Navein Reet: Nordic Journal of Law and Social Research (NNJLSR) No. 9 2019, pp. 325-344

Police use of facial recognition technology and the right to privacy and data protection in Europe

Marya Akhtar[1]

Abstract: This article examines the human rights challenges of police use of facial recognition technology from a European perspective. Based on both international human rights law, the European Convention on Human Rights and EU law, the article argues that the technology challenges human rights. The focus of the article is on the right to privacy and data protection, as this right is fundamentally at risk by the technology. Acknowledging that other rights and guarantees are also negatively impacted by the use of facial recognition technology, the article makes reference to the risk of discrimination, and the unregulated cooperation between State and the surveillance technology industry. However, a central point in the article is that *irrespective* of whether the technology can be refined to eliminate risk of discrimination, and *even if* sufficient safeguards for cooperation between State and the industry are put in place, *fundamental* challenges remain in relation to the right to privacy and data protection. The technology captures the unique facial features of an individual known as biometric data which is highly sensitive data and creates an interference with the right to privacy and data protection. By allowing facial recognition, society allows for an entirely new type of intensive surveillance. The use of the technology also entails a risk of chilling effect on e.g. freedom of assembly which furthers negative implications on human rights. The article concludes that when it comes to police use of facial recognition technologies, States should tread carefully and ensure that a sufficient human rights-based regulatory framework and adequate safeguards are in place before considering using the technology.

Introduction

The use of facial recognition technology has been debated extensively in many parts of the world during the last couple of years. The technology is based on Artificial Intelligence (AI) and can be used for *identifying* or *verifying* the identity of individuals

1 Senior Legal Advisor at the Danish Institute for Human Rights and External Lecturer at the University of Copenhagen, Faculty of Law. Parts of the article are based on legal analysis by the author in Overview on Facial Recognition to Combat Crime, Danish Institute for Human Rights, December 2019 available here: https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/udgivelser/overblik_ansigtsgenkendelse_uk_02.pdf

or for *categorisation* where information about an individual's characteristics (such as e.g. sex, age or ethnicity) are extracted.

The focus of this article is on *police* use of the technology and the human rights challenges which this raises. Whilst the technology is used for different commercial or public purposes ranging from unlocking smartphones (Pardes 2018) to automatic border control gates (so-called ABC gates) in airports[2], and more recently, has also been discussed in the wake of Covid-19[3], specific challenges arise when police make use of the technology for investigations. This is so because by enforcing law – if necessary, by use of force – the police are empowered with far-reaching public authority (and assume a major responsibility) in society. Consequently, any technological measures which they make use of must be viewed considering both the important societal task and the responsibility placed upon them.

Furthermore, the article deals with police use of the technology from a *European* human rights perspective. Thus, the article deals with rights and freedoms ensured not only in the international human rights regime, but also by the regional regimes established by the Council of Europe and the European Union, including case law of the two regional European courts – the European Court of Human Rights and the European Court of Justice. Particularly EU law provides comprehensive protection of personal data and is legally binding directly within the Member States (differing from international public law in this supranational – binding – character). Because of this established regional human rights regime, if European countries decide to use of facial recognition technology, they will have to argue compliance with established rules and principles in European law.

Another distinct characteristic which forms the backdrop for discussions related to facial recognition technology in this article, is the on-going work on *AI and human rights* both within the Council of Europe and the European Union. Here, ethical and human rights approaches (and combinations of both) to AI are being examined and the question of introducing an altogether new legal framework for AI is being raised. This developing cross-disciplinary field explores questions related to ethics vis-à-vis legal obligations; State responsibility vis-à-vis product liability and questions related to programming "fair", "accountable" or "transparent" algorithmic models vis-à-vis ensuring human

2 European Union Fundamental Rights Agency in "Facial Recognition Technology: fundamental rights considerations in the context of law enforcement" November 2019

3 COVID-19 opens door to Facial Recognition Technology, 11 May 2020DLA Piper, available here: https://denmark.dlapiper.com/da/pdf/news/2357

rights in the design, development and deployment of the model.[4] For the purpose of this article, it suffices to highlight that the lack of a clear position on the legal implications of AI is a consequence of the many-facetted and far-reaching challenges posed by AI, many of which society is yet to identify and understand fully.

Lastly, the focus of the article is on the *right to privacy and data protection*. This does not mean that other human rights are not impacted by the technology; other rights are undoubtedly at risk and risks pertaining to non-discrimination (and general errors in the technology) and poorly regulated cooperation between State and the surveillance technology industry are particularly highlighted in the article. However, the position in this article is that serious impacts on privacy and data protection are *inherent* in the very technology itself. This is the case because the technology captures biometric data (comparable in terms of sensitivity with DNA), making it possible to carry out surveillance on a much more detailed and ubiquitous manner than ever before. This entails not only an increase in surveillance possibilities but can risk fundamentally altering the nature of the public space creating monumental changes in society and in the very concept of privacy (Bauman and Lyon 2013; Lyon, 2008; Murakami Wood 2003). Whilst other challenges (such as risk of discrimination and State collaborations with surveillance technology companies) can *theoretically* be mitigated, the privacy concerns are ingrained in the nature and purpose of the technology itself.

The rest of the article is structed as follows: in Section 2, a brief overview of the technology and perspectives on its use globally and in Europe are provided; in Section 3, risks pertaining to discrimination are presented followed by Section 4 in which main concerns regarding the collaboration between State and the private surveillance technology industry are described. In Section 5 the fundamental challenges to privacy

4 To name a few initiatives where these and other questions are posed, see e.g. from the European Union: High-Level Expert Group on AI established under the EU Commission and their Ethics Guidelines for Trustworthy Artificial Intelligence from April 2019; Paper on EU guidelines on ethics in artificial intelligence: Context and implementation, PE 640.163 by the European Parliamentary Research Service, September 2019 and EU Commission White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final, February 2020. From the Council of Europe, see e.g. the so-called Wagner report, Study on the Human Rights Dimensions of Automated Data processing Techniques (in particular Algorithms) and possible regulatory implications, DGI(2017)12 prepared by the Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT), March 2018; by the same Expert Committee: Study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework, DGI(2019)05, September 2019 and Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, adopted by the April 2020 at the 1373rd meeting of the Ministers' Deputies.

and data protection are dealt with in detail and specific issues highlighted in relation to mass surveillance and the risk of "chilling effects" on other rights. Section 6 provides some concluding remarks and perspectives.

An overview of the technology and its use

Facial recognition is based on so-called AI (which remains subject to many differing definitions[5]) and captures the unique facial features (biometric data) of individuals to identify them. The technology has many uses, ranging from verifying an image with an individual (so-called "one-to-one" comparison) to recognising facial images against large databases ("one-to-many" comparison). Facial recognition can be used to scan material on the internet and to surveil individuals in public spaces.[6] The technology can be used without a person reviewing the material (fully automated), or by ensuring "human control" during or after the automated process. One-to-one comparison is used for *verification* (also called authentication). In these cases, the technology compares the two facial images and if the likelihood that the two images show the same person is above a certain threshold, the identity is verified.[7] One-to-many comparison is used for *identification* which entails that the facial image of an individual is compared to many other images in a database to find a possible match. Sometimes images are checked against databases, where it is known that the reference person is in the database (closed-set identification), and sometimes, where this is not known (open-set identification).[8] In addition, *categorisation* entails matching general characteristics such as sex, age and ethnic origin without necessarily identifying the individual.[9]

The technology has led to research into e.g. emotional recognition (see e.g. Barrett, et. al. 2019)[10] and – as a somewhat perplexing retrogression back to 17th century criminologist Lombroso – research claiming that facial recognition can be used to detect

5 See e.g. the paper by the AI High Level Expert Group set up by the EU Commission, "A definition of AI: Main capabilities and scientific disciplines", 8 April 2019

6 For a general overview on the use of the technology and its implications on Human Rights, see the European Union Fundamental Rights Agency in "Facial Recognition Technology: fundamental rights considerations in the context of law enforcement" November 2019

7 Ibid

8 Ibid

9 Ibid

10 European Commission, "Smart lie-detection system to tighten EU's busy borders," 24 October 2018, and the website of iBorderCtrl.

if someone is "likely going to be a criminal".[11] Such highly controversial (and mostly unsubstantiated) claims raise great concerns both on a legal and ethical level. However, even if these novel and worrisome claims are put aside, police use of the technology in its "simple" form, challenges the rights of individuals. This is the case when the technology is deployed by the police for *identification* based on watchlists (in order to identify specific individuals) or for general surveillance in the public space (mass surveillance e.g. for intelligence purposes). *Verification* (particularly if put under "human control") does not raise the same type of concerns. *Categorisation* can be problematic particularly if deployed in a discriminatory manner.

People's faces are – for the most part – visible, but facial features constitute unique biometric data comparable in sensitivity to DNA. There is a historically strong focus on privacy, data protection and protection against mass surveillance in Europe, but the human rights challenges of the technology are not by any means limited to Europe.[12] The lawfulness of facial recognition technology for law enforcement purposes has been put into question because of its serious implications on human rights. Use of the technology has been met with criticism from a wide range of NGO's and civil rights organisations[13], the UN[14] and even some of the companies which develop the technology.[15]

---

11 The claim from scientists from Harrisburg University led to an outcry amongst data scientists and lawyers alike. See description of the research here https://web.archive.org/web/20200506013352/https://harrisburgu.edu/hu-facial-recognition-software-identifies-potential-criminals/ and a statement from the University about halting the publishing of the paper here: https://harrisburgu.edu/hu-facial-recognition-software-identifies-potena tial-criminals/

12 For more on the historical background for the European perspective on privacy, see e.g. Grabenwarter 2014, For more on the history of human rights and arguments which counter the traditional narrative of human rights (civil and political rights in particular) as "Western" concepts see e.g. Jensen, S., 2016.

13 See e.g. Amnesty International, Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance, 11 June 2020.

14 See e.g. UN Human Rights Commissioner, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peace protests, 24 June 2020, A/HRC/44/24; the United Nations Human Rights Council, "Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 28 May 2019, A/HRC/41/35; and The United Nations Human Rights Council, "Rights to freedom of peaceful assembly and of association - Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", 17 May 2019, A/HRC/41/41

15 See e.g. the letter from IBM June 8, 2020 addressed to Congress on Racial Justice Reform; press release from Amazon June 10 2020 "We are implementing a one-year moratorium on police use of Rekognition"; and statement from Microsoft President Brad Smith June 11 on Washington Post Live, The Path Forward: Technology & Society

Troublesome use of facial recognition technology has already been demonstrated in the United States and in China where the technology has been deployed widely. Distinct issues have been raised in the current US debate on facial recognition – particularly with reference to the Black Lives Matter movement and the risk of discrimination in the technology.[16] Similarly, use of the technology in China is to be viewed in its own national and regional context.[17] Experiences from both countries show that the technology can be deployed with considerable harmful impacts on human rights. While comprehensive examples from the two countries and their contexts fall outside the scope of this article, one case may serve to illustrate the global impacts of the technology:

The Chinese government's alleged counterterrorism actions against minorities in the Xinjiang region has led to accusations of mass surveillance[18] in which the technology has supposedly been deployed for racial profiling (*categorisation*).[19] The mass surveillances in Xinjiang with the help of advanced surveillance technology has raised concerns on

16 For further reading, see e.g. Report by Algorithmic Justice League, "Facial Recognition Technologies in the Wild: a Call for a Federal Office", 29 May 2020; Kashmir Hill, "Wrongfully Accused by an Algorithm", 24 June 2020, The New York Times; and WCPO Statement 24 June 2020 in Response to The New York Times Article.

17 Denis de Castro Halis elaborates more on the use of facial recognition technology during the Hong Kong protests in his article, Digitalization and Dissent in Legal Cultures. Chinese and Other Perspectives in this issue of the journal. For more on Chinese police surveillance, see also Daniel Sprick, Predictive Policing in China: An Authoritarian Dream of Public Security, in this issue of the journal.

18 See Human Rights Watch, Data Leviathan: China's Burgeoning Surveillance State, 16 August 2019. For more on Chinese police surveillance, see also Daniel Sprick, Predictive Policing in China: An Authoritarian Dream of Public Security, in this issue of the journal.

19 See Mozur, "One month, 500,000 face scans: how China is using A.I. to profile a minority", The New York Times, 14 April 2019; and Thomas Phillips, China testing facial-recognition surveillance system in Xinjiang, 18 January 2018, The Guardian.

an international level.[20] One of the companies whose systems have evidently been used in Xinjiang is Hikvision[21] whose surveillance products are also purchased by European countries.[22] Furthermore, some of the company's technology is designed and developed in Europe.[23] Large surveillance technology companies have a global reach and their commercial interests may collide with human rights and aid potential violations of human rights. This raises principle issues related to collaborations between State and private companies; the case illustrates the question if and how State responsibility is applicable to companies enabling human rights violations elsewhere in the world. This question is explored more below in Section 4.

In Europe, facial recognition technology has yet mostly been used on trial basis.[24] In its White Paper on Artificial Intelligence from February 2020, the EU Commission announced that in order to address possible societal concerns relating to technology such as facial recognition, the Commission will launch a broad European debate on the specific circumstances, if any, which might justify such use, and continued that there is a need for a European debate on the necessary legal guarantees if the technology

20 See e.g. Concluding observations on the combined fourteenth to seventeenth periodic reports of China (including Hong Kong, China and Macao, China) by the Committee on the Elimination of Racial Discrimination, CERD/C/CHN/CO/14-17, 19 September 2018; joint letter by Mandates of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; the Working Group on Arbitrary Detention; the Working Group on Enforced or Involuntary Disappearances; the Special Rapporteur on the right to education; the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful assembly and of association; the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health; the Special Rapporteur on the situation of human rights defenders; the Special Rapporteur on minority issues; the Special Rapporteur on the right to privacy; the Special Rapporteur on freedom of religion or belief; and the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, OL CHN 18/2019, 1 Nivember 2019; Human Rights Watch, China: Big Data Fuels Crackdown in Minority Region Predictive Policing Program Flags Individuals for Investigations, Detentions, 26 February 2018; and Human Rights Watch "Eradicating Ideological Viruses" China's Campaign of Repression Against Xinjiang's Muslims, 9 September 2018.

21 Buckley and Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities", The New York Times, 22 May 2019; and Cadell, "Hikvision, a surveillance powerhouse, walks U.S.-China tightrope", Reuters, 29 August 2019

22 Seidelin and Broberg, "Overvågningsudstyr fra omstridt kinesisk firma bruges i Danmark", Jyllandsposten, 19 June 2020

23 Kjeldtoft, "Aalborg Universitet hjalp kontroversielt kinesisk overvågningsfirma", Politiken, 23 June 2020

24 European Union Fundamental Rights Agency in "Facial Recognition Technology: fundamental rights considerations in the context of law enforcement" November 2019

is used.[25] So far, there has been no judicial review of the legality of facial recognition by the regional human rights courts in Europe and the question of the legality of the technology remains unanswered on a European level.[26]

Above all, facial recognition is an interference with the right to privacy and protection of personal data. Historically, privacy implies a negative relation between the individual and State which is that of non-interference unless necessity is demonstrated. Technology which introduces new and intensive forms of ubiquitous surveillance raises the principle question whether the nature of being in a public space is changing altogether and with that, the notion of privacy (Timan et al 2017).

Before turning to the question about privacy and data protection, some remarks on the risk of discrimination and the lack of safeguards in State-company collaborations within the surveillance technology industry are provided in the following two sections.

Flawed technology leads to risk of discrimination

Even the most advanced facial recognition technology has margins of error. In addition, the technology has been criticised for having particularly high error rates for women and people with a non-western appearance. This firstly diminishes the effectiveness and adequacy of the technology (by creating a risk of false positives or false negatives) but more importantly creates a risk of discrimination insofar as the ability to identify or recognise individuals correctly is worse for women and people with a non-western appearance (See e.g. Joy. 2018; Inioluwa et al. 2019).

For this reason alone, the human rights framework entails that States should be very careful in using the technology, especially when it comes to police use. Flawed and discriminatory technology used for investigatory purposes will create serious challenges to the non-discrimination principle which follows from e.g. the freestanding rights in

25 COM(2020) 65 final, White Paper on Artificial Intelligence - A European approach to excellence and trust p. 22

26 The question of legality of police use of the technology is being tried in the UK where the High Court ruled on a case in September 2019 and found that South Wales Police's use of the technology was consistent with the requirements of the Human Rights Act 1998 (HRA) and data protection legislation, see Bridges, R (On Application of) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) (04 September 2019). The case was appealed and on 11 August 2020, the Court of Appeal rules firstly that the criteria that interferences with the right to privacy shall be "in accordance with law" had not been met and secondly that authorities had failed to investigate whether the technology exhibited any race or gender bias, see [2020] EWCA Civ 1058, Case No: C1/2019/2670.

Article 26 of the International Covenant on Civil and Political Rights and Article 21 of the Charter of Fundamental Rights of the European Union.

Furthermore, flawed technology (irrespective of whether it is discriminatory) will have trouble meeting the criteria of necessity and adequacy ensured in most provisions in the international human rights framework including the right to privacy dealt with in further detail below in Section 5. Similarly, considerations related to rule of law would make police use of flawed surveillance technology highly problematic.

However, *even if*, at some point, the technology reaches a point where it no longer shows a considerable (discriminatory) error rates *and* adequate safeguards are put in place to mitigate the risk, fundamental issues related to the right to privacy and protection of personal data remain unresolved.

Lack of clear rules in cooperation between State and the surveillance technology industry

Turning to the more structural challenges with surveillance technologies (which facial recognition is a part of), State cooperation with the industry gives rise to concern from a democratic and human rights perspective (see e.g. Murray 2020; and on public opinion of police use of the technology, see Ben el al. 2020). This is the case both in relation to State *purchase* of surveillance technologies, and State regulation of *design, development and export* of the technology.

The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has examined the challenges and has stated in relation to *purchase* that "Governments and the private sector are close collaborators in the market for digital surveillance tools. Governments have requirements that their own departments and agencies may be unable to satisfy. Private companies have the incentives, the expertise and the resources to meet those needs. They meet at global and regional trade shows designed, like dating services, to bring them together. From there, they determine whether they are a match." [27]

Moving on to the *design* and *development* side, human rights obligations are also lacking. Similarly, considerations on whether States can (and should) control research which

27 The United Nations Human Rights Council, "Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 28 May 2019, A/HRC/41/35.

contributes to surveillance technology are lacking. With regards to *exports*, the UN Special Rapporteur states that export controls are an important element of the effort to reduce risks caused by the surveillance industry and the repressive use of its technology but are vaguely regulated. Additionally, the UN Special Rapporteur raises concerns regarding problematic influences on State regulation of export and gives an example from the EU: "During recent negotiations on the European Union export control regime, business interests were alleged to have influenced the decision to significantly curtail the inclusion of human rights safeguards in proposed regulatory changes, despite broad agreement on their adoption in the European Parliament (Daniel 2018; Lucie 2017; Catherine 2018).[28]

One of the main problems is that State-company cooperation is not adequately regulated neither in relation to State responsibility nor company due diligence. There are no international or European rules that *effectively* control the purchase, or design, development and export of surveillance technology for police purposes. While public procurement rules may refer to human rights compliance, the criteria for such compliance are vague and no rules ensure *thorough* human rights impact assessments by the State in public procurements of surveillance technology.[29] Private actors such as companies developing or selling surveillance technology for their part are not bound by international human rights rules or regulations. They are encouraged to observe the UN Guiding Principles on Business and Human Rights but ultimately, State responsibility is the measure through which human rights are effectively enforced. Pursuant to the Guiding Principles, States are urged to exercise adequate oversight to meet their international human rights obligations when they contract with or legislate for companies to provide services that may have an impact on the enjoyment of human rights (For more on State responsibility and the responsibility of private actors, see e.g. Lagoutte, et. al 2016).

The overall problem is so serious that the UN Special Rapporteur recommends an immediate moratorium on the global sale and transfer of the technology from the

28 The United Nations Human Rights Council, "Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 28 May 2019, A/HRC/41/35. See also European Commission, "Proposal for a regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast)", 28 September 2016.

29 See item 52 in the UN Special Rapporteur report. In regard to EU public procurement rules, see Directive 2009/81/EC of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security.

surveillance industry until rigorous human rights safeguards are put in place to regulate such practices and guarantee that States and non-State actors use the technology in legitimate ways.

However, *even if* an adequate human rights framework is set in place for the cooperation between State and surveillance technology companies, we are yet again left with serious challenges to the right to privacy and the protection of personal data which are examined in the following Section.

Privacy and data protection challenges form an inherent part of the technology

Whilst rigorous control and legislation and an explicit human rights impact assessment in the design, development, purchase and deployment of the technology *may* theoretically solve (or minimise) the challenges related to non-discrimination and unregulated State-company cooperation in the area, the issues related to privacy are harder to solve.

Facial recognition technology captures the unique facial features of individuals. This type of data is categorised as biometric data and the use of this (for *verification, identification or categorisation*) is inherent in the technology.

This use of biometric data fundamentally changes the nature of the surveillance – in fact, that is the entire point of the technology. The UN Human Rights Commissioner has described it as a paradigm shift compared to regular CCTV, as it dramatically increases the capacity to identify individuals. This, the Commissioner stated, is particularly problematic if live facial recognition technology is deployed, permitting real-time identification as well as targeted surveillance and tracking of individuals.[30]

The former Article 29 Data Protection Working Party (now replaced by the European Data Protection Board) under the EU stated in its Opinion 4/2007 on the concept of personal data (p. 8) that a particularity of biometric data is that they can be considered both as content of the information about a particular individual (this is the facial features of person X) as well as an element to establish a link between one piece of information and the individual (these facial features correspond to person X who is thus

30 UN Human Rights Commissioner, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peace protests, 24 June 2020, A/HRC/44/24

identified). As such, they can work as "identifiers". This dual character simultaneously provides information about the human body and allows for identification of a person.

The collection of biometric data is protected in various rules within international human rights law and European law: police use of biometric data is covered both by the right to privacy and the protection of personal data.

The right to privacy follows *inter alia* from Article 17 of the International Covenant on Civil and Political Rights and is furthermore protected in Article 8 of the European Convention on Human Rights. The right is also protected in Article 7 of the EU Charter of Fundamental Rights.

The right is penned out in detail in Article 8 of the European Convention on Human Rights (and other rules generally provide the same scope of protection). The provision entails that there is no interference with the right by a public authority except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. With smaller variations, this generally entails a threefold test of i) Legitimacy, ii) Necessity and iii) Proportionality.

The protection of personal data will in most instances, where police collect the data, be covered by the right to privacy. However, a specific protection of personal data also follows from Article 8 of the EU Charter of Fundamental Rights pursuant to which everyone has the right to protection of personal data concerning themselves. The data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or on a legitimate basis laid down by law.

Furthermore, the Council of Europe's Convention 108+ (a modernised version of Convention 108) on the Protection of Individuals with Regard to Processing of Personal Data provides certain rights. In Article 6 it states that the processing of e.g. biometric data that uniquely identifies a person is allowed only where appropriate safeguards are enshrined in the law. Additionally, Article 6 states that such safeguards must guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the individual, notably a risk of discrimination.

In relation to personal data collected by the police in particular, the EU Directive on the processing of personal data for the purposes of the prevention, investigation,

detection or prosecution of criminal offences, sets forth certain rights for individuals as well. In a somewhat similar manner as Convention 108+, it follows from Article 10 of the Directive that the processing of e.g. biometric data for the purpose of uniquely identifying an individual is only allowed where it is strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject. Furthermore, processing is only allowed where authorised by law; to protect the vital interests of the data subject or of another person; or where the processing relates to data which are manifestly made public by the data subject.

So, whilst no rules regulate the use of facial recognition technology by the police explicitly, the fundamental human rights rules of course all apply. This leaves us with the question whether police use of the technology is in accordance with these rules or not.

As mentioned in Section 3, insofar as the technology is flawed (irrespective of whether it is in addition to that also discriminatory), it would not meet the criteria of adequacy which is a prerequisite for any interference with the right to privacy to be lawful. Thus, a technology which interferes with the right to privacy and has an error rate which makes it inadequate for achieving the legitimate aim (which in this case would be law enforcement), would violate the right to privacy as it would not meet the conditions of the threefold test.

If we assume that the technology could with time be refined or developed in such a manner that its error rate would diminish, two main distinctions need to be made: is the technology used for mass surveillance[31] capturing the biometric data of everyone irrespective of whether the individuals are under suspicion? Or is the technology used on one or more specific individuals e.g. functioning as watchlists or deployed for manhunts?

Depending on how facial recognition is used, it may lead to more or less intensive interferences with the right to privacy. The more intensive the interference, the more compelling the justification for applying such a measure needs to be.

As mentioned above, the European regional courts have not ruled on the use of facial recognition technology yet. The courts have, however, ruled on police use of mass surveillance by other technological means:

31 See more on mass surveillance in the judgment by the European Court of Justice in Joined Cases C-203/15 and C-698/15, Tele2 Watson, 21 December 2016

The European Court of Justice has stated that general and indiscriminate retention of data on citizens may lead to a violation of the right to privacy. Legislation which allowed mass surveillance of electronic communications for fighting crime violated the right to privacy and the right to data protection according to the Court.[32] Currently, a number of cases are pending before the Court on the consequences of this landmark ruling on mass surveillance.[33]

The European Court of Human Rights has stated that secret surveillance of citizens by the authorities is only compatible with human rights law if the surveillance is strictly necessary and that the mere threat of surveillance, even when secret, coupled with a lack of remedy, can constitute an interference with the right to privacy.[34] Additionally, a number of cases regarding mass surveillance (by bulk interception into communication) are pending before the Court.[35]

Taking into consideration the invasive nature of the technology – including risks related to how and when biometric data is captured and stored – it is not an unlikely outcome that the European courts may find mass surveillance based on facial recognition technology unlawful.[36] This assumption is further supported by the chilling effect which mass surveillance by facial recognition technology may give rise to (see more on this below).

The second question; whether the technology may be used to help locate individuals on watchlists or during manhunts, cannot be answered as simply.

---

32 Judgment by the European Court of Justice in Joined Cases C-203/15 and C-698/15, Tele2 Watson, 21 December 2016, paragraph 100.

33 See Case C-623/17, joint cases C-511/18 and C-512/18, case 520/18 and case C-746/18.

34 See judgment by the European Court of Human Rights in the case of Rotaru v. Romania, 4 May 2000, paragraph 47 and para. 171. See also A/HRC/27/37, para. 20.

35 See an overview of the Court's case law, including pending cases, in the European Court of Human Right's Factsheet on Mass Surveillance, September 2019.

36 On the illegality of the technology for mass surveillance see Overview on Facial Recognition to Combat Crime, Danish Institute for Human Rights, December 2019 available here: https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/udgivelser/overblik_ansigtsgenkendelse_uk_02.pdf and European Digital Rights (EDRI) report, "Ban Biometric Mass Surveillance – a set of fundamental rights demands for the European Commission and EU Member States on the use of technology for the untargeted mass processing of special categories of personal data in public spaces" May 2020. See also European Union Fundamental Rights Agency in "Facial Recognition Technology: fundamental rights considerations in the context of law enforcement" November 2019

In these cases, principles related to necessity, adequacy and proportionality of the interference may lead to different degrees of risk of violation and a number of factors will in and of themselves or taken together provide different outcomes. These factors include whether there are adequate legal safeguards in place to prevent unlawful interferences; whether the technology is used to solve serious crimes or minor offences; whether the use of facial recognition technology will be restricted in terms of time and geographical location or be generally available to the police. Indeed, the assessment would also take into account whether there is a risk of security breach or other risks related to the cooperation between State and companies mentioned in Section 4.

To sum up, the answer to the second question cannot be given clear-cut but will depend on a case-by-case basis. For this reason, certain minimum guarantees have been suggested by various actors.[37] Such guarantees include, e.g. systematic human rights due diligence before deploying the technology and throughout the entire life cycle of the tools and effective, independent and impartial oversight mechanisms for the use of facial recognition technology.

The risk of a chilling effect on the freedom of assembly

A consequence of the considerable interference with the right to privacy is that it can create a chilling effect on other rights, most notably freedom of assembly.[38] Freedom of assembly is protected under Article 21 of the International Covenant on Civil and Political Rights, Article 11 of the European Convention on Human Rights as well as Article 12 of the European Union's Charter of Fundamental Rights.

Intensive surveillance by the police with the use of facial recognition technology during a demonstration, can potentially reveal information about individuals, including sensitive data such as their political affiliation and thus create a so-called chilling effect on individuals' willingness to take part in demonstrations.

Most recently, the UN Human Rights Commissioner recommended never to use facial recognition technology to identify those who are peacefully participating in an

37 European Union Fundamental Rights Agency in "Facial Recognition Technology: fundamental rights considerations in the context of law enforcement" November 2019; UN Human Rights Commissioner, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peace protests, 24 June 2020, A/HRC/44/24; and Overview on Facial Recognition to Combat Crime, Danish Institute for Human Rights, December 2019

38 UN Human Rights Commissioner, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peace protests, 24 June 2020, A/HRC/44/24

assembly. Furthermore, it was recommended that States refrain from recording footage of assembly participants, unless there are concrete indications that participants are engaging in, or will engage in, serious criminal activity, and such recording is provided by law, with the necessary robust safeguards. Lastly, the Commissioner recommended a moratorium on the use of facial recognition technology in the context of peaceful assemblies, at least until the authorities responsible can demonstrate compliance with privacy and data protection standards as well as the absence of significant accuracy issues and discriminatory impacts.[39]

The UN Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association has stated that the use of surveillance techniques for arbitrary surveillance of individuals exercising their freedom of assembly should be prohibited. This is because identification and data collection rule out the possibility of anonymity in public spaces and can have a chilling effect on the willingness to take part in public assemblies. For example, citizens may fear that their participation will be registered in a police database. The Special Rapporteur notes that this chilling effect may be aggravated if the demonstration concerns views that differ from the majority view.[40]

These chilling effects are present if the technology is used for mass surveillance (rather than for locating a specific individual). As mentioned above, mass surveillance gives rise to serious concerns based on privacy alone. However, these concerns are amplified, when the concern of chilling effect is added to the matter. This makes it very hard to imagine that the technology could be deployed for mass surveillance in a manner which would not violate the rights and freedoms of individuals.

Concluding remarks and perspectives

There are compelling arguments for deeming the use of facial recognition technology as a violation of human rights law, especially when the cumulative sum of adverse effects on non-discrimination, privacy and freedom of assembly as well as problems related to State-company cooperation are taken into account. The case of Hikvision shows that the technology and its challenges are global. However, law does not provide a clear-

39 UN Human Rights Commissioner, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peace protests, 24 June 2020, A/HRC/44/24

40 The United Nations Human Rights Council, "Rights to freedom of peaceful assembly and of association - Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", 17 May 2019, A/HRC/41/41, items 56- 57 and 76

cut answer in terms of the illegality of the technology which cannot be said to violate human rights *per se*.

Nevertheless, it is true that the use of the technology for *mass surveillance* technology, for example, in demonstrations, can hardly be in accordance with human rights. Whilst no judicial review on a European or international level has yet been undertaken, it may also be assumed based on the provisions in the international human rights framework as well as case law from the European courts that use of *flawed* facial recognition technology with high error rates will most likely amount to violations of the right to privacy and the protection of personal data. In other than these cases, the answer is somewhat murky and rests on whether sufficient safeguards are ensured.

This lack of clarity calls for caution. The fact that not all police use of the technology is illegal *per se* should not necessarily be an argument towards introducing the technology but rather an argument for States to tread carefully so long as the wide-reaching human rights implications of the technology cannot be mitigated, and sufficient safeguards cannot be ensured. This is particularly the case because law enforcement plays a crucial role in society and entails intensive use of public authority. Furthermore, facial recognition technology changes the nature of surveillance as it dramatically increases the capacity to identify individuals in the public space.

On a more ethical level, the enhanced surveillance by facial recognition technology can put into question the very concept of identity (Bauman and Lyon, 2013; Lyon 2008; Murakami Wood 2003; Hayles 2003) which will serve as a concluding perspective here: Biometric data is data *about* us but does not comprise the entirety of our being. This distinction risks being lost e.g. when States control populations and regulate bodies through *classification* or by extensive and constant *identification* in the public space. David Lyon, an expert on surveillance societies puts it this way: "Surveillance contributes to how the state 'sees' its citizens […]. Surveillance processes thus contribute to […] the 'disappearance of disappearance' as being 'invisible' (or anonymous for that matter) in a surveillance-saturated world becomes increasingly difficult. Biometrics takes this process even further, implicating 'body data' in the surveillant visibility of 'who we are' at a very basic but highly consequential level" (Lyon 2008).

Consequently, the intensity and ubiquitous manner of biometric surveillance can risk fundamentally altering the nature of the public sphere creating monumental changes in society which are not easily mitigated. Such changes need to be identified and addressed before deploying the technology any further.

Bibliography

Barrett, L. F., Adolphs, R., Marsella, S., Martinez, A. M., & Pollak, S. D. (2019). Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements. Psychological Science in the Public Interest, 20(1), 1–68.

Bauman, Zygmunt and David Lyon (2013) Liquid Surveillance: A Conversation, Polity Press.

Bradford, Ben, Yesberg, Julia A, Jackson, Jonathan and Dawson, Paul (2020), Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology, The British Journal of Criminology.

Buolamwini, Joy and Gebru, Timnit (2018) "Gender shades: intersectional accuracy disparities in commercial gender classification", Proceedings of Machine Learning Research, vol. 81 (2018), pp. 1–15.

Grabenwarter, Christoph (2014) The European Convention for the Protection of Human Rights and Fundamental Freedoms: A commentary, Hart Publishing

Hayles, N. Katherine (2009) RFID: Human Agency and Meaning in Information-Intensive Environments, Theory, Culture, and Society 26(2/3):1-26.

Jensen, S (2016) The Making of International Human Rights: The 1960s, Decolonization, and the Reconstruction of Global Values: Cambridge University Press.

Krahulcova Lucie (2017) The European Parliament is fighting to strengthen the rules for surveillance trade, Access Now, 8 December 2017.

Lagoutte, S., Gammeltoft-Hansen, T., Cerone, J., (2016) Tracing the Roles of Soft Law in Human Rights, Oxford: Oxford University Press.

Lenaerts, Koen (2003) Interlocking Legal Orders in the European Union and Comparative Law, International and Comparative Law Quarterly.

Lyon, David (2008) Biometrics, identification and surveillance. Bioethics. 22. 499-508

Moßbrucker, Daniel (2018) "Surveillance exports: how EU Member States are compromising new human rights standards", netzpolitik.org, 29 October.

Murakami Wood, David (2003) Editorial: Foucault and Panopticism Revisited. Surveillance & Society 1 (3): 234-239.

Murray, D. (2020) Using Human Rights Law to Inform States' Decisions to Deploy AI. AJIL Unbound, 114, 158-162.

Pardes, Arielles (2018) "Facial Recognition Tech Is Ready for Its Post-Phone Future", 9 October 2018, Wired.

Raji, Inioluwa Deborah and Buolamwini, Joy (2019) "Actionable auditing: investigating the impact of publicly naming biased performance results of commercial AI products", Conference on Artificial Intelligence, Ethics and Society.

Stupp, Catherine (2018) "Nine countries united against EU export controls on surveillance software", Euractiv, 11 June.

Timan, Tjerk, Newell, Bryce Clayton and Koops, Bert-Jaap, (2017) Privacy in Public Space, Conceptual and Regulatory Challenges, Elgar Publishing