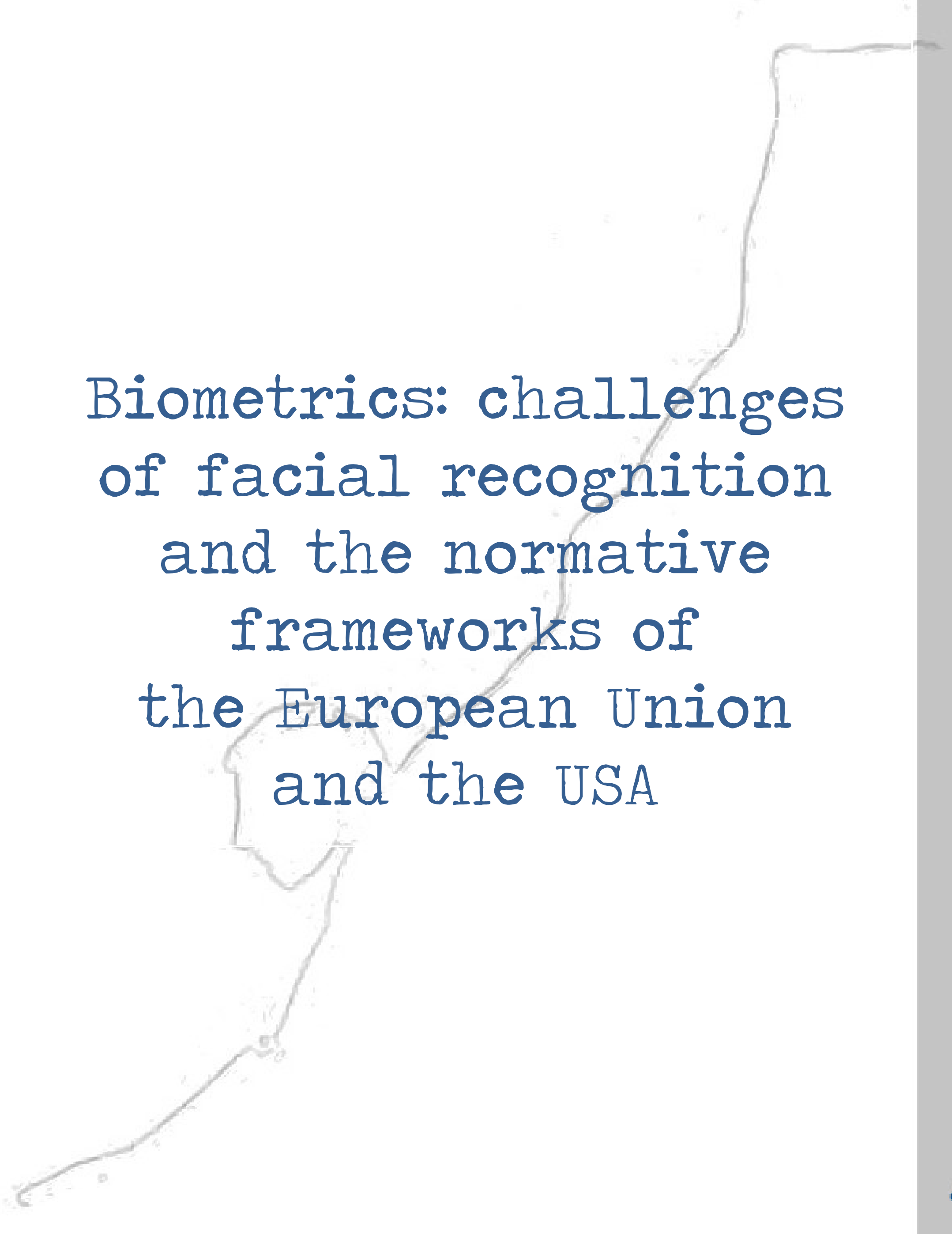
PAPER N. 30

a.a. 2018/2019

Trento BioLaw Selected Student Papers



Biometrics: challenges of facial recognition and the normative frameworks of the European Union and the USA

Chiara O'Connor

Jean Monnet European Centre University of Trento

Co-funded by the Erasmus+ Programme of the European Union

Università di Trento Facoltà di Giurisprudenza

I paper sono stati selezionati a conclusione del corso *BioLaw: Teaching European Law and Life Sciences (BioTell)* a.a. 2018-2019, organizzato all'interno del Modulo Jean Monnet “BioLaw: Teaching European Law and Life Sciences (BioTell)”, coordinato presso l'Università di Trento dai docenti Carlo Casonato e Simone Penasa.

Biometricis: challenges of facial recognition
and the normative frameworks of the European Union and the USA

*Chiara O'Connor**

ABSTRACT: The following paper aims at illustrating the issues related to the present and future use of facial recognition systems for purposes of security and police cooperation. After a general overview on the adoption of such systems and their positive and negative impacts, importance will be given to the legal framework of Europe and the USA as well as to possible legislation to be adopted taking into account both the fundamental right to protection of one's privacy and the purposes of crime prevention and security.

KEYWORDS: Biometrics; facial recognition; crime-prevention; protection of privacy; development

1. Facial recognition technology

In recent years, many steps have been made towards the adoption of Artificial Intelligence technologies to assist or even replace human beings in an ever-growing variety of fields. One of these novelties is the development of facial recognition software.

Nowadays, almost everyone is familiar with facial recognition systems as they might even be installed on our smartphones, or for their use on social media. So far, this innovation has reached a much wider breadth than one might expect, mainly in the field of police cooperation and crime prevention. However, before entering into detail, there is a difference that needs to be drawn when talking about facial recognition between what is mere biometric identification and authentication. The first one is a system recognizing "one to one" data whereas the second one makes a "one to many" comparison[1]. As a matter of fact, facial identification systems allow to capture faces of individuals, whereas facial recognition goes a step further by authenticating the face identified and by matching it to a photo of a specific person contained in a database. It is as simple as it seems, in fact, the system picks out one or different faces and rapidly measures each one's facial features, using algorithms to encode the data in so-called faceprints or templates. The faceprints are then compared with a database entailing a variety of pictures and checks whether it matches with someone's identity.

The birth of the idea of facial recognition can be traced back to the 60s when Bledsoe invented a mechanism to classify photos by hand through a tablet recognizing traits and biometric lines of people by coordinating

* *Student at the University of Trento, Faculty of Law.*

[1] R.E. NICHOLS, *Biometrics: Theory, Applications, and Issues*, New York, 2011, 123.

the location of facial features. Gradually, hand in hand with technological developments, this discipline started to get more of an up-to-date aspect. The first innovation in this sense was brought by The Defense Advanced Research Projects Agency (DARPA) and the National Institute of Standards and Technology which gave birth to the Face Recognition Technology (FERET) program beginning in the 1990s in order to encourage the commercial face recognition market. They came up with the creation of a database of facial images, updated in 2003 to provide high-resolution colour versions of images. From this point on, it was left to technological development to set the field for higher sophisticated mechanisms[2]. The latest developments of such systems have been exposed to many critiques asserting that the database they use are too wide and that most of them have a very low level of accuracy, and this proves to be essential when dealing with recognition of criminals.

2. Uses of facial recognition systems

Despite the sceptical views of data protection experts, legal advisors and scholars on the usage of facial recognition systems in criminal matters, it is correct to start by pointing out the numerous advantages of this innovation. Indeed, technological development is not thought to be harmful per se, but it is usually its side effects that prove controversial, and what they actually aim at bringing about is progress. The system is utilized to assist security, intelligence and law enforcement personnel in the performance of their duties when, for instance, biometric data are combined with the issuing of identity documents, like fingerprints, but also face match is starting to be used at border checks and airports to compare the portrait on the passport or ID with the holder's face[3]. Face recognition is also commonly utilized for biometric surveillance. Banks, shops, stadiums, airports and other public places use facial recognition to reduce crime and prevent violence. As a matter of fact, this technology allows recognition and identification of criminals in action or people with criminal records entering certain monitored areas.

Use of face recognition is, nevertheless, not limited to security scopes and crime-prevention goals but it is also employed in smartphones to unlock them, or on social media where for example Facebook allows you to track any uploaded contents where a photo of you is present. What is more, this innovation also helped in the identification of old photographs, as well as possibly diagnosing specific rare genetic diseases through facial feature recognition[4]. A further example of an advantageous use of facial recognition systems is that of detecting and recognizing people missing or having fled. As the South China newspaper reported in April

[2] https://www.facefirst.com/blog/brief-history-of-face-recognition-software/.

[3] A.L. Rukhin, *The Recognition Problem of Biometrics*, 2004.

[4] S. Mohapatra, Use of Facial Recognition Technology for Medical Purposes: Balancing Privacy with Innovation, 2016 Pepperdine University School of Law, Pepperdine Law Review.

2018, the police department of Chongqing managed to trace back a mentally ill man's origins after he got lost and wandered around the railway station there thank to a facial recognition system. Since he could not remember where he came from, the authorities could bring him home after missing for a year[5].

As already stated above, many of these systems are blamed for lacking in accuracy and for presenting biased outcomes, thus generating discrimination. But where do these critiques stem from? A compelling example of discrimination when dealing with such software is the one adopted by NIST and the FBI based on tattoo recognition. This practice allowed for the collection of pictures of different kinds of tattoos to be inserted into a database and grouped according to the idea that «visible similarities also lead to invisible similarities between the subjects having them»[6], in this case people with similar tattoos. The racial thought behind this is almost the same as the one applied to racism based on the skin colour for example, when it leads a person to think that all people with the same kind of skin tone are also associated to the same inclination to commit crimes or whatever, although there is of course no genetic basis to prove this. What is more, many software designed to carry out a facial recognition function proved to be biased and less accurate when dealing with the picture of black-skinned people or women. The reason for this is a mere technical lack of accuracy which might stem from a biased software developer, but there is also no solution to this because there are no tests to evaluate whether a software is biased, supposedly because no one wants to carry out one[7]. More specifically, a test done by "MegaFace Challenge", a project of the University of Washington on algorithms on a million persons' scale, found that most of facial recognition systems dealing with such a large dataset have levels of accuracy lower than expected. As a matter of fact, only two systems achieved circa 75% of accuracy, whereas the rest only scored 33% in the test[8]. Another example of a facial recognition system is Amazon's "Rekognition" which was accused of racial and gender bias, and of being too dangerous because it has access to too wide a number of photos. The company responded by saying the study proving inaccuracies in their system was misleading.

By researching on this topic, it becomes clear that the prevailing opinion claims there is a strong need for stricter legislation setting limits to the use of facial recognition mainly in its employment in criminal matters, but not necessarily with a view to criticize such practice but rather to ensure a secure and fully legal development of it. Different systems across the world have adopted different kinds of norms. The rationale behind the adoption or not of such rules depends mainly on the different ways of protecting fundamental rights. As a matter of fact, the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and directives aimed at data protection were adopted at European Union

[5] https://www.scmp.com/news/china/society/article/2142119/mentally-ill-chinese-man-lost-year-reunited-family-thanks-facial.

[6] F. Bacchini, L. Lorusso, *Biometrica, discriminazioni e stile di pensiero razzista,* in M. Mori, *Bioetica rivista interdisciplinare*, XXV, 2-3, 2017, 259.

[7] F. Bacchini, L. Lorusso, *Biometrica, discriminazioni e stile di pensiero razzista*, cit., 251-270.

[8] https://www.dailymail.co.uk/sciencetech/article-3658797/Facial-recognition-ISN-T-reliable-Massive-test-using-million-faces-finds-controversial-technology-not-accurate-claimed.html.

level whereas in the rest of the world this practice is addressed in a different way, depending on the type of government, culture and history. A striking example is that of India, where in 2009 the government introduced a biometric identification system, the Aadhaar-a national scheme, issuing every citizen a unique identification number while storing their personal biometric data. The latter was challenged by the Indian supreme court in 2017[9] which established that the right to privacy constitutes a fundamental right, thus in need of protection by the government. Yet, it did not declare the system in violation of the Indian Constitution because of its mandatory linking with all government welfare schemes and services[10]. It would be interesting to see how the same constitutionality question would be decided in Europe or in the USA. To this end, a closer look to the supranational and national pieces of legislation is worth it.

3. The legal framework of the European Union

Generally speaking, face biometrics employed in police checks is quite widespread and also rigorously controlled in Europe. For instance, the man responsible for the Brussels terror attacks of 2016 was identified thanks to FBI facial recognition software. The South Wales Police also implemented it at the UEFA Champions League Final in 2017. The question, however, how usage of this technology is regulated is also relevant. At European Union level, the latest enactment regarding facial recognition is the text spelling out the conclusions on the Coordinated Plan on the development and use of Artificial Intelligence Made in Europe. Here, the Permanent Representatives Committee remarks the goals to be reached by the Union in the development of artificial intelligence and among these, reference is made to the need «for ensuring accountability and the protection of fundamental rights», and it also foresees reviewing of legislation in line with the principles of Better Regulation in order for it to be in line with new opportunities and challenges raised by Artificial Intelligence including safety, privacy and liability and fully automated decisions and actions, thus it is implicitly addressing facial recognition technology too[11]. As regards more specific legislative acts regulating the use of facial recognition systems, Regulation 2016/679 (GDPR) on the processing of personal data and its free movement, only mentions biometric data in general. Article 9 classifies it as sensitive data whose processing is allowed only with explicit consent of the individual except where Union or Member State law maintain that such prohibition «may not be lifted by the data subject or insofar as

[9] Puttaswamy I, Writ Petition (Civil) No. 494 of 2012 1, 262–63 (Sup. Ct. India Aug. 24, 2017).

[10] M.J. Levine, *Biometric Identification in India Versus the Right to Privacy: Core Constitutional Features, Defining Citizens' Interests, and the Implications of Biometric Identification in the United States*, University of Miami School of Law Institutional Repository, 2019.

[11] *Conclusions on the Coordinated Plan on the development and use of Artificial Intelligence Made in Europe*, 6177/19, Brussels, 11 February 2019.

processing of such data is necessary for reasons of substantial public interest»[12]. Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 deals in detail with 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. The decision to issue a directive rather than a regulation is a consequence of what was stated in declaration number 21 «on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation» annexed to the treaty of Lisbon, which states that legislation in this area may prove necessary because of the specific nature of these fields[13]. This is also stated in whereas (14) of the directive, holding that «since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) should not be considered to be activities falling within the scope of this Directive». Since the main use of facial recognition software is in the criminal field, states are not as limited in their action as when processing personal data in accordance with the GDPR, because the Directive leaves Member States freedom of choice in the way to apply the standards provided by the latter and they are also allowed to adopt more restrictive measures. The Directive is based on Article 16 TFEU, which recalls the content of Article 8 of the Charter of Fundamental Rights of the EU, core provision aimed at the protection of personal data, and it serves also as legal basis for the European Parliament and Council to legislate in this field when acting under the regime of Union law. The Directive specifically refers to "biometric data" in whereas (51) and in article 10, where it is referred to as a special category of personal data and whose processing requires more attention as it «shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only: where authorised by Union or Member State law; to protect the vital interests of the data subject or of another natural person; or where such processing relates to data which are manifestly made public by the data subject».

As remarked by the former president of the Italian authority for data protection, the practice of facial recognition in criminal instances is not specifically regulated by a European regulation but by the aforementioned directive. The latter has been transposed in the Italian system by a law *Decreto legislativo*

[12] 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).

[13] Declarations annexed to the final act of the intergovernmental conference which adopted the treaty of Lisbon, signed on 13 December 2007, declaration number 21.

del 18 maggio 2016 n. 51[14] which foresees that processing of biometric data for criminal and judicial purposes can occur even without consent of the data-subject. Article 3 of the act sets out the principles to be applied in the processing of such data. Article 7, instead transposes the content of Article 9 of the GDPR, namely the treatment of sensitive data including biometric data, which shall only occur where strictly necessary and granting protection of the fundamental rights and freedoms of the individual and where foreseen by Union or state law able to guarantee fundamental rights protection, and only where the processing is apt to protect a vital interest of the data-subject or of another person or if it deals with data made available by the subject. Moreover, article 24 specifically mentions biometric data as a special category of data whose processing shall only take place after having consulted the national authority for data protection[15].

So far, the use of facial recognition systems in Italy seems to have been quite limited. However, also Italy avails of a software capable of recognizing individuals through algorithms, i.e. facial recognition and it is called SARI, *Sistema Automatico di Riconoscimento Immagini* which matches biometric data with pictures of the A.F.I.S. database, "Automated Fingerprint Identification System", containing not only fingerprints but also pictures of almost 16 million profiles, as communicated by the Italian police. SARI can work in two ways: "enterprise", namely comparing the detected image with those stored in the AFIS database, or "real time", by monitoring a certain area and searching for matches of peoples' faces on a watch list. This system was employed in the identification of two burglars who broke into a flat in Brescia[16]; its database was in possess of their biometric features because they had been previously recorded by the police. Yet the usage of SARI is not left uncriticized: a question on its legitimacy has been posed and is currently being evaluated by the ministry of the interior[17].

In Germany, instead, the "Anwaltsverein", the German lawyers' union, made it clear several times that the lack of a legal basis to allow facial recognition projects, such as those carried out in Berlin-Südkreuz and in Hamburg, should as soon as possible be brought to the attention of the legislator, since the control and recognition of biometric data of citizens in public places is a clear violation of fundamental rights as enshrined in the German constitution. The outcome of the experiment carried out in Berlin didn't prove as successful as expected, since according to the ministry of the interior 30% of the faces were erroneously recognized and 1% mistakenly identified. What is more, the ministry did not give many explanations about the project. Data

[14] Decreto legislativo 18 maggio 2018, n. 51, *Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.*

[15] https://www.cyberlaws.it/en/2019/riconoscimento-facciale-privacy-garante/.

[16]https://www.repubblica.it/cronaca/2018/09/07/news/come_funziona_sari_il_sistema_di_riconoscimento_facciale_usato_dalla_polizia_scientifica-205804445/?awc=15069_1556628886_16fe628a51d995a668029245e55528bb&source=AWI_DISPLAY.

[17] Atto Camera: Interrogazione a risposta scritta 4-01149 presentato da D'INCÀ Federico testo di Mercoledì 19 settembre 2018, seduta n. 47.

protection advisors across Germany warned citizens to look at the application of new technologies not in an isolated way, but in combination with the new police acts which are being issued in the Länder and the overreaching competences they are given as well as with the new passport and ID regulations. The consequences these kinds of regulations bring with them are mainly in the field of crime prosecution: the police are allowed to control a person's activities in the planning of crime commission, issue exclusion orders, or a ban on contact, or upholding suspects for prevention even without specific evidence to prove their intention to do so[18].

Another interesting example is that of France, where privacy protection was set aside in the aftermath of the terrorist attacks of November 2015, when a series of stricter laws for security were implemented. One example is TES (titres électroniques sécurisés), a system collecting biometric data of all passports and now even IDs of French citizens, introduced through a decree of October 2016. Yet this system is only accessible by police authorities and Interpol and it allows authentication only of those subjects whose information has been inserted in the database. Since 2016 the system has been implemented in the whole French and overseas territories notwithstanding the fact that its adoption was even brought before the *Conseil d'Etat* because assumed in breach of the Charter of Fundamental rights[19]. The Conseil, however, rejected the request to revise the decree establishing the Titres Electroniques Sécurisés because it held that the collection, storing and processing of such data is carried out with sufficient precaution and is subject to adequate restrictions. Essentially, the Conseil asserted, the system does not disproportionally infringe privacy rights as it serves the purpose for which it was established, namely that of protecting public order[20].

In conclusion, what emerges from this analysis, is that in the utilization of facial recognition technologies the importance of the protection of fundamental rights is stressed both in the national constitutions and in the aforementioned instruments of the EU. As will be examined later, the United States, instead, tends more toward the strengthening of public security and is lacking in the protection of privacy and liberty which the EU tries to afford. Whether that protection is eventually afforded in Europe or not, is still an open question, and in fact an evaluation of these rules proves hard to carry out. A reason why such systems have not brought any substantial problems yet, may be that it is still a technology under development and at the same time not everyone is probably aware of it or at least of the dangers it entails. Still, what is certain, is that a legal basis providing stricter and clearer rules for disciplining the development and future utilization of such systems needs to be established as soon as possible, because transparency plays a pivotal role in democratic societies.

[18] https://www.datenschutzbeauftragter-info.de/du-kommst-hier-nicht-rein-gesichtserkennung-im-fussball-stadion-rechtswidrig/.

[19] L. SCAFFARDI, *Giustizia, Genetica e tutela della persona. Uno studio comparato sull'uso (e abuso) delle Banche Dati del DNA a fini giudiziari*, San Giuliano Milanese (MI), 2017, 133-135.

[20] https://www.lemonde.fr/pixels/article/2018/10/18/vie-privee-le-conseil-d-etat-valide-le-fichier-rassemblant-les-informations-de-60-millions-de-francais_5371436_4408996.html.

4. The law in the USA

Regulations on data protection in the USA were first introduced by the work of the Federal Trade Commission in 1914, which aimed at protecting privacy in a consumer context. But no independent instrument overseeing data protection has ever been adopted in the USA such as the GDPR for the EU. Nevertheless, data protection is afforded in the United States by the fourth amendment of the US constitution which prohibits «unreasonable searches and seizures» by the government. Reasonableness is established if the search is carried out pursuant to a valid warrant showing a probable cause and on a particular description of the property to be searched and the items to be seized, or if established by a court. If violated, the remedy afforded for a violation of the amendment is either the suppression of evidence or suing the government official for civil remedies[21]. The practice of facial recognition in the United States is as little protected by law as in the rest of the world. As reported by to the non-profit Project on Government Oversight, neither Congress nor states within the USA have put any limits to the use of facial recognition, except for Oregon[22]. Also, the county and city of San Francisco has just proposed the adoption of an Ordinance amending the Administrative Code on Surveillance Technology, also called "Stop Secret Surveillance Ordennance" which is meant to ban the use of facial recognition by governmental and federal authorities against citizens[23].

According to a report by the Centre on Privacy and Technology of the Georgetown University a lot of police- and other agencies are implementing facial recognition technologies without worrying for the lawfulness of it. But it's clear they don't, since any legal framework is missing. The American idea seems to be based on the terror of delinquency, thus it is as if any mechanism adopted to reinforce public security were justified for the sake of it. This feeling arose particularly after the attacks of 9/11, when the government started thinking of stricter measures to combat international terrorism, comprising facial recognition systems. As a consequence, most developers and supporters of facial recognition systems do not even pose the question of their lawfulness since they believe that in the trade-off between privacy and security, gains from security are far more than the losses in privacy and liberty where for instance a mistaken arrest is an equitable trade-

[21] F. Bignami, Directorate general for internal policies policy department c: citizens' rights and constitutional affairs civil liberties, justice and home affairs, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens,* Study of the LIBE committee, Brussels, 2015.

[22] https://www.theregister.co.uk/2018/12/07/microsoft_facial_recognition/.

[23] *Ordinance amending the Administrative Code to require that City departments acquiring Surveillance Technology submit a Board of Supervisors approved Surveillance Technology Policy Ordinance and a Surveillance Impact Report to the Board in connection with any request to appropriate funds for the purchase of such technology or to accept and expend grant funds for such purpose, or otherwise to procure Surveillance Technology equipment or services; require each City department that owns and operates existing surveillance technology equipment or services to submit to the Board a proposed Surveillance Technology Policy Ordinance governing the use of the surveillance technology; and requiring the Controller, as City Services Auditor, to audit annually the use of surveillance technology equipment or services and the conformity of such use with an approved Surveillance Technology Policy Ordinance and provide an audit report to the Board of Supervisors*, introduced 01/29/2019.

off for the chance of arresting a criminal who might still be free[24]. Only four of the fifty-two agencies observed, bothered to adopt a public policy for regulating this practice, since this is not mandatory. Many of them even increase the risk of non-controllability of such data by giving access to their database to other agencies. What is more, the report also states that very little agencies consider the reliability of such systems when adopting them, and even less have a clue about what kind of traineeship is needed to manage such systems. Researchers fear a quick and uncontrollable spread of this practice among the States, and it is mainly agencies which make the most indiscriminate use of them[25]. Not long ago, Microsoft's president Bradford L. Smith called for attention on the regulation of employment of facial recognition systems which he feels is a dangerously lacking element. As he stated, whereas medical technology is highly regulated, adoption of facial recognition systems enjoys too much freedom.[26] In his opinion, these systems too often lead to errors and discrimination, and they can intrude on people's privacy, as well as undermine democratic freedoms. Nonetheless, he is not denouncing the practice of facial recognition as such, but pushing for a more controlled and accurate use of it. Microsoft suggest a two-fold approach to legislating in this area, aimed at ensuring both transparency and enabling third-party testing and comparisons, and also to protect consumers and citizens. To this purpose, he announced the principles which will mark facial recognition systems developed by Microsoft, namely: fairness, transparency, accountability, non-discrimination, notice and consent, and lawful surveillance[27].

5. International law

Since no case of violation of privacy through usage of facial recognition systems has ever been brought before national nor international tribunals, the question arises whether such litigation could be solved following precedents dealing with violation of other personal data, as for instance retention of finger prints by the police. One example is that of *S. and Marper v UK*, a prominent judgement of the European Court of Human Rights. In this case, the two plaintiffs were both UK citizens and had been accused and then acquitted of two different crimes. Both applicants asked the police to destroy their fingerprints and DNA samples, but unsuccessfully. The applicants applied for judicial review of the police decisions and the administrative court first, and the court of appeal in a second stage, which rejected their application maintaining that DNA profiles and fingerprints do not entail such a dangerously great amount of data and the retention of such data produced more benefits than negative effects, hence embracing a utilitarian logic. The European Court of Human Rights, analysed the case in light of the positions of the parties: first, it dealt with the relevant laws,

[24] P. BREY, *Ethical aspects of facial recognition systems in public places*, in *Journal of Information, Communication and Ethics in Society*, 2, 2 2004, 97-103. Permanent link to this document: https://doi.org/10.1108/14779960480000246.

[25] F. BACCHINI, L. LORUSSO, *Biometrica, discriminazioni e stile di pensiero razzista*, cit., 247.

[26] https://www.gemalto.com/govt/biometrics/facial-recognition.

[27] https://www.theregister.co.uk/2018/12/07/microsoft_facial_recognition/.

then it went on to assess whether the interference with the samples is to be considered «necessary in a democratic society» (still leaving some margin of appreciation to the member state in this). In its final judgement the Court found that the retention of the data did serve a legitimate aim, but it stated that member states must afford appropriate safeguards in processing such data as according to Article 8 of the European Convention on Human Rights which is to be regarded especially when the data is being automatically processed. Furthermore, it suggests that the domestic law must also guarantee that retained personal data is efficiently protected from misuse and abuse. The Court observes that the protection afforded by Article 8 of the Convention would be deeply weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. The Court further held that the mere retention and storing of personal data by public authorities, however obtained, do have a direct impact on the private-life interest of an individual, irrespective of whether subsequent use is made of the data. And that to a major extent when dealing with biometric or genetic data of juveniles, since they shall be protected from any future negative effects resulting from the retention of such data. This led the Court to state that there had been a violation of Article 8 of the Convention[28]. The Judgement has gained much visibility and accordingly many comments were published. One of the major points which have been discussed is the proper scope of the usage of such databases, namely whether they shall be used only to prosecute violent and dangerous offenders, so using only “arrestee” databases or more generally anyone and expanding the database to a “universal” one. Many scholars, in fact focus their discussion on this and, as opposed to European and American courts, they are convinced that retention of genetic data is only acceptable when dealing with convicted and not merely arrested people thus rejecting the idea of a universal database, whereas others believe that having such a wide database could set aside discrimination and put everyone on the same level. In the case of *S. and Marper v UK* the Court did not fully face the problem since it held that widespread universal databases would be too costly and thus not possible to accomplish. Moreover, what the ECtHR achieved was a new path in assessing privacy violation since it did not only put a limit to the expansion of databases but it marked the correlation between identity and identification which cannot be seen as independent practices for the powerfulness of data they entail. Leaving the privacy debate aside, the court underlined the importance of a legal confrontation about the neutrality of fingerprints which it considers not given, because fingerprints contain unique information. This theory was nonetheless confuted

[28] Case of *S. and Marper v. the United Kingdom* (applications nos. 30562/04 and 30566/04) Strasbourg, 4 December 2008.

by scholars because genetic data can only be read insofar as it is confronted with other individuals' data[29]. In another writing, a further argument of the ECtHR is quoted, namely that the purpose of preventing crime had such a general character that it could result in too extensive interpretation. Moreover, it is worth noting that only the forty-seven member states to the Council of Europe are bound by the decision, whereas the practice of DNA collection in the rest of the world is freer, as mentioned above, in the USA for which security beats privacy and liberty[30].

Another similar case is that of *Murphy v UK* now pending before the ECtHR, where the questions posed are based on the previous decision of *S. and Marper v UK*. Other ECHR case-law regarding retention of fingerprints, cellular samples and/or DNA by authorities[31] are for instance that of *Peruzzo and Martens v Germany*, where the Court confirmed that the collection and retention of DNA interfered with the right to respect for private life guaranteed by Article 8, but it held that this interference had been necessary in a democratic society and underlined the wide margin of appreciation of the national authorities in their assessment. The safeguards provided for by the law in question were considered as appropriate since only DNA material from frequent criminal offenders or from individuals suspected of serious crimes were retained. Furthermore, taking into account that the retained DNA profiles could only be disclosed to the relevant authorities for security purposes the Court rejected the complaint.

In the light of these and other cases it seems that the Court adopted a number of security-oriented decisions, rather than giving more importance to the protection of privacy and individual freedom, in the sense that all violations of article 8 ECHR were considered inadmissible as long as the data retained was that of criminals. The only cases in which a violation was found, were those in which the data belonged to persons who had been acquitted, thus not explicitly representing a threat for national security. If the same reasoning were applied to practices of facial recognition, the outcome would be that most database should be destroyed or not even utilized, since they entail thousands and thousands of pictures of innocent people. In order not to infringe article 8 ECHR, the database should only contain pictures of suspects whose freedom threatens public security. Some may argue, this idea could go against the aim of facial recognition as such, because, in the instance that someone who has never been recorded commits a crime it would prove almost impossible to find out any information about him/her, which would be possible instead, if facial recognition systems databases were richer. Accordingly, it is clear that the balance to be struck between privacy and security rights turns out to be fairly complicated, and this expounds why legislators find it hard to come up with a clear norm.

[29] S.A. Cole, *De-neutralizing identification: S. & Marper v United Kingdom, Biometric databases, Uniqueness, Privacy and Human Rights* in J. Caplan, E. Higgs, *Identification and Registration Practices in Transnational Perspective People, Papers and Practices*, Hampshire, 2013, 77-91.

[30] G.J. Annas, J.D., M.P.H., *Protecting privacy and the public – Limits on Police Use of Bioidentifiers in Europe* in *Health Law, Ethics, and Human Rights,* in *The new England journal of medicine*, 361, 2, July 9, 2009.

[31] Research Report: Bioethics and the case-law of the Court, Council of Europe/European Court of Human Rights, 2016.

6. Facial recognition: a guarantee for security or a violation of privacy? Possible legislative solutions

At present, it is probably too early to assess whether the adoption of facial recognition systems in practice fulfils the purpose of crime prevention. Interestingly enough, facial and fingerprint recognition systems were still a "future prospect" of crime prevention in 2007, considered among other technological developments which could only be satisfactory if sufficiently accurate. Yet it is important to keep in mind three main factors for future developments namely «things that will change, things that will change only very slowly and those which are within our gift to change or maintain». These three categories refer to technology, human nature and organizational and governmental aspects, and since we can only exercise control over technology and governmental decisions, these are the two aspects to work on[32].

First of all, to serve the goal of crime prevention, what governments are required to do is investing in durable and reliable systems which suitably reduce crime commission rates. Consequently, there are many and different ways to prevent crime and they differ from state to state, if one looks for instance at the crime rate of Japan, it emerges that is the lowest among industrialized societies, but at what cost? Should citizens have to live under constant pressure in order to ensure public safety? The same happens in Singapore where the high level of public security is afforded thank to very intrusive governmental means[33]. But when progress in technology occurs faster than ever, the government shall intervene in the regulation of its development and usage, since we might be headed towards a realisation of George Orwell's *1984* idea of the government as a totalitarian regime monitoring every aspect of our lives, or comparing police to a "big brother". The novel itself was actually meant as an exaggeration to warn people of such danger, because the danger is undoubtedly there as soon as our privacy is somehow interfered with. In effect, the danger is there, and technological development cannot be stopped but one can attempt to control it, hence the way in which we look at facial recognition systems has to be relativized to its possible infringements of fundamental rights and principles. As a consequence, it is fair to ask whether nowadays surveillance by the government and police authorities is too widespread or still acceptable, and also how far this might go in the future. At the same time, since any democratic state builds upon the rule of law, one might argue that development and usage of systems without a clear legal basis and any regulations might even prove unconstitutional as infringing the principle of legality requiring transparency and primacy of the law, so if no further step is taken in terms of regulations, the consequences might be very serious. As a matter of fact, and this is true for the whole world of artificial intelligence, either will these new technologies have to be subject to old rules by extension of

[32] S. Palidda, *Politiche della paura e dell'agire pubblico*, in A. Dal Lago, *Un mondo di controlli,* in *Conflitti globali 5*, Truccazzano (MI) 2007, 198-200.

[33] H. Shaftoe, *Crime prevention facts, fallacies and the future*, New York, 2004, 124.

their scope, or special legislation will have to be enacted. Considering the different standing points of Europe and the United States mentioned above, one could accordingly envisage distinct concrete legislative proposals to regulate the utilization of FRT (which stands for facial recognition technology).

In the United states, this longing for more security is characterized by a tendency to delegate more power to governmental authorities, since the majority of the population believes they will be afforded public safety in exchange for their private data[34]. But, authorities in the US favouring usage of FRT pretend not to see it as an infringement of privacy rights and assert that once you are in a public place, you willingly give up on some privacy and one cannot expect it to be protected. Yet privacy is a fundamental right, and this is exactly what should be stressed in US legislation: there is need for a law to discipline the employment of facial recognition systems which threaten to limit people's freedom and privacy[35]. And this shall apply not only to its usage by police authorities, but also the private collection of data which tends to supersede the contents of data at public disposal and that hardly responds to any legal requirements[36]. To this end, it is necessary to offset the limitation of freedom and privacy with the degree of security granted by government by, for example, allowing facial recognition only under strict circumstances, hence in presence of a grave offence and also to establish a system of notice when data is collected about one person, that is, to let the person under arrest know that his/her biometric data is being processed and that it will be stored until proved innocent. What is more, the problem of function creep shall also be addressed, namely the risk that the data stored is not only used for one specific scope but that it is passed to other systems[37].

To overcome the current legal status quo in Europe, instead, a way to improve the situation could be that of adopting scope-oriented facial recognition, with clear-cut rules about it. EU regulation for biometric facial identification of passport holders, for example could be seen as a scope-oriented norm[38]. Article 1 of the said regulation states: «Passports and travel documents shall include a storage medium which shall contain a facial image. Member States shall also include fingerprints in interoperable formats». This aspect, however, is analysed in an opinion issued by the EU Commission, holding that the aforementioned goal might be too far reaching, since usually the retention of such data shall be limited to criminal scopes[39]. As a matter of fact, what is needed at European level are clearer rules balancing the right to security and freedom. This could occur through the introduction of legislation defining which types of serious crimes justify resorting to the utilization of facial recognition, the agencies allowed to use them and foreseeing a system of notice to inform

[34] S. Palidda, *Politiche della paura e dell'agire pubblico*, cit., 13-23.

[35] P. Brey, *Ethical aspects of facial recognition systems in public places,* cit.

[36] Presidenza del Consiglio dei Ministri, Comitato nazionale per la bioetica, *L'identificazione del corpo umano: profili bioetici della biometria,* 26 Novembre 2010. http://bioetica.governo.it/media/1846/p95_2010_identificazione-corpo-umano-biometria_it.pdf.

[37] *Ibid.*

[38] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

[39] Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

citizens of when their biometric data is being collected, to limit images in the database, foresee elimination of the non-matched images, and finally to limit its usage to highly exposed public places.

In January 2020, the European Commission issued a draft white paper on Artificial Intelligence. The aim of the latter was that of promoting new EU-approaches to deal with problems posed by artificial intelligence and in its option 2 it envisaged sectorial requirements for public administration and facial recognition, and one of the measures adopted would be that of completely banning facial recognition systems employed by private or public actors in public places. This idea stems from the right in the GDPR «not to be subject of a decision based solely on automated processing, including profiling». The measure would have lasted from three to five years, time in which the Community shall have identified a methodology for assessing the impacts of this technology and possible risk management measures[40]. Nonetheless, in the latest update of the draft white paper on Artificial Intelligence[41], the Union backed off from this initiative in favour of establishing 'clear criteria' in future mass-scale deployment of biometric identification systems in the EU.

Certainly, the introduction of an independent supervisory body responsible for controlling the lawful utilization of biometric data retrieval would be an important step forward, both in the USA and in Europe, in guaranteeing a limit to abuse of facial recognition systems. Ideally, this body would have the power to address complaints from the public and work also as a committee for advising the legislator in the adoption of ad-hoc rules.

[40] https://www.euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf (last consultation: 14.02.2020).

[41] https://www.biometricupdate.com/202001/eu-no-longer-considering-facial-recognition-ban-in-public-spaces (last consultation 14/02/2020).