3. Facial recognition AI technology in healthcare and the law

Vera Lúcia Raposo

1. INTRODUCTION

Artificial intelligence (AI), in its various modalities, is increasingly being used in healthcare.[1] One such modality is facial recognition technology (FR) – a group of technologies that uses biometrics to analyse facial features.[2] Facial features are one of the many biometric features used to identify a person. Biometric features encompass both behavioural (one's signature, voice, walking style) and physical features (fingerprints, palmprints, DNA, iris, face features).[3]

Roughly speaking, FR analyses a person's unique facial features, either from a video or a photo, with or without the person's knowledge, in real-time or a posteriori. Subsequently, the analysed information is converted into a template, that is, a mathematical representation of those features.[4] Depending on the specific use for which FR is being employed, the template might be subsequently compared against a previously stored template or a database of preregistered templates.

After this introduction, this chapter is composed of two main sections. First, it analyses the different uses of FR in healthcare, highlighting its benefits and hazards. Second, it explores the main legal concerns raised by FR, with a focus on European law.

1 cf Lalit Garg and others (eds), *Artificial Intelligence in Healthcare* (Springer 2022).

2 In detail see Paramjit Kaur and others, 'Facial-Recognition Algorithms: A Literature Review' (2020) 60(2) Medicine, Science and the Law 131.

3 David Zhang, Guangming Lu and Lei Zhang, *Advanced Biometrics* (Springer 2018).

4 Claude Castelluccia and Daniel Le Métayer Inria, 'Impact Analysis of Facial Recognition: Towards a Rigorous Methodology' (2020) 6–7 <https:// hal .inria .fr/ hal -02480647/ document> accessed 28 April 2024. For technical details, see Catalin-Mircea Dumitrescu and Ioan Dumitrache, 'Combining Deep Learning Technologies with Multi-Level Gabor Features for Facial Recognition in Biometric Automated Systems' (2019) 28(2) Studies in Informatics and Control 221.

2. USES OF FR IN HEALTHCARE

FR is being used by many different actors and industries, with each setting raising its own challenges.[5] This section will focus exclusively on its uses in the healthcare setting, although some of these uses go beyond healthcare delivery.[6]

2.1 FR for Classification and Categorisation

In classification and categorisation, the individual is assigned to a specific category of people based on his or her facial features – for instance, to a specific gender or ethnic group.[7] This use is not common in healthcare. There are situations in which screening people for sex or ethnic origin could have some use, such as in clinical trials or another type of experimental study. However, the effective benefit of this kind of screening would only be visible in studies involving large numbers of people. In smaller studies, categorisation either is not required or can be efficiently carried out by humans.

More controversial forms of classification and categorisation involve the inference of sexual orientation or political affiliation, among other non-behavioural characteristics, from a biometric template.[8] However, the usefulness of this information for healthcare delivery, or generally for any purpose in a healthcare environment, is yet to be demonstrated.

---

[5] On the different uses of FRT, see Joy Buolamwini and others, 'Facial Recognition Technologies: A Primer' (Algorithmic Justice League 2020) 2–8 <https:// people .cs .umass .edu/ ~elm/ papers/ FRTprimer .pdf> accessed 28 April 2024; Desara Dushi, 'The Use of Facial Recognition Technology in EU Law Enforcement: Fundamental Rights Implications' (Global Campus of Human Rights 2020) 3; Ella Jakubowska, 'Facial Recognition and Fundamental Rights 101' (*EDRi*, 4 December 2019) <https://edri.org/facial-recognition-and-fundamental-rights-101/ > accessed 28 April 2024; European Union Agency for Fundamental Rights, 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (2019) 7–8 <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights -considerations -context -law> accessed 28 April 2024; Jenny Brennan, 'Facial Recognition: Defining Terms to Clarify Challenges' (*Ada Lovelace Institute*, 13 November 2019) <https://www .adalovelaceinstitute.org/blog/facial-recognition-defining-terms-to-clarify-challenges/> accessed 28 April 2024. On the risks of FRT, see Brenda Leong, 'Facial Recognition and the Future of Privacy: I Always Feel Like … Somebody's Watching Me' (2019) 75(3) Bulletin of the Atomic Scientists 109, 111–12.

[6] See Christopher Libby and Jesse Ehrenfeld, 'Facial Recognition Technology in 2021: Masks, Bias, and the Future of Healthcare' (2021) 45 Journal of Medical Systems 1.

[7] See Opinion 3/2012 of the Article 29 Data Protection Working Party on Developments in Biometric Technologies [2012] WP193 <https://www.pdpjournals.com/docs/87998.pdf> accessed 29 April 2024 (Opinion 3/2012).

[8] Michal Kosinski, 'Facial Recognition Technology Can Expose Political Orientation From Naturalistic Facial Images' (2021) 11 Scientific Reports 1; Yilun Wang and Michal Kosinski, 'Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation from Facial Images' (2018) 114(2) Journal of Personality and Social Psychology 246.

2.2 Facial Characterisation

Facial characterisation refers to using FR to impute a person's reactions and feelings by analysing the face and its micro-expressions.[9] A person's face is a rich source of information about the emotions a person is experiencing and, therefore, analysing the face is crucial to identify those emotions.[10]

In healthcare, FR may be deployed to track how patients react to physical pain, an extremely useful feature for patients who cannot communicate verbally (such as individuals with intellectual disabilities or newborns).[11] Mere behavioural observation might not be enough for that realm, nor does it allow continuous monitoring. FR, on the other hand, achieves those purposes and also allows the measurement of pain intensity.[12] Emotional pain – which frequently leads to depression and even suicide – may also be tracked by FR.[13] By detecting emotions, FR can potentially assess whether the patients took their medication, and allow patients' monitoring in outpatient routine with a simple smartphone, as failure to take certain medications can change the patient's state of mind and thus his or her emotions.[14]

The use of this technology is not restricted to patients. FR may also be used to analyse the emotional state of physicians and other healthcare workers. Deploying FR for this purpose may be particularly useful for coping with increasing healthcare worker burnout in the wake of the COVID-19 pandemic.[15]

In other situations, emotion recognition is not applied to patients or doctors but operates as a medical tool to help patients communicate. Patients with an autism spectrum disorder are a good example. At times, such patients face difficulty in recognising facial emotions, but

---

[9] cf Lisa Feldman Barrett and others, 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements' (2020) 20(1) Psychological Science in the Public Interest 1.

[10] Safaa El Morabit and others, 'Automatic Pain Estimation from Facial Expressions: A Comparative Analysis Using Off-the-Shelf CNN Architectures' (2021) 10(16) Electronics 1.

[11] Kristina Grifantini, 'Detecting Faces, Saving Lives – How Facial Recognition Software Is Changing Healthcare' (2020) 11 IEEE Pulse 2; Ehsan Othman and others, 'Automatic vs. Human Recognition of Pain Intensity from Facial Expression on the X-ITE Pain Database' (2021) 21(9) Sensors 1.

[12] Philipp Werner and others, 'Automatic Recognition Methods Supporting Pain Assessment: A Survey' (2019) 13 IEEE Transactions on Affective Computing 530.

[13] Subarna Shakya, Suman Sharma and Abinash Basnet, 'Human Behavior Prediction Using Facial Expression Analysis' (2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, April 2016) 399.

[14] Nicole Martinez-Martin, 'What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?' (2019) 21(2) AMA Journal of Ethics 180, 181; Young-Shin Lee and Won-Hyung Park, 'Diagnosis of Depressive Disorder Model on Facial Expression Based on Fast R-CNN' (2022) 12(2) Diagnostics 1.

[15] See the details in the Medscape National Physician Burnout, 'Depression & Suicide Report 2021' (*Medscape*, 2021) <https://www.medscape.com/slideshow/2021-lifestyle-burnout-6013456> accessed 24 March 2022.

algorithms trained in FR can provide photos of correctly labelled different human emotions, to assist them in recognising those emotions.[16]

2.3 FR for Diagnosing and Predicting Medical Conditions

FR may also potentially be used in healthcare to identify rare genetic conditions, based on the analysis of facial traits. Such traits can be extremely difficult to detect, as some of them are so subtle that the human eye cannot recognise them.[17] FR systems can perform the task with greater accuracy, by analysing patients' facial features and comparing the result against a database of biometric templates from patients suffering from different diseases.[18] The technology is being used to diagnose autism spectrum disorders, Cushing's syndrome and Cornelia de Lange syndrome, among others.[19]

FR may also be used as a telemedicine tool, to identify more common medical conditions. The so-called health mirror is an FR mechanism that operates through medical apps to measure heart rate, blood pressure and stress levels by analysing facial features. It is convenient, non-invasive and even contact-free, and thus might become popular for adoption.[20]

The analysis of facial features also allows for the tracking of signs of ageing as well as risk factors associated with several diseases, such as smoking (wrinkles around the mouth), alcoholism (larger nose) and diseases resulting from excessive exposure to the sun (brown spots

---

[16] Rosa Angela Fabio and others, 'Correlations Between Facial Emotion Recognition and Cognitive Flexibility in Autism Spectrum Disorder' (2020) 6(3) Advances in Autism 195, 195; Haik Kalantarian and others, 'Labeling Images with Facial Emotion and the Potential for Pediatric Healthcare' (2019) 98 Artificial Intelligence in Medicine 77.

[17] Dian Hong and others, 'Genetic Syndromes Screening by Facial Recognition Technology: VGG-16 Screening Model Construction and Evaluation' (2021) 16 Orphanet Journal of Rare Diseases 1; even when the analysis can be accurately performed by human operators, it is difficult to fund trained staff for such tasks. See Seema Mohapatra, 'Use of Facial Recognition Technology for Medical Purposes: Balancing Privacy with Innovation' (2016) 43(4) Pepperdine Law Review 1017, 1022.

[18] See, in particular, the app Face2Gene (Yaron Gurovich and others, 'Identifying Facial Phenotypes of Genetic Disorders Using Deep Learning' (2019) 25 Nature Medicine 60); see also Martinez-Martin (n 14). A 2014 study, carried out by researchers from Oxford University, concluded that '[a]lterations in the face and skull are present in 30–40% of genetic disorders' and thus they can be tracked with FR (Quentin Ferry and others, 'Diagnostically Relevant Facial Gestalt Information from Ordinary Photos' (2014) 3 Elife 1, 2).

[19] See Fabio and others (n 16); Kalantarian and others (n 16); RP Kosilek and others, 'Automatic Face Classification of Cushing's Syndrome in Women – A Novel Screening Approach' (2013) 121(9) Experimental and Clinical Endocrinol Diabetes 561; L Basel-Vanagaite and others, 'Recognition of the Cornelia de Lange Syndrome Phenotype with Facial Dysmorphology Novel Analysis' (2016) 89(5) Clinical Genetics 557. It has been stated that the use of AI solutions for genetic diagnosis could undermine the right to genetic privacy and the right not to know genetic information (Mohapatra (n 17) 1031–35). However, this is not a problem specific to AI, but applies to any kind of medical testing.

[20] Anastasiya Zharovskikh, 'Facial Recognition for Healthcare Disruption. Key Use Cases' (*InData Labs*, 2 July 2020) <https:// indatalabs .com/ blog/ ai -face -recognition -in -healthcare> accessed 28 April 2024.

and wrinkling).[21] Predicting risk factors using FR allows patients to take adequate measures to improve their health status and reduce such risks.[22]

2.4 Identification of a Person

The best-known use of FR relates to identification. As facial features are tendentially immutable, they become a distinctive identification feature.[23] Identification can operate in the form of authentication or verification (confirming that the person is who he or she claims to be) or in the form of identification or recognition (confirming that the person is whom we believe him or her to be).[24] In both cases the technology 'measures' the person's facial features and creates a template. For authentication, the template will be compared with another previously captured biometric template from that same person. By contrast, in recognition, the template will be compared with various templates from several individuals stored in the database.[25]

In hospital settings, this speedy and efficient method has obvious advantages for admission.[26] FR can expedite the check-in process. The patient can be identified as soon as he or she enters the hospital and can be immediately redirected to the service where the medical appointment will take place, using an SMS or an in-app message to provide orientation and

---

[21] Mohapatra (n 17) 1023–24.

[22] Some studies have argued the peril of employers having access to this information and, based on that, adopting discriminatory measures against workers (Mohapatra (n 17) 1030–31). Although this is a real peril, the issue is not connected to FR (or to AI in general), but with the access of employers to the employees' private medical and genetic information.

[23] However, the identification of a face might be hampered by some 'incidents', such as ageing (H Yassin, S Hoque and F Deravi, 'Impact of Age and Ageing on Face Recognition Performance' (2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Melbourne, December 2019) 1), medical conditions that affect face expression (LC Bulnes and others, 'The Effects of Botulinum Toxin on the Detection of Gradual Changes in Facial Emotion' (2019) 9 Scientific Reports 1), cosmetic surgery (Christian Rathgeb and others, 'Plastic Surgery: An Obstacle for Deep Face Recognition?' (2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Seattle, June 2020)) or even the mere fact that a face mask is being used (Jesús Tomás and others, 'Incorrect Facemask-Wearing Detection Using Convolutional Neural Networks with Transfer Learning' (2021) 9(8) Healthcare 1050), as was frequently the case during the peak of the pandemic.

[24] A major advantage of FR for authentication purposes is the fact that the identifying feature – the face – cannot be easily stolen (John Petersen, 'The Complexity of Consent and Privacy In Biometrics – Worldwide' (2019) 2019(8) Biometric Technology Today 5), unlike what happens with passwords, commonly used for this same purpose; cf Vera Lúcia Raposo, '(Do Not) Remember my Face: Uses of Facial Recognition Technology in Light of the General Data Protection Regulation' (2022) Information & Communications Technology Law 1.

[25] cf Stephen Caines, 'The Many Faces of Facial Recognition' in Roland Vogl (ed), *Research Handbook on Big Data Law* (Edward Elgar Publishing 2001) 29; Commission Nationale de l'Informatique et des Libertés (CNIL), Reconnaissance Faciale – Pour Un Debat À La Hauteur Des Enjeux, (2019) 3 <https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf> accessed 28 April 2024.

[26] See, however, the considerations about mistaken identifications in section 3.

directions without much bureaucracy, thus decreasing the workload.[27] FR can be especially useful in facilitating admission processes of unconscious patients or patients facing difficulties in communicating (such as children, elderly patients or patients with mental incapacities).[28] FR can also prevent identity theft. Quick and accurate identification can eliminate instances where surgery is performed on the wrong patient or where medication is provided to the wrong patient.[29] Traditional patient identification operates by verifying the name, date of birth or hospital patient number, but many mistakes still occur, especially in urgent cases. With FR, however, a mere face scan is enough.

This technology is also used for tracking a patient's medical record (most likely, an electronic health record) solely using the information provided by the FR system, without the patient being required to show any identification document. Important information – such as allergies, blood type and the existence of advance directives – could be easily tracked by immediately linking the patient's face to his or her electronic health record.[30]

Additionally, FR as authentication can address circumstances where the patient's identification is relevant to providing them with access to their health information, such as the sharing of results from medical examinations or tests or the patient accessing their medical records, even remotely, using an app or secure portal.[31]

Another possible use of FR relates to getting access to restricted physical spaces for patients, relatives and healthcare workers.[32] If the FR system does not provide a green light to the authentication – for example, automatically opening a door – the person will not be allowed to get in. Likewise, identification to control who goes in and out can prevent patients with diminished capacity, such as children, from leaving a facility. It can also be used to avoid abduction, as has sometimes occurred with newborns.

---

[27] Kanubhai K Patel, Jignesh J Patoliya and Miral M Desai, 'IoT Based Smart Health Monitoring System with Patient Identification Using Face Recognition' Proceedings of the International Conference on Innovative Computing & Communication (ICICC, 2021) 1.

[28] Byoungjun Jeon and others, 'A Facial Recognition Mobile App for Patient Safety and Biometric Identification: Design, Development, and Validation' (2019) 7(4) JMIR mHealth and uHealth 1.

[29] ibid.

[30] Barak Bassman and others, 'Facing Up to Tough Issues: Health Care Compliance Concerns with Facial Recognition Technology' (*JDSUPRA*, 12 May 2021) <https:// www .jdsupra .com/ legalnews/ facing -up -to -tough -issues -health -care -9118586/ ?utm _content = bufferb82a3 & utm _medium=social&utm_source=twitter.com&utm_campaign=buffer> accessed 29 April 2024.

[31] S Jayanthy and others, 'Facial Recognition and Verification System for Accessing Patient Health Records' (2019 International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, May 2019) 1266.

[32] Daniel Florez Mendez and others, 'Facial Recognition System for Security Access Control' (2021) 11842 Proc. SPIE Applications of Digital Image Processing XLIV 1184217.

3. FAILURES, BIASES AND RIGHTS

While FR can improve accuracy, it is not immune from error. Indeed, the results provided by this technology are merely probabilistic.[33] Any AI system never gives a 'yes' or 'no' answer but merely provides percentages of the likelihood of some hypothesis. For instance, within an FR system that confirms the identity of a patient based on the analysis of his or her facial features, the system will only indicate how likely it is (in terms of percentage) that the person is who he or she claims to be. Thus, a key factor is the level of probability achieved. Even though accuracy has increased with technological developments, there is still much room for improvement.[34]

Errors can be related to the environment where the image (on which the biometric template is based) was collected. In a controlled environment, with the correct light, and the most appropriate face position, the accuracy of the measurements are higher and, therefore, the likelihood of a successful identification increases.[35] In contrast, in non-controlled environments, as usually happens in one-to-many identification (such as cameras placed in public spaces), images are less clear, and the resulting biometric template becomes less trustworthy.[36] The quality of the images used is, thus, crucial.[37]

Another source of error relates to the insufficiency or inaccuracy of training data. If the data provided to 'teach' the algorithm are not diverse and accurate, FR may lead to mistaken outcomes for some populations. The risk of misidentification is higher for patients belonging to a minority group or for women; the risk of these individuals being misidentified increases by 10–100 times when compared with misidentifications of patients who do not belong to any minority.[38] The same concern applies to disease recognition: when detecting genetic conditions, many FR systems do not perform well on non-Caucasians.[39] Likewise, FR is not

---

[33] Frank Pasquale, 'When Machine Learning Is Facially Invalid' (2018) 61(9) Communications of the ACM 25, 26–27.

[34] Wenying Wu and others, 'Gender Classification and Bias Mitigation in Facial Images' (Proceedings of 12th ACM Conference on Web Science, Southampton, July 2020).

[35] Manminder Singh and AS Arora, 'Varying Illumination and Pose Conditions in Face Recognition' (2016) 85 Procedia Computer Science 691; Mathias Becuywe and others, 'Landscape of Start-Ups Developing Facial Recognition: Analysis and Legal Considerations' (2022) 27–30 <https://ai-regulation.com/frlandscape/> accessed 28 April 2024; Tambiama Madiega and Hendrik Mildebrath, 'Regulating Facial Recognition in the EU' (European Parliamentary Research Service 2021) 6.

[36] Davide Castelvecchi, 'Beating Biometric Bias' (2020) 587 Nature 347; European Union Agency for Fundamental Rights (n 5) 8 and 27; Patrick Grother, George Quinn and Mei Ngan, 'Face in Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects' (NIST Interagency/Internal Report 2017) <https://doi.org/10.6028/NIST.IR.8173> accessed 29 April 2024.

[37] 'Guidelines on Facial Recognition' (Council of Europe 2021) 12–13 <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3> accessed 29 April 2024.

[38] Patrick Grother, Mei Ngan and Kayee Hanaoka, 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects' (NIST Interagency/Internal Report 2019) <https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf> accessed 29 April 2024.

[39] Elie Dolgin, 'AI Face-Scanning App Spots Signs of Rare Genetic Disorders' (2019) Nature 1; Jacqueline G Cavazos and others, 'Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?' (2021) 3(1) IEEE Transactions on Biometrics, Behavior,

immune to gender issues, and, in general, it performs better when analysing male rather than female biometrics.[40]

These inaccuracies have led to the qualification of this technology as being biased.[41] As noted above, the problem lies in the dataset used to train the FR algorithm. Thus, when using modern software, trained with a wide panoply of different images, FR accuracy rises to 99 per cent.[42]

An important tool against failures and biases is constant monitoring using, for instance, audits and due diligence. Governing authorities or independent auditors should regularly confirm that the databases used to train and test the algorithms and the design of those algorithms do not lead to biased results. However, the problem is that the technology's novelty and lack of transparency might hamper such procedures. With them being so complex and nebulous (the famous black box label), one wonders if these monitoring procedures can generate any effective result. Moreover, the novelty of the technology gives rise to business secrecy which may discourage developers and manufactures from disclosing relevant information.[43] Indeed, fearing disclosure of trade secrets to their competitors, some AI developers have refused to provide the authorities in charge with the information required to examine the performance of the AI system.[44]

4. LEGAL COMPLIANCE TO REDUCE LEGAL RISKS

In theory, compliance with the requirements of various legal regimes can help protect patient rights. When it comes to the EU, however, FR is governed under a complex array of different legal regimes, which may hamper rather than help development.

---

and Identity Science 101; current FR systems have managed to solve this failure. See Paul Kruszka and others, '22q11.2 Deletion Syndrome in Diverse Populations' (2017) 173(4) AJMG 879; US Government Accountability Office, 'Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses' (*GAO*, 13 July 2020) <https://www.gao.gov/products/gao-20-522> accessed 29 April 2024.

[40] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 1.

[41] Frederik Zuiderveen Borgesius, 'Discrimination, Artificial Intelligence, and Algorithmic Decision-Making' (Council of Europe 2018) <https:// rm .coe .int/ discrimination -artificial -intelligence-and-algorithmic-decision-making/1680925d73> accessed 29 April 2024.

[42] Michael McLaughlin and Daniel Castro, 'The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist' (*ITIF*, 27 January 2020) <https:// itif .org/ publications/ 2020/ 01/ 27/ critics -were -wrong -nist -data -shows -best -facial -recognition-algorithms> accessed 29 April 2024.

[43] Yavar Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2018) 31(2) Harvard Journal of Law & Technology 890.

[44] This is not a mere hypothetical situation. In a British case related to the use of FR for law enforcement purposes, an audit on the FR system was required to establish potential biases, but the provider of the AI refused to disclose information invoking 'business secrecy', and the court upheld this argument (*R (on the application of Edward Bridges) v The Chief Constable of South Wales Police & others* [2020] EWCA Civ 1058 [199]).

4.1 Compliance with Data Protection Norms

FR operates with biometric data, which is considered personal and sensitive data under the General Data Protection Regulation (GDPR).[45] The sensitive nature of biometric data has been acknowledged by both the European Court of Justice and the European Court of Human Rights.[46] As FR is a form of data processing, it must comply with GDPR's numerous and rather demanding requirements aimed at providing special protection to these data.[47]

4.1.1 Legal ground for data processing

Any data processing requires proper legal grounds. Given the sensitive data involved, two legal grounds are required: one for general personal data (Article 6 GDPR) and the other for sensitive data (Article 9 GDPR).

The instinct of many data controllers is to obtain the data subject's consent under the GDPR, assuming it to be the easiest way to proceed.[48] Unfortunately, in light of Articles 6(1)(a) and 9(2)(a) GDPR, consent is a difficult standard to comply with regard to FR for several reasons.[49]

First, the information provided to the data subject must be clear and concise; appropriate to the target individual and his or her level of comprehension. In the particular case of FR, the information shall include the location of the cameras, the identification of the people or entities that will have access to the data, the duration and form of data retention and the procedures to

---

[45] 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 119/1; see the definition of biometric data in Article 4(14) of the GDPR, and the limitations to its processing in Article 9 of the GDPR; there are associated privacy concerns related to this technology, namely regarding mass surveillance. However, when FR is not operated by police forces or other governmental authorities, and moreover is limited to a circumscribed setting, as in healthcare, this hazard is unlikely to materialise.

[46] For the European Court of Justice case law, see Case C-291/12 *Michael Schwarz v Stadt Bochum* [2013] ECLI:EU:C:2013:670 and Joined Cases C-446/12 to C-449/12 *W. P. Willems and Others v Burgemeester van Nuth and Others* [2015] ECLI:EU:C:2015:238; for the European Court of Human Rights case law, see *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016).

[47] The GDPR does not apply to anonymised data and thus data controllers use, whenever possible, anonymised data to have greater leeway. However, it seems that biometric data are so intrinsically personal that not even anonymisation eliminates all identifying elements: 'there is a growing scepticism in the field of data protection and privacy law that biometric data can never truly be deidentified or anonymized' (Justin Banda, 'Inherently Identifiable: Is It Possible to Anonymize Health and Genetic Data?' (*IAPP*, 13 November 2019) <https://iapp.org/news/a/inherently-identifiable-is-it-possible-to-anonymize-health-and-genetic-data/> accessed 29 April 2024.)

[48] Data controller means the natural or legal person that determines which data will be processed.

[49] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (May 2020) 7–32 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 29 April 2024 (Guidelines 05/2020); see also Raposo, '(Do Not) Remember my Face' (n 24) 9ff.

exercise the rights granted by the GDPR.[50] Consent must be explicit, meaning an affirmative action is required, and it cannot be induced from conduct (Recital 32 GDPR). Therefore, the mere fact that a person enters the hospital facility being fully aware (according to the strict rules on information provision set forth in the GDPR) that FR cameras are operating in that facility cannot be taken as consent to use and process the biometric data collected. Due to these restrictions, obtaining consent from everyone entering busy places, such as large hospitals, might be factually impossible.

The second set of difficulties relates to the proof of consent. Responsibility for demonstrating that consent has been provided rests with controllers (Article 7(1) GDPR). Unless a written statement is provided, establishing proof of mere oral consent will be difficult. When FR is used to diagnose patients or to analyse emotions, consent can be collected within the medical relationship. Consent from healthcare staff might be collected through the employment contract. In contrast, it is extremely difficult to obtain written consent from everyone going in and out of the healthcare facility (especially individuals visiting patients).[51]

Overall, major problems arise when FR is applied to multiple unknown individuals, such as when FR is used to control people going in and out of the healthcare facility (that is, for identification purposes). This is one of the most problematic scenarios, as consent must be taken from a multiplicity of people, whose identity is not always previously determined, making it extremely difficult, if not impossible, to comply with the GDPR requirements.

Even beyond the logistics of obtaining consent, there is the issue of voluntariness. Consent is only considered 'free' when the data subject had the option to not provide it without suffering negative consequences. Data authorities might consider that healthcare staff were not entirely free to give consent due to the dynamic of power and subordination between the employer (the healthcare facility) and the employees.[52] Likewise, some authorities might determine that the patient's consent was not free either, as the patient might fear being deprived of medical care if consent was not provided. As stated by the Information Commissioner's Office (ICO), the United Kingdom's data protection authority, 'If you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.'[53]

Assuming that consent cannot be collected from everyone, FR cameras must be placed in such a way that they only capture those who consented. An alternative route to enter and leave the premises without surveillance must be arranged. However, if that is the case, then the main goal of FR – to control entries and exits – is jeopardised, rendering the technology useless.

---

[50] European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data Through Video Devices' (January 2020) 5–23 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf> accessed 29 April 2024 (Guidelines 3/2019); even though these guidelines were issued to address regular video devices (that is, without FR), their considerations can be transposed to FR.

[51] Opinion 3/2012 (n 7) 5.

[52] Several data protection authorities have denied the validity of consent in such scenarios. See Raposo, '(Do Not) Remember my Face' (n 24) 13; Guidelines 3/2019 (n 50) 14.

[53] Information Commissioner's Office, 'Consent', *(ico*., n.d.) <https:// ico .org .uk/ for -organisations/ guide -to -data -protection/ guide -to -the -general -data -protection -regulation -gdpr/ lawful-basis-for-processing/consent/> accessed 29 April 2024.

In light of the previous considerations, it is possible to conclude that several legal and practical challenges arise regarding attempts to meet the requirements of consent, as provided for in Articles 6(1)(a) and 9(2)(a) of the GDPR. Thus, other possible legal grounds shall be explored.

When FR is used to provide medical care, it is easier to find a supporting legal ground. Usually, the patient can consent and, if not (unconscious patients, for instance), the processing of data for health/medical purposes can invoke several legal grounds: GDPR Articles 6(1)(b) (performance of a contract), (1)(d) and 9(2)(c) (protection of vital interests of the data subject), and 9(2)(h) (preventive or occupational medicine).

In some scenarios the legitimate interest ground, as set out in Article 6(1)(f), may also be used, such as when the aim is to prevent patients from leaving the facility (especially in mental hospitals) or prevent the kidnapping of newborns.[54] However, there is no similar ground in Article 9, which prevents the use of this legal ground. Moreover, national data protection authorities have been quite restrictive in the interpretation of this clause.[55]

4.1.2 Data subject rights provided for in the GDPR

In Chapter III, the GDPR lays down several rights for data subjects, some of them resulting from the core principles listed in Article 5.

Information rights are repeatedly invoked in this chapter. The purpose for which biometric data is being collected must be communicated accurately to the data subjects, so the latter can clearly understand that purpose.[56] Whenever FR is employed, the data subjects must be informed. According to the European Data Protection Board (EDPB), information must be provided in two layers.[57] The first layer involves the first encounter between the data subject and FR, encompassing the most important information. The EDPB recommends using a warning sign in an easily visible place, with an icon (Article 12(7) GDPR), but admits that the information format can be adjusted to the specific location. The second layer of information, which must be referred to by the first layer, must be made available in a place where data subjects can easily access it (such as through a QR code, an internet link or an information desk).

An additional set of rights relates to the purpose for which the data are collected. The biometric data collected cannot subsequently be used for different purposes due to the limitations imposed by Article 5(1)(b) of the GDPR, which aims to prevent the risk of function creep.[58] When those subsequent purposes are related to research, the research exception described in

---

[54] Opinion 06/2014 of the Article 29 Data Protection Working Party on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC' [2014] WP 217; Gabriela Zanfir-Fortuna and Teresa Troester-Falk, 'Processing Personal Data on the Basis of Legitimate Interests under the GDPR: Practical Cases' (Future of Privacy Forum and NYMITY 2018) <https://fpf.org/wp-content/uploads/2018/04/20180413-Legitimate-Interest_FPF_Nymity-2018.pdf> accessed 29 April 2024.

[55] cf Raposo, '(Do Not) Remember my Face' (n 24) 9–12.

[56] Case C-275/06, *Promusicae v Telefónica de España SAU* [2007] ECLI:EU:C:2007:454, Opinion of AG Kokott, para. 53.

[57] Guidelines 3/2019 (n 50) 26–27; these guidelines were issued regarding video surveillance without FR, but the same shall apply, *ad maiori ad minus*, to FR.

[58] Lotte Houwing, 'Stop the Creep of Biometric Surveillance Technology' (2020) 6(2) European Data Protection Law Review 174.

Article 89 GDPR might apply.[59] However, the exception depends on several requirements that are difficult to meet in practice.[60] To begin with, the research exemption can only operate when there are 'appropriate safeguards […] for the rights and freedoms of the data subject' – clearly a very vague standard. Article 89(1) of the GDPR presents another challenging requirement, stating that, whenever possible, data shall be pseudonymised, or even anonymised. The problem is that facial biometric data are extremely difficult to anonymise, as they refer to intrinsic properties of a person.[61] Its individual nature is confirmed by the definition of biometric data provided in Article 4(14) of the GDPR, as data 'relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person'. Moreover, while biometric data reidentification has been possible for a long time, AI becomes a useful resource for re-identifying data subjects based on their alleged anonymised biometric data.

Additionally, data subjects are protected against automatic decision-making based solely on data processing (Article 22 GDPR). Due to this prohibition, it is not possible to have a health professional removed from his or her duties because of fear of burnout or suicide based exclusively on FR detecting emotions. The norm allows some exceptions (Article 22(2) GDPR). However, because FR involves sensitive data, the only scenarios under which such exceptions could operate are when the data subject has explicitly authorised it or when there is substantial public interest (Article 22(4) GDPR). The concept of 'substantial public interest' is not defined in the GDPR, and the specialised literature does not provide examples. One would surmise, however, that it could refer to issues related to public health or public security (for example, using profiling to exclude a doctor considered a menace to public health).

4.2 Compliance with the Medical Device Regulation

The definition of medical device outlined in Article 2(1) of the Medical Device Regulation (MDR)[62] includes any 'instrument, apparatus, appliance, software, implant, reagent, material or other article' intended for the aims described therein, which are rather broad. Even though the MDR does not expressly state that its regimes also cover AI medical devices, it is commonly understood that it does.[63] Thus, FR systems used to provide healthcare (for instance,

---

[59] Suppose that biometric data collected to provide healthcare is subsequently used in medical investigation.

[60] Alex van der Wolk and Morrison & Foerster, 'The (Im)Possibilities of Scientific Research Under the GDPR' (Cybersecurity Law Report 2020) 3–4 <https://media2.mofo.com/documents/200722-scientific-research-gdpr.pdf> accessed 29 April 2024.

[61] Banda (n 47).

[62] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, Amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and Repealing Council Directives 90/385/EEC and 93/42/EEC (Medical Device Regulation).

[63] In fact, only point 2.1 of Annex VIII of the Medical Device Regulation mentions the concept of 'artificial intelligence'.

to identify diseases or levels of pain)[64] can be considered medical devices and, as such, are submitted to the MDR.[65]

Under the MDR, a conformity assessment (Articles 2(40) and 52 MDR) is required before the device is marketed. The requirements – known as the General Safety and Performance Requirements (GSPRs) – imposed by this Regulation must be fulfilled, as only a positive assessment allows the grant of the CE marking of conformity (Article 20 MDR).[66]

Article 51 of the MDR recognises different classes of medical devices according to the respective level of risk: I, IIa, IIb and III.[67] This categorisation leads, in turn, to different types of conformity assessments, with level III being the most demanding.

Given the complex classification set forth in the MDR, FR may fall under different classifications depending on its specific use. According to Rule 11 of the MDR (Article 6.3 MDR), 'software intended to provide information which is used to make decisions with diagnosis or therapeutic purposes' will be treated, as a rule, as a class IIa device. However, when the medical decisions taken based on that software can lead to 'serious deterioration of a person's state of health or a surgical intervention', class IIb applies; and when those medical decisions can lead to 'death or an irreversible deterioration of a person's state of health', class III will apply. Rule 11 also makes a reference to software intended to 'monitor physiological processes', which should be classified as class IIa. For instance, FR employed to monitor the presence and intensity of pain will fall into class IIa unless some forms of pain are considered 'vital physiological parameters, where the nature of variations of those parameters is such that it could result in immediate danger to the patient', in which case class IIb will apply. If none of these conditions apply, the software will be classified as class I.

It is up to the manufacturer to classify the respective medical devices. For class I devices that are not sterilised, do not have a measuring function and are not reusable surgical instruments, it is also up to the manufacturer to carry out the conformity assessment and self-award the CE marking. Notified bodies may intervene, but they are not mandatory. However, for class IIa devices and higher, the assessment and the granting of the CE marking are carried out by the notified bodies.

In sum, different types of conformity assessments are established for the different classes of medical devices, forming an intricate net of requirements and assessments.[68] The potential

---

[64] Excluded is FR not targeted to medical purposes, as is the case with the one aimed at identifying natural persons.

[65] See R Beckers, Z Kwade and F Zanca, 'The EU Medical Device Regulation: Implications for Artificial Intelligence-Based Medical Device Software in Medical Physics' (2021) 83 Physica Medica 1.

[66] European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR), 'Artificial Intelligence in EU Medical Device Legislation' (2020) 10–11 <https://www.cocir.org/fileadmin/Position_Papers_2020/COCIR_Analysis_on_AI_in_medical_Device_Legislation_-_Sept._2020_-_Final_2.pdf> accessed 29 April 2024.

[67] IMDRF SaMD Working Group, 'Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations' (International Medical Device Regulators Forum 2014) <https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf> accessed 29 April 2024.

[68] For detail about the assessment and the intervention of notified bodies, see V Lücker, 'Stoffliche Medizinprodukte' (2016) 78(10) Pharmazeutische Industrie 1464; David Egbosimba,

intervention of the notified bodies in the conformity assessment adds another layer of complexity atop this already intricate procedure.

4.3 Compliance with the AI Act

In April 2021, the European Commission released its proposal for a regulation on artificial intelligence,[69] aimed at providing far-reaching AI regulation. The most recent version (as of this writing) was published on 24 March 2024 and is expected to reflect the final version (hereafter, the 'AI Act').[70]

Like the MDR, the AI Act operates with different levels of risk (the so-called risk-based approach): (i) unacceptable risk AI, which are banned in Title II of the Proposal; (ii) high-risk AI, referred to in Title III of the Proposal, which are allowed, albeit under particularly strict standards; (iii) low-risk AI, for which only transparency requisites are demanded in some cases (namely chatbots and deep fakes).

In the AI Act some forms of FR are banned.[71] However, the kind of uses envisaged for FR in the healthcare settings are allowed, although it is considered a high-risk technology. The classification as high-risk can be justified in two ways: remote biometric identification systems is a type of AI technology listed in Annex III, point 1(a), and thus considered high-risk AI by Article 6(2) of the AI Act;[72] while FR used for medical purposes will be considered a medical device, which is considered a type of high-risk AI system[73] (Article 6(1) and Section A, Annex I points 11 and 12 of the AI Act).

High-risk AI systems must comply with several requirements, *ex ante* and *ex post*. High-risk AI systems, such as FR, can only be put on the market if they 'do not pose unacceptable risks to important Union public interests as recognised and protected by Union law' (Recital 46 AI Act).

Ex ante control is a precondition for the granting of the CE marking of conformity, without which this type of AI cannot be commercialised. Before launching the AI system on the market, the developers of high-risk AI systems are required to implement models of risk assessment and risk mitigation; use high-quality datasets to train the system (which, in turn, require a huge amount of data – and if those are personal data, the GDPR might impose some obstacles); maintain regular activity logs to allow traceability; provide users with sufficient information; assure human oversight; guarantee the robustness, security and accuracy of the

---

'L'industrie des Dispositifs Médicaux: La Problématique des Rapports d'évaluation Clinique' (2019) 77(5) Annales de Biologie Clinique 514.

[69] For a critical assessment of this draft, see Vera Lúcia Raposo, 'Ex Machina: Preliminary Critical Assessment of the European Draft Act on Artificial Intelligence' (2022) 30(1) International Journal of Law and Information Technology 88.

[70] European Parliament Legislative Resolution of 13 March 2024 on the Proposal for a Regulation of the European Parliament and of the Council on Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD) (AI Act) <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html> accessed 29 April 2024.

[71] See ibid art 5(1)(h).

[72] For example, identification of people going in and out of the hospital.

[73] For example, for identification of a genetic disease.

system; and keep detailed documentation to allow the authorities in charge to assess compliance with the legal requirements.[74] Only if these requirements are met will the high-risk AI systems get the CE mark, following a prior conformity assessment.[75]

The assessment imposed by the AI Act can be either a self-assessment carried out by the AI developer itself or an assessment carried out by a third party (the notified body), in place for AI systems that are products or part of products already submitted by EU law to third-party conformity assessment (Article 43 AI Act). AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons require a third-party conformity assessment (Article 43(1) and Annex III, point 1 of the AI Act). The only exception to this rule is when the system complies with harmonised standards, to be developed by European standardisation entities.[76] As mentioned, some FR solutions that can be placed in the healthcare settings will fit into this category, as will be the case for FR cameras designed to control who comes in and out of the hospital or to identify patients for check-in purposes.

The AI Act clarifies that the conformity assessment to be carried out for high-risk systems already subject to a third-party conformity assessment will be 'merged'. Therefore, AI medical devices (such as FRT systems used for the diagnostic of certain medical conditions) will be subject to one single conformity assessment, encompassing the requirements imposed by the AI Act and the ones imposed by the MDR (Article 43(3) AI Act),[77] but it is not clear how a single assessment will, in practice, oversee so many requirements. Likewise, and even though the same norm seems to indicate that the notified bodies certified under the MDR will also be entitled to intervene under the AI Act,[78] it is unclear how that very entity will be able to carry out such different assessments.[79]

After being launched on the market, high-risk AI systems are subject to market surveillance. Providers of these systems are in charge of reporting serious incidents and malfunctions (Articles 72 and 73 AI Act). The ex-post control mechanism is also to be carried out by market surveillance authorities (Article 74 AI Act), which vary according to the domain in which they operate. In the health domain this control will most likely be performed by health authorities, eventually the very same ones in charge of the post-marketing surveillance of medical

---

[74] Such requirements were inspired by the ethical guidelines of the High-Level Expert Group on AI. See High-Level Expert Group on AI (AI HLEG), 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> accessed 29 April 2024.

[75] Theodore Christakis, M Becuywe and AI-Regulation Team, 'Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021' (2021) 4 <https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021/> accessed 29 April 2024.

[76] ibid.

[77] Anastasiya Kiseleva, 'AI as a Medical Device: Between the Medical Devices Framework and the General AI Regulation' in Hervé Jacquemin (ed), *Time to Reshape the Digital Society* (Larcier 2021) 423, 432–33.

[78] ibid 432.

[79] Erik Vollebregt, 'The New EU AI Regulation Proposal, Medical Devices and IVDs' (*Medical Devices Legal*, 3 May 2021) <https://medicaldeviceslegal.com/2021/05/03/the-new-eu-ai-regulation-proposal-medical-devices-and-ivds> accessed 29 April 2024.

devices.[80] Ultimately, the ex-post control can lead to the withdrawal of the AI system from the market.

5. FINAL CONSIDERATIONS

FR, like many other types of AI systems, has enormous potential in healthcare, either for effective medical purposes or to assist in the running of healthcare facilities. The main challenge, however, is compliance. FR systems fall under the scope of various extremely detailed and demanding European regulations, making it difficult for developers and users to comply with the numerous legal demands.

The problem is that the current legal paradigm is overly complex, with potential overlaps (involving conformity assessments and notified bodies) and conflicting requirements (for instance, the imposition to use a wide array of data to train AI systems, as set out in Article 10(3) of the AI Act, might be jeopardised by the limitations derived from the GDPR pertaining to personal data).

A legal puzzle in which not all pieces fit together is a legal hurdle for developers and users of FR, and might undermine its use in healthcare. While the benefits of AI may be lost to legal hurdles, technology usually overcomes those hurdles. In the words of Andrew S. Grove, one of the 'fathers' of Silicon Valley, 'Technology will always win. You can delay technology by legal interference, but technology will flow around legal barriers.'[81]

---

[80] See Medical Device Regulation (n 62) Annex III.

[81] Jeff Burt, 'Former Intel CEO Andy Grove Dies at 79' (*eWEEK*, 22 March 2016) <https://www.eweek.com/pc-hardware/former-intel-ceo-andy-grove-dies-at-79/> accessed 29 April 2024.