access to Documents and the EU Agency Frontex: Growing Pains or Outright Obstruction?', in M Hillebrandt, P Leino-Sandberg and I Koivisto (eds), *(In)visible European Government: Critical Approaches to Transparency as an Ideal and a Practice* (Routledge 2024) 235.

[79] L Stavinoha, A Fotiadis and G Zandonini, 'EU's Frontex Tripped in Plan for Intrusive Surveillance of Migrants' (7 July 2022) Balkan Insight balkaninsight.com.

which has expanded from a supportive to an operational one. It went on to say that increased scrutiny of Frontex must follow this growth. EDPS commended the decision of Frontex to suspend further development of PeDRa pending previous critical opinions that EDPS published concerning PeDRa.[80]

### III.2. Technology foresight on biometrics for the future of travel

In 2022, Frontex published a study on the future of biometrics in EU border checks (Frontex Study).[81] It identifies key biometric technologies and creates multiple hypotheses on how the security situation will unfold in the decades to come. The Study also analyses where patents and research into biometrics originate. The Study, covering over 600 pages, examines different biometric technologies, and finds several particularly promising biometric technologies for the future. It contains other useful insights, painting a global picture of relevant actors, countries, and technologies related to biometrics. In short, this Study is important for understanding the biometric policy of Frontex. This is not the first study on biometrics published by Frontex. For example, in 2007, Frontex conducted a study which concluded that biometrics, namely iris and fingerprint recognition, were mature enough to be used at European airports for identity checks.[82]

The Frontex Study from 2022 provides useful concepts for understanding various aspects of the application of biometric technologies, biometric systems, and technologies related to biometrics. For example, the Study defines biometric systems, which are combined software and hardware components. One example of such a biometric software and hardware package is an "e-gate" which is a corridor equipped with biometric cameras through which migrants pass for border checks. Another concept is the definition of "biometric enabling" technologies, examples of which include AI and machine learning.[83] These technologies are not exclusively biometric, but they enable the application of modern biometric technologies. Regarding AI, Frontex published an AI-focused report in 2020 which concludes that among the most promising AI technologies is "object recognition", a technology closely related to biometrics, which shows the technological common ground between AI and biometric technologies.[84] More recently, Frontex published a

[80] European Data Protection Supervisor, Hearing at Committee on Civil Liberties, Justice and Home Affairs (LIBE) (8 November 2022) edps.europa.eu.

[81] See above, footnote 2.

[82] Frontex, *BIOPASS: Study on Automated Biometric Border Crossing Systems for Registered Passenger at Four European Airports* (August 2007) frontex.europa.eu.

[83] The EU Agency for the Operational Management of Large-Scale IT Systems in the AFSJ (eu-LISA) has observed that EES "incorporates a component for automated biometric matching, which will rely on machine learning techniques for biometric matching". eu-LISA, Report 'Artificial Intelligence in the Operational Management of Large-scale IT Systems' (July 2020) 5.

[84] Frontex, *Artificial Intelligence-based Capabilities for the European Border and Coast Guard* (European Border and Coast Guard Agency 2021).

report concerning the potential of AI to reshape "the border landscape", with key trends for the border-guard community, including the metaverse, extended reality, and autonomous systems.[85] These lofty visions aside, AI has been important for the recent development of biometric technologies. Machine learning has contributed to facial recognition technologies by enabling the algorithms to process and learn from millions of examples. The AI fields crucial for biometrics include computer vision (which enables computers to process visual information) as well as research into pattern and object recognition (which enables the processing of images of faces or of fingerprint ridges into data).

As a further valuable input for biometrics researchers, a significant part of the Study is devoted to an analysis of where most patents concerning biometrics originate.[86] The short answer is that the US, followed by China, dominates the lists of country of origin of many biometric technologies, with the EU lagging far behind. The main patenting organisations concerning biometric technologies are corporations, such as Microsoft, Apple, or Samsung. This is an indicator that biometric technologies often originate in the private sector and are only later repurposed by public authorities. The EU lacks such technological behemoths, especially in the consumer sector, and, consequently, the EU is a technological laggard in biometrics. Let us take the example of the 3D facial recognition technological cluster, which is one of the five biometric technologies singled out by the Study as having the greatest potential for future use in the EU in border checks. According to the patentometrics and bibliometrics analysis of the Study, the US is the geographic origin of 84 percent of priority patents in this field, followed by China at 8.5 percent and the "European region" is the third at 5.7 percent.[87] The main organisations as the sources of patents in this technological cluster are Microsoft, Amazon, Google, Apple, etc. In the top 15 organisations as sources of patents for 3D facial recognition, besides these multinational companies, we also find the Chinese Academy of Science, but not a single EU company or academic institution. In other words, the technologies that the Frontex Study singles out as the most promising for the future of EU border control are mostly being developed outside the EU by private companies, by US technological behemoths. This has security implications which are not addressed in the Study.

However, the focus of the Frontex Study is on picking the most promising biometric technologies for the future. The main conclusion is that there are five biometric technologies that hold the greatest promise.[88] These are contactless friction ridge recognition (fingerprint or palm ridges recognition without physically touching a surface), two types of facial recognition, one where a 3D image of the face is used and the other where an infrared light is used to scan the face, and two iris recognition biometric technologies,

[85] Frontex, *Technology Horizon Scanning project* (European Border and Coast Guard Agency 2023).

[86] Frontex, *Technology Foresight on Biometrics for the Future of Travel*, Annex III: Patentometric and Bibliometric Analyses of Biometric Technologies (European Border and Coast Guard Agency 2022).

[87] *Ibid*.

[88] *Ibid.* 83.

one using visible spectrum light and the other using infrared light to scan the irises. These technologies were chosen for their practicality, the perceived adoption by the public, costs, security robustness, and other factors. Unfortunately, these technologies were not considered from the perspective of their impact on fundamental rights and data protection rights.

The Frontex Study recognises art. 9(2)(g) GDPR, art. 10 LED, and the fundamental rights framework as relevant for protecting personal and biometric data in the context of the Study.[89] However, the Study lacks legal reasoning on whether certain biometric technologies may infringe fundamental rights and data protection requirements, but merely acknowledges "risks" and defers the question to papers published by FRA.[90] It is interesting that the Frontex Study, in its Note on Fundamental Rights, mentions the possibility of conducting a "fundamental rights impact assessment". This is a hypothetical type of a rights impact assessment which was proposed in a paper published by FRA concerning the regulation of AI and other modern technologies.[91] The GDPR does require a data protection impact assessment if there are high risks for the rights and freedoms of natural persons, particularly when modern technologies are used.[92] But no legal assessment, either a data protection or a fundamental rights impact assessment, is even sketched out in the Frontex Study. It is a mistake not to include any legal reasoning on how biometric technologies analysed in the Study would impact data protection and the fundamental rights of individuals in an otherwise detailed study. The Frontex Study in multiple places mentions that its objective is to be "fully compliant with EU regulations and values", explaining in another place that this means compatibility with fundamental rights, data protection, general legal requirements, and even ethical requirements.[93] Therefore, it is not the case that the Study explicitly excludes legal considerations and focuses on technical or practical aspects alone. However, the problem with this technology-centred approach is that no study of the application of biometric technologies by public authorities makes sense without fully considering fundamental rights and legal requirements. Biometric technologies cannot be considered in a vacuum, but only in relation to how these technologies affect humans.

The attitude that the Frontex Study adopts towards fundamental rights is illustrated in one paradigmatic example. Table 20 on page 81 of the Study shows that, according to the Study, all twenty potential biometric technologies fulfil the legal and ethical requirements to be applied at border checks. Such a conclusion is absurd, especially since no analysis is made on how these biometric technologies potentially interact with fundamental rights. These twenty potential biometric technologies are considered for three

[89] *Ibid*. 16.
[90] *Ibid*.
[91] FRA, 'Getting the Future Right Artificial Intelligence and Fundamental Rights' (2020) 87.
[92] Art. 35 GDPR cit.
[93] Frontex, 'Technology Foresight on Biometrics for the Future of Travel' 26.

other factors besides legal and ethical suitability. Some biometric technologies are considered vulnerable to adversary attacks, some are not appropriate for application in times of pandemics, and some biometric technologies examined in the Study are considered to lack the potential to enable seamless border checks. Only for the category of satisfying legal and ethical requirements is every biometric technology considered compliant. This is unlikely to be true, as it is doubtful that, for example, examining the DNA profile of a person would be considered proportionate to the purpose of checking identity at a border crossing. DNA profiling raises great proportionality challenges. As already demonstrated, different biometric technologies have different levels of impact on the privacy of an individual.[94] Besides, if public authorities want to introduce DNA profiling or any new biometric technology, they must justify why such a modern technology is necessary in addition to or as a replacement for an existing technology, such as fingerprinting. Otherwise, this proportionality requirement, contained in the CFR as well as in the GDPR and LED concerning biometric and personal data processing, will not be satisfied. Proportionality challenges and the necessity for introducing any biometric technology should be a starting point for a discussion on the future of biometrics in the EU, which this report fails to address. Luckily for those averse to having their DNA profiled every time they cross EU external borders, DNA biometrics are (currently) considered merely impractical in the Study. It is false that such extreme biometric technologies would be deemed necessary in a democratic society, proportionate to the purpose of border checks and satisfying other legal requirements, as we have seen from the case law of ECtHR.[95] Worrying in this regard is that FRA experts contributed to the Frontex Study, but without raising these issues.[96] Frontex is obliged to respect fundamental (human) rights and the rule of law in all its activities.[97]

There are other potentially intrusive biometric technologies in the Frontex Study for which it would be important to consider the fundamental rights framework established for biometrics before proceeding to other aspects of their applicability. This would include considering questions such as whether eye-vein recognition is justified interference of private life in view of its legitimate purpose of border checks, or what margin of appreciation public authorities have when applying gait recognition for the purpose of border checks. The Study would then be more beneficial because many of the considered biometric technologies would be eliminated on the grounds of failing the fundamental rights or data protection frameworks. The Study implies but fails to address these crucial security challenges for public authorities in the EU, namely that the EU is dependent on importing biometric technologies which originate from abroad.

[94] *Supra,* section II.2.
[95] *Supra*, section II.2.*b).*
[96] The research was supported by FRA, according to Frontex www.frontex.europa.eu.
[97] Art. 81 Frontex Regulation cit.

When considering in abstract the legal implications of biometric technologies, a definitive assessment of the legality of a certain biometric technology cannot be made. There are other important questions that need to be answered in addition to the nature of biometric technology. These questions include for how long the biometric data are stored and whether they can be deleted, with whom the biometric data are shared and under what circumstances, the procedural safeguards that individuals can rely upon, and how clear the law is that regulates the operation of a biometric technology by public authorities.[98] These factors determine the assessment both before the ECtHR and courts in the EU, including the CJEU in relation to modern technologies, data protection and biometric data in particular.[99] There is additionally a special responsibility of public authorities in the case of the application of a novel technology.[100] The level of interference caused by the taking of fingerprints compared to DNA profiling is not the same. The Frontex Study, however, presumes all biometric technologies are equally compliant with fundamental rights, which is the wrong approach in assessing biometrics.

The Frontex Study is a failed opportunity for Frontex to critically compare technical and legal questions concerning biometrics. With its immense budget, staff, and responsibilities, but lacking appreciation of fundamental rights, Frontex may come to be perceived as a danger for fundamental rights. This must be avoided. To assert a positive role in relation to fundamental (human) rights and to ensure its own survival in a democratic and liberal society, Frontex must start to envisage its role from a fundamental rights perspective instead of a security one. It is easier to prevent abuse and the overreach of a biometric system when it is still a policy for the future than having to dismantle it once it is operational and perhaps uncontrollable.

## IV. Conclusion

Current biometric technologies are fingerprint recognition and, to a lesser extent, facial recognition. Others, such as DNA biometrics, are used in narrower circumstances. But innovation, investment, and the need for data are accelerating. So, what are the biometric technologies for the future? The Frontex Study ultimately does not answer this question because it fails to consider the fundamental rights implications of modern biometric technologies. The biometric technologies that will be used in border control in the EU depend on innovation, security needs, and public acceptance. They also depend on the law, especially on the fundamental rights framework. Legal requirements are shaping the use of biometric technologies and the processing of biometric data, especially in the EU. This is a good thing since it guarantees the individual a certain level of protection against the use of their body to extract information for security or for the other needs of public

[98] Conditions of art. 9(2) GDPR cit. and art. 8 ECHR.
[99] *Supra,* section II.1.
[100] *Marper v UK* cit. para. 112.

authorities. Any study approaching biometric technologies either as a policy or a technological phenomenon should examine the legal requirements for their application, which Frontex in its Study fails to do. The future of biometric technologies in the EU will be determined by the quality of the law that regulates these technologies and the vigilance of courts and individuals in upholding individual rights against unrestricted use of biometrics.