Global Campus
South East Europe

Policy Briefs
2020

Desara Dushi

The use of facial recognition technology in EU law enforcement: Fundamental rights implications

Supported by

Table Of Contents

The use of facial recognition technology in EU law enforcement: Fundamental rights implications

Desara Dushi

EXECUTIVE SUMMARY

Facial recognition technology is a type of biometric application used to identify people's faces based on datasets and then makes assessments about those people based on algorithmic predictions.[1] This technology can be used for three types of analytics: verification (matching the ID photo in airports), identification (matching a photo in a database) and classification (gender, age, etc).[2] This technology is widely used by private companies for advertisement and marketing, by analysing facial expressions of clients to predict their preferences; for identifying ideal job candidates; or for automatic tagging of people in photos (Facebook for example). But, facial recognition is not used only by the private sector. Its evolution has attracted the public sector too, especially law enforcement and border management. This has generated many debates on the impact on human rights.

Artificial Intelligence (AI) systems are typically trained on data generated by people.[3] Therefore, it is possible that any AI system would reflect the social biases of the people who developed their datasets.[4] On the other hand, it raises concerns of breach of privacy when used in public spaces (ie mass surveillance), discrimination (the algorithm has proven problematic for people of colour), false labelling based on facial expressions (ie in interviews or for criminal profiling), unwanted tagging and when used to send advertisements based on shops people have visited. It also causes intimidation to people and a feeling of intrusiveness. Public safety and expression of consent by people are classic justifications behind the use of such identification technology. But questions remain: Is it necessary? is it the best/right remedy? is it proportional? is it effective? and, ultimately, is the expressed consent informed consent?

1 Ella Jakubowska, 'Facial Recognition and Fundamental Rights 101' (*EDRi*, 4 December 2019) <https://edri.org/facial-recognition-and-fundamental-rights-101/> accessed 25 April 2020.

2 Ibid.

3 Council of Europe, 'Discrimination, Artificial Intelligence, and Algorithmic Decision-Making' (Council of Europe 2018).

4 Ibid.

INTRODUCTION

Surveillance cameras have been used long before facial recognition technology was created. Private businesses and public institutions have deployed surveillance cameras all around their properties facing the public areas in order to detect any potential property theft or attack. Many states have legislation in place that allows law enforcement to take the recordings of those cameras for the investigation of any criminal act that may have occurred in those areas. Law enforcement officials would use these recordings to detect the faces of the offenders which they would then manually match with pictures of offenders they had in their archives. The innovations brought by facial recognition technology are the new analytical capabilities and the automatic identification in real time, thus an increased intrusiveness of these tools, posing many risks to human rights.

There are two main purposes of the use of facial recognition technology by law enforcement: to identify known criminals and as a predictive method to identify unknown individuals who may be potential criminals. This policy paper is focused on issues arising from the use of facial recognition technology by law enforcement agencies (LEA) and human rights compliance. It focuses on the risks that a European face database would cause to illegal surveillance and the risks of its algorithmic bias and inaccuracy, causing discrimination, particularly for people of colour and other marginalised social groups. During the data collection of a dataset, data may be collected, digitised, adapted and entered into a database according to human-designed criteria.[5] This means that behind the rationale of how data is categorised, which data is included or discarded and how an algorithm assesses those data are human decisions.[6] This means that the bias of human designers can be reflected in algorithmic bias.

This policy brief analyses these issues in the context of breaches of fundamental human rights by the use of facial recognition technology by law enforcement. It focuses not only on privacy and non-discrimination, but also on democracy, freedom, anonymity, equality and the potential of creating a culture of fear. After using a three-part test analysis, this policy brief recommends adopting legislation that specifically regulates facial recognition technology. The legitimacy, necessity and proportionality test should be a crucial element before approving the use of such technology in any specific area. In the digital ages in which we are living, banning a technology completely is not the best solution. Banning facial recognition technology will not stop its creation and further development. We need to find flexible solutions that are in compliance with human rights regulations.

PROBLEM DESCRIPTION

Human rights law requires that any interference with individual human rights must be in accordance with the law, pursue a legitimate aim and be necessary in a democratic society. There are signs that the European Union (EU) could soon be creating a network of national police facial recognition databases which would be shareable among EU countries.[7] It is highly possible that the use of facial recognition by law enforcement would be inadequate with the 'in accordance with the law' requirement under human rights law. This shows a need for reforming how the incorporation of new technologies and policing practices is approached by law enforcement and a need for incorporation of human rights considerations into law enforcement actions. Should the EU ban the use of facial recognition by law enforcement, such as in California, or should they allow innovation and experiment in this direction?

Cyberlaw is a very dynamic area which re-

5 Tarleton Gillespie, Pablo J Boczkowski and Kirsten A Foot (eds), *Media Technologies* (MIT Press 2014) 1-30.

6 Ibid.

7 Zach Campbell and Chris Jones, 'Leaked Reports Show EU Police are Planning a Pan-European Network of Facial Recognition Databases' (*The Intercept*, 21 February 2020) <https://theintercept.com/2020/02/21/eu-facial-recognition-database/> accessed 25 February 2020.

quires adequate regulation in order to prevent the negative effects of technology and innovation which can cause serious damage to individuals and their human rights. The EU, as with every other region, is constantly working towards finding innovative ways of fighting crime and deviancy, with a special focus on less time-consuming methods of identification of criminals. Since law enforcement are challenged with a very dynamic criminal environment, especially due to technological innovation which is widely used by criminals, with new challenges and threats, the EU's law enforcement policy must be equally dynamic and flexible enough to effectively respond to crime development.

While the concept of face recognition is very recent, we are witnessing a rapid increase of the use of such technology in the region, and there is a high potential of such technology being used by law enforcement for identification of criminals, and even of potential criminals based on some scientific algorithms that such face recognition technology would use to study facial features and behaviour. Such potential use by LEA points out the high risks that the EU population, and other nationals while in the EU territory, would face in cases of no regulation of the use of face recognition technology or weak policies. Such risks include but are not limited to: breach of privacy, discrimination (for ie racial and ethnic discrimination) or false labelling based on facial expressions (ie algorithms might consider an innocent person as having a high potential for committing a crime, or algorithms predicting risks of recidivism by analysing facial expressions). Moreover, if people know they are being recognised and/or surveilled, this could cause a change of behaviour when in public spaces, not only leading to people feeling less free, but also to misinterpretation of such changes of behaviour by the algorithms, which would bring us back to the false labelling.

FUNDAMENTAL RIGHTS IMPLICATIONS OF USING FACE RECOGNITION TECHNOLOGY: JUSTIFIED INTERFERENCE WITH HUMAN RIGHTS?

Interferences with fundamental rights can only be justified if they respect the requirements of the EU Charter of Fundamental Rights[8] and of the European Convention on Human Rights (ECHR).[9] Pursuant to the three-part test developed by the European Court of Human Rights (ECtHR), any rights interference has to pursue a legitimate aim, be in accordance with the law, as well as necessary in a democratic society (necessity and proportionality test).

'In accordance with the law' requirement

Currently there is no regulation regarding the use of face recognition technology neither in public nor in private sectors. In deciding upon the use of face recognition technology in law enforcement, the EU must follow written regulations that are clear and not ambiguous. Otherwise, LEA might not know when and how to use the face recognition technology, leading to many abuses of civil rights and liberties. So far, the tests and deployments of facial recognition technologies in EU member states by public authorities have mainly focused on technical accuracy and did not assess fundamental rights implications more broadly.[10] There is a need for a multidisciplinary assessment of the face recognition technology implications before drafting legislation on the matter.

Legitimacy, necessity and proportionality requirements

Any law enforcement activity must be fully compliant with fundamental human rights laws, regardless of the technology used. EU law

8 Charter of Fundamental Rights of the European Union.

9 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

10 European Union Agency for Fundamental Rights (FRA), 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (FRA 2019).

recognises people's facial images as 'sensitive data',[11] which are a form of biometric data. Facial images have been recognised as personal data also by the Court of Justice of the European Union and the ECtHR.[12] This kind of sensitive personal data is very easy to collect in public spaces, and may result in breaches of privacy and other human rights. This is why EU data protection law provides specific protection for this kind of data.[13]

Nevertheless, privacy rights are not absolute rights. They can be subject to limitations for pursuing a legitimate aim. Pursuant to article 8 of the ECHR, the legitimate grounds for restricting privacy are for the protection of national security and/or public order.[14] Under these specifics, legitimate aims for the use of face recognition technology by law enforcement include prevention, detection and investigation of terrorism and other serious crimes. Considering that the use of face recognition technology poses risks to certain human rights, including privacy, the legitimate grounds for using facial recognition technology should be a complete exhaustive list, not an open-ended list that states can modify. Any restriction must pass the legitimacy test and, if successfully passed, such restrictions should be applied only when really necessary and only in proportionate terms. The use of face recognition technology disproportionally will create a fear of being in public, a feeling of lack of freedom, leading to forced changes of behaviour when in public areas.

Therefore, there is a need to strike a balance between the increased security that face recognition technology is supposed to guarantee and the measures taken. Even if the legitimate grounds for using face recognition technology are met, such technology should not be used without public knowledge of it being used. This does not mean that face surveillance stops being a threat to civil rights and liberties if its use is fully known to the public. People may still feel less safe and less free if they know their identities and locations will be tracked.

Privacy and personal data protection

The ability of face recognition technology to track people's location and movements raises many privacy concerns. When this tracking is associated with storing and processing these data, it raises many concerns about personal data protection too. Location tracking means that the government or any other entity using face recognition technology would be able to study a citizen's movements, habits, lifestyle and association. This would cause a legitimate fear of lack of anonymity, autonomy and freedom while walking down the street that only privacy can provide.

Since facial recognition technology uses personal data, collecting and processing facial images by such technology must be in line with the data protection principles of European data protection law, especially the EU's General Data

11 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 OJ 2016 L 119/89 (Law Enforcement Directive) OJ L 119 (4.5.2016) art 10(1); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119 (4.5.2016) art 9(1); Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 On the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of Such Data, and Repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC OJ L 295 (21.11.2018) art 10(1).

12 Case C-291/12 *M Schwarz v Stadt Bochum* [2013] 22, 48-49; *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016) 56.

13 FRA, Council of Europe and EDPS, 'Handbook on European Data Protection Law' (FRA 2018); FRA, 'Preventing Unlawful Profiling Today and in the Future: A Guide' (FRA December 2018) 35-38.

14 European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights – Right to Respect for Private and Family Life, Home and Correspondence' (Council of Europe 2019) paras 133, 136.

Protection Regulation (GDPR). Pursuant to article 5 of the GDPR and also article 4 of the Law Enforcement Directive (LED), the processing of facial images must be lawful, fair and transparent, have an explicit legitimate purpose and comply with the requirements of data accuracy, storage limitation, data security and accountability.[15] Articles 35 and 36 of the GDPR require conducting a Data Protection Impact Assessment of this technology analysing its risks and compliancy with the GDPR and other data protection principles,[16] and also prior consultation with the Data Protection Authority. The role of the Data Protection Authority is essential in this regard for safeguarding fundamental human rights.

Non-discrimination

As previously mentioned, LEA have been using data from surveillance cameras long before facial recognition technology was created. The main difference with facial recognition is that the face detections and the matches are now done automatically by a specific AI technology. This saves a lot of valuable time for LEA. However, research shows that this kind of technology does not always have a high accuracy rate, especially on moving videos,[17] and that it tends to wrongly identify women and people of colour.[18] Such lack of accuracy could cause discrimination, and if used in cases of immediate action from LEA (being wrongfully stopped or even arrested by the police), can even cause the wrong person to get hurt or killed.

Moreover, the feeling of being watched would lead to forced changes of behaviour as already mentioned. People would try to change behaviour in public in order to fit to public norms of a certain country or city, even though they do not agree with them, out of fear of being discriminated. Freedom of movement in anonymity and respect for private life are directly associated with the exercise of other human rights, such as the freedom of thought and religion, freedom of expression, and freedoms of assembly and of association, rights which would be directly affected out of fear of being under surveillance.

USE OF FACE RECOGNITION TECHNOLOGY BY LAW ENFORCEMENT IN THE EU

Many cities in the United States have decided to ban the use of facial recognition technology, including for law enforcement.[19] Others have not taken any action or have accepted its use by the police for crime prevention. In the United Kingdom, facial recognition technology is being used by police in public spaces but is currently under legal challenge.[20] Several EU member states have been conducting tests and made plans for using facial recognition technology.[21]

The EU has not made any decisions yet in regard to the use of facial recognition technology, potentially because of the ongoing debates on

15 General Data Protection Regulation (n 9) art 5; Law Enforcement Directive (n 9) art 4 and recital 26.

16 Law Enforcement Directive (n 9) arts 27-28.

17 J Buolamwini and T Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 1, 1-15. See also Gender Shades, 'Gender Shades Project' <http://gendershades.org/overview.html> accessed 20 March 2020; NIST, 'NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software' (*NIST*, 19 December 2019) <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software> accessed 30 March 2020.

18 B Smith and CA Browne, *Tools and Weapons: The Promise and the Peril of the Digital Age* (Penguin Press 2019).

19 Eoin O'Carroll, 'Face off? Americans fear privacy loss to recognition software' (*The Christian Science Monitor*, 20 June 2019) <https://www.csmonitor.com/Technology/2019/0620/Face-off-Americans-fear-privacy-loss-to-recognition-software> accessed 20 March 2020; T Rosenberg, 'Oakland Passes Facial Recognition Ban' (*Oakland Privacy*, 14 May 2019) <https://oaklandprivacy.org/san-francisco-approves-oversight-of-surveillance-tech-and-becomes-1st-municipality-in-the-country-to-ban-the-use-of-facial-recognition/> accessed 30 March 2020.

20 Liberty, 'Liberty fights for facial recognition ban following court ruling' (*Liberty*, 4 September 2019) <https://www.libertyhumanrights.org.uk/issue/liberty-fights-for-facial-recognition-ban-following-court-ruling/> accessed 27 February 2020.

21 See Ella Jakubowska, 'The many faces of facial recognition in the EU' (*EDRi*, 18 December 2019) <https://edri.org/the-many-faces-of-facial-recognition-in-the-eu/> accessed 25 April 2020.

mass surveillance in the region. However, the EU's GDPR, which passed two years ago, has introduced a number of restrictions on the use of individuals' identifiable information, including images of their faces. One may argue that databases of face images do not have any difference to databases of fingerprints and DNAs in that they are all identifiable information. Therefore, if fingerprints and DNA databases are allowed to be used for crime investigation, then face recognition technology databases should be created and used too. But, fingerprints and DNA cannot be recognised by AI at a distance, therefore they cannot be used in public places for identifying and tracking individuals. This means that face recognition technology poses a higher risk on human rights and liberties since it can be used in public spaces and without people's knowledge.

An important issue of the use of facial recognition technology by law enforcement is also the interoperable exchange of biometrics information by law enforcement on an international level. Such an exchange of this data in the field of police and judicial cooperation in criminal matters within the EU is regulated by the LED.[22] The definition of 'biometric data' provided by article 3(13) of the LED includes facial images. Both the GDPR and LED pay particular attention to the quality of data, including the quality of facial images. Under article 5(1)(d) of the GDPR and article 4(1)(d) of the LED, the information used by the authorities should be accurate and up to date. This means that LEA are obliged to use facial images of a low quality more cautiously because their accuracy is lower, having a higher potential of error and wrong matches.

Pursuant to article 10 of the LED, the processing of biometric data is allowed only 'where authorized 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'. Whereas article 10 of the LED provides for the use of automated individual decision-making in criminal matters, including profiling, only when authorised by EU or member state law 'to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller' and only when 'legitimate interests are in place'. Therefore, the LED pays particular attention to the safeguarding of human rights and to proportionality for the processing and transferring of databases of facial recognition technology as a technology based on automated processing and profiling.

Informed consent poses an important issue in the processing of facial images by LEA. Operations carried out by LEA, including the use of facial recognition technology for criminal investigations, might work only without informed consent, otherwise the investigations of criminals might be compromised. This is why this limitation of the right to informed consent must be strongly justified.

POLICY RECOMMENDATIONS

According to a recent report by Tilburg University, it is necessary to distinguish between the purposes of the use of facial recognition technology, in order for the legislators to make sound decisions on regulations that need to be put in place.[23]

With the rapid evolvement of technology and its use by criminals, who are often a step ahead of the LEA, banning the use of a technology which would fasten the identification of criminals and their location, by also reducing the number of law enforcement agents needed for a specific case, would most probably not be the best solution. It should also be taken into consideration that if LEA know such technology exists, some may try to find a gap in the law that allows them

22 Law Enforcement Directive (n 9) 89-131.

23 Esther Keymolen and others, 'Op het eerste gezicht. Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties' (in Dutch) (Tilburg University/TILT April 2020) <https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z07066&did=2020D15053> accessed 24 April 2020; Tilburg University, 'Dutch Experiment with Facial Recognition: Privacy Risks Require Legislative Choices' (*Tilburg University Press*, 21 April 2020) <https://www.tilburguniversity.edu/current/press-releases/privacy-risks-facial-recognition-technology> accessed 24 April 2020.

to use it anyway, or even if the law would be such that leaves no gaps, there will still be some LEA that will illegally use it to the benefit of their investigations. Thus, it is inevitable that at some point in time, most probably not very far from now, facial recognition technology will be the new trend in investigation tools. Leaving facial recognition technology unregulated would cause a large scale of mass surveillance, leading to further breaches of fundamental human rights and liberties.

Therefore, the most viable solution would be very detailed regulations and policy that would frame the use of facial recognition technology to the benefit of LEA and the whole criminal justice system, but through safeguarding human rights. Such policies would include a close cooperation with human rights agencies and experts and tech development experts, so as to remove as much as possible the margins of error of the algorithms, by assuring a human control on the results of such technology. These steps would be in conjunction with human rights-based regulation.

Banning law enforcement from using technology that would allow them to perform better in tackling crime and better protecting the society is not the ideal solution. Instead of no regulation or bans, there is a need for careful, detailed regulations that do not leave spaces for misinterpretation. Any gaps in such regulations can easily be (ab)used by companies and governments who want to control their citizens. No regulation means each state has complete freedom of using and abusing this technology. Therefore, there is a need for regulations at regional and global levels, with a primary focus on human rights and privacy protection. Regulations would ensure that governments do not abuse such technology for mass surveillance purposes (as in the case of China with its Social Credit System) and guarantee that it is used in compliance with fundamental rights and liberties.

Nevertheless, there is not yet enough research to prove the high impact of face recognition technology in criminal investigations, its level of accuracy and reliability. Specific research is needed also on the accuracy of this technology for certain demographic groups defined by age, sex and race, vulnerable to discrimination. Therefore, there is a need for further research on the effectiveness of the use of face recognition technology by law enforcement and the legal, ethical and social implications of the deployment of this technology. Further research is needed on the rate of successful identification of wanted criminals and if it really helps to solve any crimes. Until such research exists, proving the impact of facial recognition technology in effective and rapid criminal investigations, such that cannot be obtained by other less intrusive techniques, therefore justifying its deployment, such technology should not be used.

If research proves the high positive impact of the use of face recognition technology in criminal investigations, then, and only then, can we talk about allowing limited deployment of such technology. Its deployment would then have to be limited to only investigations of specific crimes which pose a high threat to national security and public order, and to specific vulnerable groups (ie for identifying online child sexual abuse perpetrators and suspected terrorists, especially in cases of cyber terrorism). These measures would be taken hand in hand with increased public awareness of the use of such technology and informed consent of the public when such technologies are used in public spaces. Yet, legislation would still have to allow the use of face recognition technology for criminal investigations with the condition that it is accompanied by further evidence. The face recognition technology can be used for making the potential offender identification easier and faster and then further investigating the identified suspect until additional evidence is found. Basing a judgement only on face recognition technology, without any other evidential support, should be banned.

Countries would then also have to establish strict regulations on privacy and data protection related to the use of face recognition databases and results from investigations with such technology, especially on the transferring of data across borders. Such policies should be based on GDPR and other related legislation. In any case, there should be human verification of all automated matches.

With the rapid developments in technology and society, the day when the use of face recog-

nition technology will become a new normality, despite the many contestations, does not look that far away. This is why, there is a need for increased funding for and support of the development of algorithms of face recognition technology with a human rights by design feature.

An important measure would also be the introduction of licenses for allowing the use of pre-tested face recognition technology only for an exhaustive list of entities. This diversified approach of explicitly specifying which technology is permitted and by which entities would eliminate any legal uncertainty. Any fundamental changes/modifications to the technology, that would result in providing different outputs by such technology, would require a license too.

As a conclusion, for the time being, strict regulation seems to be the most suitable solution. Such regulation could be later evaluated and reconsidered once the facial recognition technology has developed further and extensive research on its effectivity and impact has been conducted.

REFERENCES

Buolamwini J and Gebru T, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 1

Campbell Z and Jones C, 'Leaked Reports show EU Police are Planning a Pan-European Network of Facial Recognition Databases' (*The Intercept*, 21 February 2020) <https://theintercept.com/2020/02/21/eu-facial-recognition-database/?te=1&nl=the-privacy%20project&emc=edit_priv_20200225> accessed 25 February 2020

Case C-291/12 *M Schwarz v Stadt Bochum* [2013]

Charter of Fundamental Rights of the European Union

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)

Council of Europe, 'Discrimination, Artificial Intelligence, and Algorithmic Decision-Making' (Council of Europe 2018)

Davies B, Innes M and Dawson A, 'An Evaluation of South Wales Police's Use of Automated Facial Recognition' (Universities' Police Science Institute and Crime & Security Research Institute, Cardiff University 2018)

The Public Voice, 'Declaration: A Moratorium on Facial Recognition Technology for Mass Surveillance' (October 2019) Tirana, Albania <https://thepublicvoice.org/ban-facial-recognition/> accessed 25 February 2020

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 OJ 2016 L 119/89 (Law Enforcement Directive) OJ L 119 (4.5.2016)

European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights – Right to Respect for Private and Family Life, Home and Correspondence' (Council of Europe 2019)

European Union Agency for Fundamental Rights (FRA), 'Preventing Unlawful Profiling Today and in the Future: A Guide' (FRA 2018)

— 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (FRA 2019)

FRA, Council of Europe and EDPS, 'Handbook on European Data Protection Law' (FRA 2018)

Fussey P and Murray D, 'Independent Report on the London Metropolitan Police Service's Trial of Life Facial Recognition Technology' (The Human Rights, Big Data and Technology Project 2019)

Garvie C, Bedoya A and Frankle J, 'The Perpetual Line-Up: Unregulated Police Face Recognition in America' (*Georgetown Law Center on Privacy & Technology*, 18 October 2016)

Gender Shades, 'Gender Shades Project' <http://gendershades.org/overview.html> accessed 20 March 2020

Gillespie T, Boczkowski PJ and Foot KA (eds), *Media Technologies* (MIT Press 2014)

Jakubowska E, 'Facial Recognition and Fundamental Rights 101' (*EDRi*, 4 December 2019) <https://edri.org/facial-recognition-and-fundamental-rights-101/> accessed 25 April 2020

— 'The many Faces of Facial Recognition in the EU' (*EDRi*, 18 December 2019) <https://edri.org/the-many-faces-of-facial-recognition-in-the-eu/> accessed 25 April 2020

Keymolen E and others, 'Op het eerste gezicht. Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties' (in Dutch) (Tilburg University/TILT April 2020) <https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z07066&did=2020D15053> accessed 24 April 2020

Liberty, 'Liberty Fights for Facial Recognition Ban Following Court Ruling' (*Liberty*, 4 September 2019) <https://www.libertyhumanrights.org.uk/issue/liberty-fights-for-facial-recognition-ban-following-court-ruling/> accessed 27 February 2020

O'Carroll E, 'Face off? Americans fear privacy loss to recognition software' (*The Christian Science Monitor*, 20 June 2019) <https://www.csmonitor.com/Technology/2019/0620/Face-off-Americans-fear-privacy-loss-to-recognition-software> accessed 20 March 2020

NIST, 'NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software' (*NIST*, 19 December 2019) <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software> accessed 30 March 2020

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119 (4.5.2016)

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 On the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of Such Data, and Repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC OJ L 295 (21.11.2018)

Rosenberg T, 'Oakland Passes Facial Recognition Ban' (*Oakland Privacy*, 14 May 2019) < https://oaklandprivacy.org/san-francisco-approves-oversight-of-surveillance-tech-and-becomes-1st-municipality-in-the-country-to-ban-the-use-of-facial-recognition/> accessed 30 March 2020

Schneier B, 'We're Banning Facial Recognition. We're Missing the Point' (*The New York Times*, 20 January 2020) <https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html?te=1&nl=the-privacy%20project&emc=edit_priv_20200225> accessed 20 March 2020

Smith B and Browne CA, *Tools and Weapons: The Promise and the Peril of the Digital Age* (Penguin Press 2019)

Szabó and Vissy v Hungary App No 37138/14 (ECtHR, 12 January 2016)

Tilburg University, 'Dutch Experiment with Facial Recognition: Privacy Risks Require Legislative Choices' (*Tilburg University Press*, 21 April 2020) <https://www.tilburguniversity.edu/current/press-releases/privacy-risks-facial-recognition-technology> accessed 24 April 2020

Williams P and Kind E, 'Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe' (European Network Against Racism 2019)

Global Campus of Human Rights

Monastery of San Nicolò
Riviera San Nicolò, 26
I-30126 Venice Lido (Italy)

gchumanrights.org

Global Campus of Human Rights

The Global Campus of Human Rights is a unique network of more than one hundred participating universities around the world, seeking to advance human rights and democracy through regional and global cooperation for education and research. This global network is promoted through seven Regional Programmes which are based in Venice for Europe, in Sarajevo/Bologna for South East Europe, in Yerevan for the Caucasus, in Pretoria for Africa, in Bangkok for Asia-Pacific, in Buenos Aires for Latin America and the Caribbean, and in Beirut for the Arab World.

The Global Campus Policy Observatory

The Observatory is a 'virtual hub' which comprehends a team of seven researches from the regional programmes to produce, publish and publicly present seven different policy analyses in form of policy briefs, with the aim of making of each regional programme a solid focal point for policy expert advisory in human rights issues.

This document has been produced with the financial assistance of the European Union and as part of the Global Campus of Human Rights. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or of Global Campus of Human Rights.