Title: Technical and legal challenges of the use of automated facial recognition technologies for law enforcement and forensic purposes

Author: Patricia Faraldo Cabana, Professor of Criminal Law, Universidade da Coruña, Spain, Adjunct Professor, Queensland University of Technology, Australia
Facultad de Derecho, Campus de Elvina, 15071 A Coruña, Spain
patricia.faraldo@udc.es

Abstract: Biometrics covers a variety of technologies used for the identification and authentication of individuals based on their behavioral and biological characteristics. A number of new biometric technologies have been developed, taking advantage of our improved understanding of the human body and advanced sensing techniques. They are increasingly being automated to eliminate the need for human verification. As computational power and techniques improve and the resolution of camera images increases, it seems clear that many benefits could be derived through the application of a wider range of biometric techniques for security and surveillance purposes in Europe. Facial recognition technology (FRT) makes it possible to compare digital facial images to determine whether they are of the same person. However, there are many difficulties in using such evidence to secure convictions in criminal cases. Some are related to the technical shortcomings of facial biometric systems, which impact their utility as an undisputed identification system and as reliable evidence; others pertain to legal challenges in terms of data privacy and dignity rights. While FRT is coveted as a mechanism to address the perceived need for increased security, there are concerns that the absence of sufficiently stringent regulations endangers fundamental rights to human dignity and privacy. In fact, its use presents a unique host of legal and ethical concerns. The lack of both transparency and lawfulness in the acquisition, processing and use of personal data can lead to physical, tangible and intangible damages, such as identity theft, discrimination or identity fraud, with serious personal, economic or social consequences. Evidence obtained by unlawful means can also be subject to challenge when adduced in court. This paper looks at the technical and legal challenges of automated FRT, focusing on its use for law enforcement and forensic purposes in criminal matters. The combination of both technical and legal approaches is necessary to recognize and identify the main potential risks arising from the use of FRT, in order to prevent possible errors or misuses due both to technological misassumptions and threats to fundamental rights, particularly – but not only – the right to privacy and the presumption of innocence. On the one hand, a good part of the controversies and contingencies surrounding the credibility and reliability of automated FRT is intimately related to their technical shortcomings. On the other hand, data protection, database custody, transparency, accountability and trust are relevant legal issues that might raise problems when using FRT. The aim of this paper is to improve the usefulness of automated FRT in criminal investigations and as forensic evidence within the criminal procedure.

Keywords: biometrics, privacy, dignity, forensics, facial recognition, infallibility

Introduction

Biometrics covers a variety of automated technologies used for the identification and authentication of individuals based on their behavioral, physical and biological characteristics. The main biometric methods that are in use today are still fingerprint and DNA technologies. As computational power and techniques improve and the resolution of sensor modules increases, it seems clear that many benefits could be derived through the application of a wider range of biometric techniques for law enforcement and forensic purposes. Facial recognition technology (FRT), taking advantage of our improved understanding of the human body and advanced sensing techniques, makes it possible to uniquely identify individuals. It provides advantages over traditional identification methods, since 1) it is based upon who the person is and inherent characteristics that exist within the human body, which are much harder to replicate than a passport or a social security card, allowing to avoid circumvention, that is, copy or imitation by using artefacts; and 2) it is possible to capture facial images in unconstrained environments, using, for instance, video surveillance cameras or multimedia content available on social networking sites, such as photos or video recordings. Facial biometric systems are increasingly used as security and surveillance mechanisms in Europe, but there are many difficulties in using such evidence to secure convictions in criminal cases. Some are related to their technical shortcomings, which impact their utility as evidence, while others to the need to provide safeguards and protection to human rights, which has led to the EU and national legislatures putting restrictions upon the storage, processing and usage of facial biometric data, since people's facial images are recognized as sensitive data. Moreover, the use of automatic systems, which compare images and generate a matching score, with no human intervention, add its own challenges. As a result, examples of national law enforcement authorities in the EU using such systems are still quite sparse,[1] even though several are testing their potential.

This paper looks at the technical (section 2) and legal challenges of FRT (section 3), focusing on its use for law enforcement and forensic purposes in criminal matters. Recognizing that automated facial recognition has the potential to revolutionize the identification process, facilitate crime detection and reduce misidentification of suspects, the aim of this paper is to improve its usefulness as intelligence data in police investigations and as forensic evidence in the criminal justice system by highlighting the critical issues that hinder a wider use. This fills an important gap in literature. Certainly, there is a vast amount of research into the area of application of biometric techniques in forensic investigations. It has been boosted in the last two decades by computational intelligence techniques replacing manual identification approaches in forensic sciences (Saini and Kapoor, 2016) and the wide range of applications for traditional and cybercrime detection (Dilek et al., 2015). Much has been said about how automated biometric technologies in general, and FRT in particular, provide advantages over traditional identification methods. A combined analysis of technical shortcomings and legal limits of the identification of facial images for their use for investigative purposes, however, have largely escaped scientific scrutiny. The combination of both technical and legal approaches is necessary to recognize and identify the main potential risks arising from the use of FRT, in order to prevent both possible errors due to technological misassumptions and threats to fundamental rights, including, among others, human dignity, the right to respect for private life, the protection of personal data, non-discrimination, the rights of the child and the elderly, the rights of people with disabilities,

[1] FRT in relation to criminal investigations has been implemented in 11 EU member states and in two international police cooperation organizations, Europol and Interpol. Currently, 7 member states expect to implement it until 2022 (TELEFI, 2021, p. 22). FRT is much more frequent in the USA. Already in 2012 the FBI launched the Interstate Photo System Facial Recognition Pilot project in three states, a system fully deployed as of June 2014, now integrated in the Next Generation Identification System, which provides the US criminal justice community with the world's largest electronic repository of biometric and criminal history information. For other applications at state and local level, see New York City Bar Association (2020).

and the right to an effective remedy and to a fair trial (FRA, 2019). On the one hand, a good part of the controversies and contingencies surrounding the credibility and reliability of facial biometrics for law enforcement and forensic purposes is intimately related to its technical shortcomings. On the other hand, data acquisition and protection, database custody, transparency, fairness, accountability and trust are relevant legal issues that might raise problems when using FRT results as traces that target individuals and trigger police action which may have a very significant impact on their lives and freedoms.

The topic is definitely a timely one. The EU General Data Protection Regulation 2016/679[2] (henceforth GDPR), which came into force in 2018, created a complex set of new rules for the collection, storage and retention of personal data. It introduces several categories of personal data to which different regimes apply. The GDPR prohibits the processing of biometric data for the purpose of uniquely identifying natural persons – interestingly, verification, one-to-one comparison, is another kind of use and purpose than identification, or one-to-many comparison (Kindt, 2018, pp. 526-527). Such a processing is considered very privacy intrusive and likely to result in a high risk to the rights and freedoms of natural persons. Therefore, only if the processing operation falls within one of the exemptions under article 9(2) GDPR or the relevant national legislation – the GDPR grants EU member states some discretion to adopt or modify existing legal rules -, it is possible to process biometric data for the purpose of uniquely identifying individuals. There is a new obligation for the controllers to assess the impact and risks of such operations in a data protection impact assessment and to take safeguards, and if needed, to consult with the supervisory authority and obtain authorization. In the same line, Directive 2016/680[3] (henceforth LED, Law Enforcement Directive) prohibits automated decisions that produce adverse legal effects concerning the data subject or significantly affect him or her, unless such decisions are authorized by EU or member state law and include appropriate safeguards for the rights and freedoms of the data subject. Therefore, it is not sufficient to circumscribe the pertinent assessment to a reading of the GDPR. It is necessary to move towards an assessment of national legislation that either specifies the GDPR requirements or implements the LED, as member states might adopt exemptions or derogations that modulate the safeguards eventually available to individuals when their data are processed for law enforcement and forensic purposes. Therefore, the current legal landscape is fragmented. These contingencies have led to a lack of clarity on the legal requirements surrounding the automated processing of personal biometric data (Kindt, 2018).

Technical Shortcomings of FRT

Although facial biometrics have achieved satisfactory results in controlled environments, various factors such as expression, pose and occlusion, as well as sensor quality and calibration limit the practical application of this technology. Due to different positioning on the acquiring sensor, imperfect imaging conditions, environmental changes, bad user's

[2] 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 L119/89.

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

interaction with the sensor, etc., it is impossible that two samples of the same face, acquired in different sessions, exactly coincide, even if they are photographs of a suspect taken under controlled conditions (Zeinstra et al., 2018, p. 24; Tistarelli et al., 2014). There are also variations due to ageing or physical changes like beard, glasses, change in hairstyle, etc. For this reason, a facial biometric matching systems' response is also typically a matching score that quantifies the similarity between the input and the database template representations. Therefore, the automated recognition of individuals offered by facial biometric systems must be tempered by an awareness of the uncertainty associated with that recognition.

In fact, in the capture or acquisition stage, due to the natural changes in the face and expression over time as well as other challenges such as varying illuminations, poor contrast and non-cooperative approach by subjects, FRT may lead to limited recognition performances (Sarangi et al., 2018; Zeinstra et al., 2018). Facial recognition in many instances has proved unreliable for visual surveillance and identification systems. Certainly, facial biometrics are related to physical features, but there are cases in which facial features are not available, for example, for religious or sanitary reasons – e.g., Islamic veil, face mask or surgical mask -, or because those who are planning to commit crimes are aware of the fact that visual surveillance mechanisms are in operation in the area and therefore they take steps to avoid detection from the cameras by hiding their faces or disguising their physical appearance through 3D masks, make-up, facial hair, glasses or surgical operations. On the other hand, reliable acquisition of the input signal is another challenge. Changes in scale, location and in-plane rotation of the face, as well as rotation in depth - facing the camera obliquely - may seriously affect performance. Sensor quality and calibration also play an important role. Captured video image data of facial figures may have many shortcomings. For example, a too low resolution in order to reliably identify the subject from his or her facial characteristics (Bouchrika, 2016; Singh and Prasad, 2018, p. 537), or a too far distance to the subject, since facial features may not be recovered from a given distance. There are, though, some promising approaches using 3D face recognition systems (Zhou and Xiao, 2018) and night vision capacities based on thermal facial imagery (Riggan et al., 2018).

Once acquired, the raw biometric data of an individual is first assessed and, when needed, subjected to signal enhancement algorithms to improve its quality. In this phase, algorithms can be manipulated, either to escape detection or to create impostors. For example, knowledge of the feature extraction algorithms can be used to design special features in presented biometric samples to cause incorrect features to be calculated.[4] Subsequently, the initial biometric sample is transformed into a digital template that contains only the information needed to run the pattern recognition algorithm. In the comparison stage, the template is compared with another registered template in the system to produce a score-based likelihood ratio or matching ratio, according to which the

[4] This section concentrates on system vulnerabilities which are part of the biometric processing itself. Since biometric systems are implemented on server computers, they are vulnerable to all cryptographic, virus, and other attacks which plague any computer system. For example, biometric data may be stored locally on hardware within the organization, or externally at an unknown location within the cloud (Tomova, 2009), both vulnerable to hacking. The training dataset may be subject to intentional manipulations, such as data poisoning attacks (Papernot et al., 2018) and backdoor injections (Chen et al., 2017). Vulnerabilities of data storage concern modifying the storage (adding, modifying or removing templates or raw data), copying data for secondary uses (identity theft or directly inputting the information at another stage of the system to achieve authentication) and modifying the identity to which the biometric is assigned. We are aware of these issues, but do not intend to cover them in this paper.

identification of a person or the verification of her or his identity is validated or rejected. At this stage, the false non-match rate (FNMR) and the false match rate (FMR) are functions of the system threshold: If the designer decreases the acceptance threshold to make the system more tolerant to input variations, FMR increases, while if the acceptance threshold is raised to make the system more secure, FNMR increases accordingly (Fish et al., 2013). In short, designers can set the acceptance threshold value at will (Kotsoglou and Oswald, 2020, p. 88). In order to do it, however, the task, purpose and context of the FRT use is important: When applying the technology in places visited by millions of people – such as airports or train stations – a relatively small proportion of errors still means that hundreds of individuals are wrongly flagged, that is, either they are incorrectly identified or incorrectly rejected as a match. The consequences of these two errors are different depending on the situation. For example, if the police use a facial recognition algorithm in their efforts to locate a fugitive, a false positive can lead to the wrongful arrest of an innocent person, while a false negative may help the suspect to slip through. Each case requires a determination of the cost of different kinds of errors, and a decision on which kind of errors to prioritize. Accordingly, industrial settings such as the mentioned acceptance threshold should reflect the institutional architecture of the criminal process including its overriding objectives, i.e. acquitting the innocent, convicting the guilty and the acceptable rate of errors/trade-off between these objectives. The renowned Blackstone-ratio, stressing the ’fundamental value […] of our society that it is far worse to convict an innocent man than to let a guilty man go free’ (Blackstone, 1769 [1893], p. 358), illustrates this point.

The probabilistic nature of facial biometric systems also means that the measured characteristics of the population of those subjects the system is designed to recognize matter and affect design and implementation. A large amount of training data is required to obtain good accuracy. Because of the biased composition of police datasets, mostly white, male-dominated, but with an overrepresentation of ethnic and racial minorities, algorithms trained with these data increase the risk of false identification of women and minorities. Unequal error rates are not always indicative of bias, but they may reflect a pre-existing societal bias and can lead to inaccurate outcomes that infringe on people’s fundamental rights, including equality and non-discrimination (Eubanks, 2018).

Furthermore, the utility of facial recognition software is dependent on practitioners’ understanding of how to use it. The algorithmic process renders a match between a face captured on video and an image on the database, but then there are two possibilities. In the first one, the system operator, i.e. a human being (police officer, forensic expert), has to intervene and make his or her assessment by reviewing the ‘match’. Without specialized training, personnel reviewing matches may achieve false results. This training is not regulated. In the second one, whenever a human is not reviewing the match a confidence threshold should be introduced to prevent adverse effects on those being misidentified, requiring the algorithm to only return a result if it is x% certain of its findings. However, there are no existing standards for police, the courts and the public to assess the accuracy of facial biometric systems. There is a lack of methodological standardization and empirical validation, notably when using automatic systems (Jacquet and Champod, 2020). Despite extensive research in the area, automated FRT is still struggling to achieve sufficient reliability and repeatability for its use in forensic identifications. Moreover, regarding criminal databases, the requirements for facial images and the practices used for quality assurance show significant variations between EU member states, most of which do not apply quality standards for image capture or database entry, performed neither by human intervention nor automatically by the software (TELEFI, 2021, pp. 29-30).

Even though in the last years there have been massive steps forward in the technology´s performance (Galbally et al., 2019), no current system can claim to handle all of these problems well. Moreover, only limited studies have been done on accuracy and reproducibility. To overcome reliability issues of FRT and increase the possibility of recognition and verification, a multimodal fusion of a selection of biometric modalities or multiple aspects of the same feature has been proposed (Saini and Kapoor, 2016; Tistarelli et al., 2014; Ross et al., 2006). Recent advances in facial biometric technologies suggest complementing facial recognition systems with facial soft biometric traits (Arigbabu et al., 2015; Dantcheva et al., 2011). These traits can be typically described using human understandable labels and measurements, allowing for retrieval and recognition solely based on verbal descriptions. They can be physical - such as eye and hair color, skin, presence of facial hair (beard, moustache), scars, marks and tattoos, sex, body geometry, height and weight - or behavioral - like gait or keystroke. Soft biometrics are only relatively useful to identify individuals - they lack of sufficient permanence and distinctiveness (Tome et al., 2015) -, but they can complement the performance of facial recognition systems. For example, these additional techniques remove the difficulties inherent to facial biometric techniques due to expression, occlusion and pose. They take advantages of high resolution images and rely upon micro-features in the face to increase reliability. These techniques, however, still fail to overcome the difficulties that arise where the face is obscured by the suspect. Moreover, although data fusion may involve the same biometric trait – face -, acquired from different devices, little effort has been devoted to the multimodal integration and fusion of data from multiple sensor modules (Tistarelli et al., 2014).

Legal Challenges of FRT

FRT is coveted as a mechanism to address the perceived need for increased security, but there are many aspects of these technologies that give rise to legal concerns regarding their use for law enforcement and forensic purposes. The first problem is related to the taking of the biometric sample from the individual through image capture (Benzaoui et al., 2017). Fingerprint and DNA methods, while being long standing methods of being used as proof of crimes, require invasive methods for their collection. Hence, only those who have already been suspected or convicted of crimes have their information stored in a database, which limits the detection of crime to existing offenders. By contrast, facial recognition is unique from other forms of biometric surveillance in that it tracks one's face, that is, something that is difficult to hide and easy to observe in the open, without the consent of the observed person. Researches in the field of FRT appear to regard the ability to obtain biometric data by non-invasive means and without the requirement to obtain consent from the data subject as a benefit (see, for instance, Singh and Prasad, 2018, p. 537). Certainly, depending on the perspective, the reduced requirement for human subject compliance may be an advantage of this method (New York City Bar Association, 2020, p. 2; Arigbabu et al., 2015). Capture without constraint is a prerequisite in surveillance environments and lightens the workload of criminal investigations. It allows authorities to circumvent the legal limitations inherent within the collection of DNA and fingerprint evidence. At the same time, it subjects these techniques to significant privacy concerns about the collection of such data (Kindt, 2018, 2013, pp.

297-306), which in turn lead to significant civil and political resistance against such a collection due to its high potential for misuse.

The second concern regards the processing of the acquired image, including, whether or not by automated means, collecting, recording and storing (Article 4.2 GDPR). In respect of data protection, the processing of a subject's image with FRT individualizes him or her from others. Since this act constitutes the processing of sensitive personal data, data protection principles apply. As a general principle, the processing of biometric data for the purpose of uniquely identifying a natural person, as the processing of all other special categories of personal data, is forbidden for all entities falling under the material scope of the GDPR, including public authorities, governments and private organizations (Article 9.1 GDPR). However, several exemptions from the prohibition exist (Article 9.2 GDPR). Moreover, for law enforcement agencies (LEAs) a separate regime applies. They are allowed to process biometric data for unique identification under three cumulative conditions: (i) if 'strictly necessary', and (ii) if subject to appropriate safeguards for the rights and freedoms of the data subject, and only (iii) (a) where authorized by Union or member state law; (b) to protect the vital interests of the data subject or of another natural person; or (c) where such processing relates to data which are manifestly made public by the data subject (Article 10 LED). Therefore, for LEAs, further national law is awaited implementing Directive 2016/680, which does not prohibit per se the use of biometric data for identification purposes. Such national law is still not enacted in many countries or does not offer clear guidance on police collection and use of biometric data.

The third problem is related to the storage of the image or template in a database. Challenges are similar to those posed by human genetics databases (Sutrop, 2010). Retention of all available data on those who have committed serious crimes seems to be unproblematic (Bichard, 2004). It leads to the improved detection of crime and act as a deterrent. Conversely, retention of biometric data of individuals who have not been convicted of a criminal offence, even if deemed dangerous, has been subjected to successful legal challenge in some jurisdictions, such as the United Kingdom[5] or France.[6] Furthermore, the European Court of Human Rights clearly stated in S. and Marper[7] that already the mere retention of fingerprints – because objectively containing unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances - by LEAs amounts to an interference with the

[5] For example, in S & Marper v United Kingdom [2008] ECHR 1581, the European Court on Human Rights found the retention by the British police of DNA samples of individuals who had been arrested but had later been acquitted, or who had had the charges against them dropped, to be a violation of their right to privacy under Article 8 ECHR (Sampson 2018). Furthermore, in some EU member states the indefinite retention of biometric samples, including DNA evidence and fingerprints of data subjects, has been successfully challenged, except for in exceptional circumstances. See, for the (pre-Brexit) UK, R (on the application of GC & C) v The Commissioner of Police of the Metropolis [2011] UKSC 21. Also in the UK the High Court of Justice (England and Wales) was called upon to determine whether the current legal regime in that country was 'adequate to ensure the appropriate and non-arbitrary use of automated facial recognition in a free and civilized society'. In R (Bridges) v Chief Constable of the South Wales Police [2019] EWHC 2341 (Admin), the judgment was that the use of FRT was not 'in accordance with law' and implied a breach of Article 8 (1) and (2) ECHR and of data protection law, and it failed to comply with the public sector equality duty.

[6] The Constitutional Court in France stated that the keeping of a database with biometric identity information allowing identification interferes with the fundamental right to respect of privacy. Cons. const. (France) no. 2012-652, 22 March 2012 (Loi protection de l'identité), Article 6.

[7] ECtHR, S. and Marper v. United Kingdom, nos. 30562/04 and 30566/04, 4 December 2008, Articles 84 and 86.

right to respect for private life. This applies even more when such data undergo automatic processing and are retained and used for police purposes for an indeterminate period without appropriate guarantees, such as the prospect of a successful request to be removed.[8] Since European and national case law tend to favor a strict interpretation of the necessity and proportionality tests as they apply to law enforcement use, the critical issue therefore is how to achieve the correct balance between the needs of LEAs to detect those responsible for serious crimes and the needs of the public to keep their own personal data private and protected from misuse.

The fourth concern regards the use of facial biometric data for purposes other than the one for which they were originally captured and stored. The gradual widening of the use of a technology or system beyond the purpose for which it was originally intended is known as 'function creep'. It occurs whenever the original purpose for which the data collection is justified is overreached and the biometric data is used for other purposes (Mordini and Massari, 2008, p. 490).). Such an expansion to other domains entails both technical and legal risks. One example of the former is using the data collected in a domain purely for the sake of convenience in a domain that demands high data integrity, assuming incorrectly that collected data are of greater fidelity that they really are (National Research Council, 2010, p. 4). For the latter, vast name and face databases of law-abiding citizens already in existence (i.e. driver's license records, ID photos, databases relating to aliens, asylum seekers or missing persons), which were created for purposes other than investigative ones, may be used to access facial images that allow the identification of persons not in custody for which reasonable suspicion of criminal involvement may not be present. Currently, the police of some EU member states has legal access to non-criminal databases containing facial images that can be used for facial recognition in criminal investigations (TELEFI, 2021, p. 31). Such a police seizure of a person registered in these civil databases for the purpose of subjecting that person to an identification procedure does implicate the right to privacy.

The fifth concern is related to the impact of these technologies on racial and ethnic minorities and other vulnerable and disadvantaged groups. On a general level, facial recognition software trained with police databases has a higher chance of disproportionately affecting racial and ethnic minorities when used for law enforcement purposes. Members of these minorities are more likely to be enrolled in these database systems as they are arrested and subject to criminal law proceedings at a higher rate than their population share. This disproportion leads to a vicious circle in which more members of minorities are detected, which in turn amplifies the need to police minority groups already heavily over-policed. In turn, if trained with other biometric data sets, facial recognition software is usually built around whiteness, maleness and ability as default categories (Browne, 2015, p. 113), showing disproportionate failure at 'the intersection of racialized, queered, gendered, classed, and disabled bodies' (Magnet, 2011, p. 50), where the characteristic uncertainty of facial biometrics is greater (Abdurrahim et al., 2018; Howard and Etter, 2013; Beveridge et al., 2009). Moreover, the attempt to reduce identity to a bodily characteristic is especially problematic for subjects who are already in a marginalized position (Wevers, 2018). In fact, biometric technologies do not recognize that identities and faces have social and cultural dimensions (Sharp, 2000), and that identity is much more than a face or a bodily appearance.

[8] ECtHR, M.K. v. France, no.19522/09, 18 April 2013, Articles 44–46 ('ECtHR, M.K. 2013').

Last but not least, scores generated by AI-based software have proved to be highly influential on human decision-makers, who may find it difficult to bypass the system output (Cooke and Michie, 2013). In general, many studies have shown that police officers, courts and jurors have difficulties in discerning reliable biometric evidence from unreliable evidence, and as a consequence they place too high a probative value on such evidence (Završnik, 2020; Maeder et al., 2017; Freeman, 2016; Cummings, 2014; Garrett and Mitchell, 2013). The reliability problem is not unique to these so-called second generation forensic techniques (Murphy, 2007), such as facial and iris-based biometric systems (Thompson 2018; Keenan 2015), automated speaker recognition (Bonastre et al., 2015, pp. 263-275) or automated handwriting identification and verification (Working Group on Human Factors in Handwriting Examination, 2020, pp. 68-71). Traditional biometric techniques, such as DNA (Lieberman et al., 2008), fingerprints (Nigam et al., 2015; Cole, 2004, p. 73), handwriting (Sulner, 2018) or voice identification (Morrison et al., 2016), also fail sometimes to meet standards of scientific validation, despite their long history of admissibility.

Conclusion

FRT has been promoted as the 'magic bullet' that will solve the problem of the real and urgent need to accurately identify people on the internet, especially since many financial crimes and other crimes of deception are committed online (Keenan, 2015). But, as shown in section 2, the aura of infallibility sometimes associated with automated biometric technologies generates expectations that are often not met in the concrete reality of criminal investigations. Automated facial recognition is an inherently probabilistic endeavor, and hence inherently fallible. The probabilistic nature of the output, and the building of certain values into the tool, raise questions as to the justifiability of regarding the tool's output as 'objective' grounds for reasonable suspicion (Kotsoglou and Oswald, 2020, p. 86). Some of the obstacles to reliability of such methods have been considered here. Certainly, there is constant innovation in the area of facial biometric technologies that seeks to overcome the difficulties of existing applications, such as the use of soft biometrics, but they still need some time to spread. Furthermore, as detailed in section 3, there are also concerns about fundamental rights protection, function creep and social discrimination. To overcome them, transparency is an important tool. But biometric technologies are still ruled by proprietary solutions, kept secret and protected by patents. In many cases, that bars an independent evaluation of the device performances and of its real capabilities (Esposito, 2012, p. 9). If the right to a fair trial is to be upheld, the means by which the identification takes place must be disclosed to the defense, together with information regarding disregarded 'matches' and error rates and uncertainties of the system itself (Kotsoglou and Oswald, 2020, p. 88). The GDPR requires the explainability of decisions made by algorithms, but there is a gap with regards to tools and techniques that enable the forensic analysis of performance and failures in AI-enabled systems and the quantification of uncertainty (Baggili and Behzadan, 2019, p. 1; Champod and Tistarelli, 2017). FRT is no exception in this regard. This compromises the legal soundness of the results.

There are also other challenges that still prevent the large-scale adoption of facial biometric techniques within criminal investigations. Most importantly, biometric data derive from the human body. From a legal perspective, there are understandably areas of resistance based upon individual, religious or socio-cultural factors (Tomova, 2009, p. 112). Fair processing of personal data requires that the data subject be informed of the storage of data. The data controller also has responsibility to establish a certain degree of accuracy of the system and to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, for instance by ensuring him or her the right to obtain human intervention on the part of the controller, to express his or her point of view, and to contest the decision, including the right of the data subject to receive meaningful information about the logic involved in automated processing. Hence there is a need within the various cultural, social and religious contexts for the right balance to be achieved between security needs for identification and verification and legal and ethical requirements for data protection. More uniform, comprehensive laws are also needed to fill the regulatory void, particularly evident at national level. These laws should provide the conditions that make acceptable the exceptional use of FRTs by LEAs. The setting of minimum accuracy standards across the industry can also reduce uncertainty of what defines an acceptable use of FRTs for law enforcement and forensic purposes.

Even with the present deficits, there are clear advantages of automated facial biometric approaches to criminal investigations. In particular, automated FRTs help in analyzing the evidence by overcoming the limitations of human cognitive abilities and thus increase both the efficiency and effectiveness of investigations. Moreover, these methods provide a solid scientific basis for the standardization of crime investigation procedure. They show a great potential as an instrument to help the experts to assess the strength of evidence and complement the human-based approach.

References

Abdurrahim, S. H., Samad, S. A., & Huddin, A. B. (2018). Review on the effects of age, gender, and race demographics on automatic face recognition. *The Visual Computer*, *34*, 1617-1630. https://doi.org/10.1007/s00371-017-1428-z

Arigbabu, O. A., Ahmad, S. M. S., Adnan, W. A. W., & Yussof, S. (2015). Recent advances in facial soft biometrics. *The Visual Computer*, 31, 513–525. https://doi.org/10.1007/s00371-014-0990-x

Baggili, I., & Behzadan, V. (2019). Founding The Domain of AI Forensics. arXiv:1912.06497v1.

Benzaoui, A., Adjabi, I., & Boukrouche, A. (2017). Experiments and improvements of ear recognition based on local texture descriptors. *Optical Engineering*, *56*, 043109. https://doi.org/10.1117/1.OE.56.4.043109

Beveridge, J. R., Givens, G. H., Phillips, P. J., Draper, B. A. (2009). Factors that influence algorithm performance in the face recognition grand challenge. *Computer Vision and Image Understanding*, *113*(6), 750-762. https://doi.org/10.1016/j.cviu.2008.12.007

Bichard, M. (2004). *The Bichard Inquiry. Report* (No. HC 653). The Stationary Office.

Blackstone, W. (1893). *Commentaries on the laws of England*. J. B. Lippincott Co. Originally published in 1769.

Bonastre, J.-F., Kahn, J., Rossato, S., & Ajili, M. (2015). Forensic Speaker Recognition: Mirages and Reality. In S. Fuchs, D. Pape, C. Petrone, & P. Perrier (Eds.), *Individual Differences in Speech Production and Perception* (pp. 255-285). Peter Lang.

Bouchrika, I. (2016). Evidence Evaluation of Gait Biometrics for Forensic Investigation. In A. E. Hassanien, M. M. Fouad, A. A. Manaf, M. Zamani, R. Ahmad, & J. Kacprzyk (Eds.), *Multimedia Forensics and Security: Foundations, Innovations, and Applications* (pp. 307–326). Springer.

Browne, S. (2015). B®anding Blackness: Biometric Technology and the Surveillance of Blackness. In S. Browne (Ed.), *Dark Matters: On the Surveillance of Blackness* (pp. 89-130). Duke University Press.

Champod, C. & Tistarelli, M. (2017). Biometric Technologies for Forensic Science and Policing: State of the Art. In M. Tistarelli, M., & C. Champod (Eds.), *Handbook of Biometrics for Forensic Science* (pp. 1-15). Springer.

Chen, X., Liu, C., Li, B., Lu, K., & Song, D. (2017). Targeted backdoor attacks on deep learning systems using data poisoning. arXiv preprint arXiv:1712.05526.

Cole, S. A. (2004). Fingerprint Identification and the Criminal Justice System. In D. Lazer (Ed.), *DNA and the Criminal Justice System. The Technology of Justice* (pp. 63-89). MIT Press.

Cooke, D. J., & Michie, C. (2013). Violence risk assessment: from prediction to understanding - or from what? To why? In C. Logan, & L. Johnstone (Eds.), *Managing Clinical Risk* (pp. 22-44). Routledge.

Cummings, M. L. (2014). *Automation Bias in Intelligent Time Critical Decision Support Systems*. American Institute of Aeronautics and Astronautics.

Dantcheva, A., Velardo, C., D'Angelo, A., & Dugelay, J.-L. (2011). Bag of soft biometrics for person identification. New trends and challenges. *Multimedia Tools and Applications*, *51*, 739-777. https://doi.org/10.1007/s11042-010-0635-7

Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. *International Journal of Artificial Intelligence and Applications*, *6*(1), 21-39.

Esposito, A. (2012). Debunking some myths about biometric authentication. ArXiv abs/1203.03333.

Eubanks, V. (2018). *Automating Inequality. How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

Fish, J. T., Miller, L. S., & Braswell, M. C. (2013). *Crime Scene Investigation*. Routledge.

Galbally, J., Ferrara, P., Haraksim, R., Psyllos, A. I., & Beslay, L. (2019). *Study on Face Identification Technology for its Implementation in the Schengen Information System*. Publications Office of the European Union.

FRA European Union Agency for Fundamental Rights (2019) Facial recognition technology: fundamental rights considerations in the context of law enforcement. Available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

Garrett, B., & Mitchell, G. (2013). How Jurors Evaluate Fingerprint Evidence: The Relative Importance of Match Language, Method Information, and Error Acknowledgment. *Journal of Empirical Legal Studies*, *10*(3), 484-511.

Freeman, K. (2016). Algorithmic injustice: how the Wisconsin Supreme Court failed to protect due process rights in state V. Loomis. *North Carolina Journal of Law and Technology*, *18*(5), 75–106.

Howard, J. J., & Etter, D. (2013). The Effect of Ethnicity, Gender, Eye Color and Wavelength on the Biometric Menagerie. 2013 IEEE International Conference on Technologies for Homeland Security (HST), IEEE.

Jacquet, M., & Champod, C. (2020). Automated face recognition in forensic science: Review and perspectives. *Forensic Science International*, *307*: 110124. https://doi.org/10.1016/j.forsciint.2019.110124

Keenan, T. P. (2015). Hidden Risks of Biometric Identifiers and How to Avoid Them. In Canadian Global Affairs Institute, *Black Hat USA 2015* (pp. 1-13). University of Calgary.

Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*. Springer.

Kindt, E. J. (2018). Having yes, using no? About the new legal regime for biometric data. *Computer Law & Security Review*, *34*, 523–538. https://doi.org/10.1016/j.clsr.2017.11.004

Kotsoglou, K. N., & Oswald, M. (2020) The long arm of the algorithm? Automated Facial Recognition as evidence and trigger for police intervention. *Forensic Science International: Synergy*, *2*, 86-89. https://doi.org/10.1016/j.fsisyn.2020.01.002

Lieberman, J. D., Carrell, C. A., Miethe, T. D., & Krauss, D. A. (2008). Gold versus platinum: Do jurors recognize the superiority and limitations of DNA evidence compared to other types of forensic evidence? *Psychology, Public Policy, and Law*, *14*(1), 27–62. https://doi.org/10.1037/1076-8971.14.1.27

Maeder, E.M., Ewanation, L.A., Monnink, J. (2017). Jurors' Perceptions of Evidence: The Relative Influence of DNA and Eyewitness Testimony when Presented by Opposing Parties. *Journal of Police and Criminal Psychology*, *32*, 33-42. https://doi.org/10.1007/s11896-016-9194-9

Magnet, S. (2011). *When Biometrics Fail: Gender, Race, and the Technology of Identity,* Duke University Press.

Mordini, E., & Massari, S. (2008). Body, Biometrics and Identity. *Bioethics*, *22*(9), 488-498.

Morrison, G. S., Sahito, F. H., Jardine, G., Djokic, D., Clavet, S., Berghs, S., & Goemans Dorny, C. (2016). INTERPOL Survey of the Use of Speaker Identification by Law Enforcement Agencies. *Forensic Science International*, *263*, 92-100.

Murphy, E. (2007). The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence. *California Law Review*, *95*(3), 721-797. https://doi.org/10.15779/Z38R404

New York City Bar Association (2020). Power, Pervasiveness and Potential: The Brave New World of Facial Recognition Through a Criminal Law Lens (and Beyond). Available at http://documents.nycbar.org.s3.amazonaws.com/files/2020662-BiometricsWhitePaper.pdf

National Research Council (2010). *Biometric Recognition: Challenges and Opportunities*. The National Academies Press. https://doi.org/10.17226/12720

Nigam, I., Vatsa, M., Singh, R. (2015). Ocular biometrics: A survey of modalities and fusion approaches. *Information Fusion*, *26*, 1–35. https://doi.org/10.1016/j.inffus.2015.03.005

Papernot, N., McDaniel, P., Sinha, A., & Wellman, M. P. (2018). SoK: Security and Privacy in Machine Learning. *2018 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 399-414). Institute of Electrical and Electronics Engineers.

Riggan, B. S., Short, N. J., & Hu, S. (2018). Thermal to Visible Synthesis of Face Images using Multiple Regions. arXiv:1803.07599 [cs.CV].

Ross, A. A., Nandakumar, K., & Jain, A. K. (2006). *Handbook of Multibiometrics*. Springer.

Saini, M. & Kapoor, A. K. (2016). Biometrics in Forensic Identification: Applications and Challenges. *Journal of Forensic Medicine*, *1*(2), 1-6. https://doi.org/10.4172/2472-1026.1000108

Sarangi, P. P., Mishra, B. S. P., & Dehuri, S. (2018). Fusion of PHOG and LDP local descriptors for kernel-based ear biometric recognition. *Multimedia Tools and Applications*, *78*, 9595-9623. https://doi.org/10.1007/s11042-018-6489-0

Sharp, L. (2000). The Commodification of the Body and Its Parts. *Annual Review of Anthropology*, *29*, 287-328.

Singh, S., & Prasad, S.V.A.V. (2018). Techniques and Challenges of Face Recognition: A Critical Review. *Procedia Computer Science*, *143*, 536-543.

Sulner, S. (2018). Critical Issues Affecting the Reliability and Admissibility of Handwriting Identification Opinion Evidence. *Seton Hall Law Review*, *48*(3), 631-717.

Sutrop, M. (2010). Ethical Issues in Governing Biometric Technologies. In *Proceedings of the Third International Conference on Ethics and Policy of Biometrics and International Data Sharing, ICEB'10* (pp. 102-114). Springer. https://doi.org/10.1007/978-3-642-12595-9_14

TELEFI (2021). *Summary Report of the project "Towards the European Level Exchange of Facial Images"*. https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf

Thompson, E. (2018). Understanding the Strengths and Weaknesses of Biometrics. *Infosecurity Magazine*. Available at https://www.infosecurity-magazine.com:443/opinions/strengths-weaknesses-biometrics/ .

Tistarelli, M., Grosso, E., & Meuwly, D. (2014). Biometrics in forensic science: Challenges, lessons and new technologies. In V. Cantoni, D. Dimov, & M. Tistarelli (Eds.), *Proceedings of the First International Workshop on Biometric Authentication (BIOMET 2014), Sofia, Bulgaria, June 23-24* (pp. 153-164). Springer. https://doi.org/10.1007/978-3-319-13386-7_12

Tome, P., Vera-Rodriguez, R., Fierrez, J., & Ortega-Garcia, J. (2015). Facial soft biometric features for forensic face recognition. *Forensic Science International*, *257*, 271–284. https://doi.org/10.1016/j.forsciint.2015.09.002

Tomova, S. (2009). Ethical and Legal Aspects of Biometrics. In E. Mordini, & M. Green (Eds.), *Identity, Security and Democracy: The Wider Social and Ethical Implications of Automated Systems for Human Identification* (pp. 111-114). IOS Press.

Wevers, R. (2018). Unmasking Biometrics' Biases: Facing Gender, Race, Class and Ability in Biometric Data Collection. *TMG Journal for Media History*, *21*(2), 89-105.

Working Group for Human Factors in Handwriting Examination (2020). *Forensic Handwriting Examination and Human Factors: Improving the Practice Through a Systems Approach*. U.S. Department of Commerce, National Institute of Standards and Technology. NISTIR 8282.

Završnik, A. (2020). Criminal justice, artificial intelligence systems, and human rights. *ERA Forum*, *20*, 567-583.

Zeinstra, C. G., Meuwly, D., Ruifrok, A. C. C., Veldhuis, R. N. J., & Spreeuwers, L. J. (2018). Forensic face recognition as a means to determine strength of evidence: a survey. *Forensic Science Review*, *30*(1), 21-32.

Zhou, S., & Xiao, S. (2018). 3D face recognition: a survey. *Human-centric Computing and Information Sciences*, *8*, 1-27. https://doi.org/10.1186/s13673-018-0157-2