DECEMBER 2019

FACIAL RECOGNITION TO COMBAT CRIME

The Danish Institute for Human Rights recommends that the Danish government postpone the introduction of facial recognition to combat crime until we know the human rights consequences for the right to privacy, the right to the protection of personal data and the freedom of assembly. This memo provides a summary of the human rights issues involved.

Facial recognition is a particularly intensive and intrusive method, challenging the protection of privacy and of personal data. In the absence of necessary legal safeguards, facial recognition may pose a serious risk to rule of law. If used for mass surveillance, facial recognition methods could also potentially challenge the freedom of assembly.

Any use of facial recognition will aggravate human rights concerns currently associated with CCTV surveillance.

Right now, there are ongoing discussions and investigations of the human rights consequences of facial recognition technology in the EU, the Council of Europe, the UN[1] and in European countries which have allowed or have plans to allow the police (or other authorities) to use facial recognition technology. Neither the European Court of Justice nor the European Court of Human Rights has had the opportunity to review the legality of facial recognition. Consequently, we do not know under which circumstances use of facial recognition by the police will be legitimate.

Overall, legality depends on whether:

1. Adequate legal safeguards are in place to prevent unauthorised interference,
2. The technology is used to combat crime or for other public authority responsibilities,
3. Surveillance focuses on suspects or is used for mass surveillance,
4. The technology is used to solve serious crimes or minor offences,
5. The use of facial recognition is restricted in terms of time and geographical location, or is generally available to the police.

The Minister for Justice has said that facial recognition raises fundamental questions[2] and expects that, at some point, the Danish Parliament will discuss facial recognition.[3] Most recently, a proposal has been presented to the Danish parliament for a resolution to prohibit public authorities' use of facial recognition technology in public spaces.[4]

On this background, the Danish Institute for Human Rights recommends:

- that facial recognition technology not be used in police investigations and activities to combat crime until the far-reaching human rights consequences of the technology have been clarified and it is clear how these consequences are to be addressed.

- that facial recognition technology not be used in investigations and activities to combat crime for the purpose of collection, processing, etc. of biometric data on citizens who are not under suspicion.

The following provides a brief legal summary of the human rights issues that legislators should be aware of.

USE OF FACIAL RECOGNITION IN DENMARK AND ABROAD

China is one of the countries in which facial recognition is most widely used. Facial recognition is used commercially, for authorities' administrative tasks, and by the police. For example, facial recognition has just become mandatory in China when buying a SIM card. Combined with other surveillance technologies, this means that mass surveillance of the Chinese population is widespread. In the US, facial recognition is also widely used by the authorities. Recently, however, an increasing number of bans have been issued against facial recognition in individual states and cities. Most recently, California issued a ban against use of the technology by the police in body cameras over the next three years. In the EU, the use of facial recognition by the police has been tested, or is being tested, in the UK, France, the Netherlands and Germany. Most of these countries have tested the possibility of surveilling/tracking the movements and whereabouts of selected persons in public spaces. In Sweden, the police have just been granted pre-approval by the Swedish Data Protection Authority to use facial recognition to combat crime.

Today, Danish police use facial recognition to verify the identity of individuals in Copenhagen Airport. This measure only involves automation of existing airport border controls and is not part of police investigation of crime. Currently, the police do not use facial recognition technology in investigations or other activities to combat crime.[5]

Using facial recognition to verify a person's identity at an airport does not give rise to the same fundamental concerns as use of the technology to combat crime or for other police tasks.

HUMAN RIGHTS REQUIREMENTS FOR USE OF FACIAL RECOGNITION BY THE POLICE

Above all, facial recognition is an interference with the right to privacy and protection of personal data. Protection of privacy and personal data entails that interference with these rights is only acceptable if such interference is permitted by law, has a legitimate purpose and is otherwise proportionate with this purpose (proportionality).

Facial recognition technology uses citizens' biometric data. From the perspective of data protection law, biometric data is sensitive personal data, like DNA for example.

If the police use facial recognition to combat crime, section 10(1) of the Danish act on the processing of personal data by law enforcement authorities applies. This provision clearly states that the police are not allowed to process biometric data to identify a natural person.

However, derogations from this prohibition are permitted according to section 10(2) if the investigation or prosecution renders such derogations strictly necessary, cf. section 1(1). This means that use of the technology may be permitted in specific cases.

What is facial recognition?

Facial recognition is based on technology that captures biometric data to identify natural persons. The technology has many uses, ranging from comparing one image with one individual (so-called "one-to-one" comparison) to more general surveillance of citizens and comparison of facial images against large databases ("one-to-many" comparison). Facial recognition can be used to scan material on the internet and to surveil citizens in public spaces. The technology can be used without a person reviewing the material (fully automated), or by conducting human checks during or after the automated process.

Like any other technological tool used in police work, for example DNA analyses, even the most advanced facial recognition technology includes some margin of error. For example, the technology has been criticised for having particularly high error rates for women and people with a non-western appearance.[6]

Section 4(6) of the Danish act on the processing of personal data by law enforcement authorities states that collected data is not to be kept in a form which allows identification of data subjects for longer than is necessary for the purposes for which the data is being processed.

In combination with other information about the citizen, data collected using facial recognition technology may form detailed profiles. This applies to data on the internet, for example data collected via social media, as well as data in registers etc. available to the police. Collating all this data will enable the police to make highly accurate analyses of citizens' private lives.

The right to privacy

The right to respect for private life is 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. Article 8 of the Charter provides for protection of personal data. The Charter applies to collection of data by the police for police investigations, as this is regulated by the Danish act on the processing of personal data by law enforcement authorities, implementing the EU Directive protecting individuals with regard to the processing of their personal data by police and criminal justice authorities.[7]

JUDGMENTS ON SURVEILLANCE BY THE EUROPEAN COURT OF JUSTICE AND THE EUROPEAN COURT OF HUMAN RIGHTS

As mentioned above, intensive surveillance of citizens can generate knowledge about the activities and beliefs of individual citizens, including knowledge of sensitive personal data that is of no relevance for the purpose.

The European Court of Justice has stated that general and indiscriminate retention of data on citizens is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance.[8]

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.[9]

Consequently, the legality of police use of facial recognition technology overall depends on whether use of the technology in a specific case is proportionate, including whether any interference affords citizens the necessary safeguards.

PROPORTIONALITY REQUIREMENT

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

If the technology is used to combat crime, an important aspect is whether the surveillance is focused on one specific person under suspicion, or whether the technology is used for general surveillance of citizens in public spaces (mass surveillance).

Mass surveillance is surveillance not directed at one or more specific individuals, but rather surveillance to collect information in a general and indiscriminate manner.[10]

The assessment of proportionality also depends on the type of crime. The methods allowed to catch a bicycle thief differ from those allowed for a terrorist suspect.

Another aspect could be whether the use of facial recognition is restricted in terms of time and geographical location, including whether it is used for all or only selected surveillance cameras to which the police have access or can gain access, and whether the police can only use the technology in fixed cameras, or also in mobile cameras, drones, etc.

Furthermore, the proportionality assessment especially depends on whether adequate safeguards against unauthorised interference are in place.

LEGAL SAFEGUARDS REQUIREMENT

Police surveillance can be arbitrary if the use of such surveillance is not accompanied by specific and effective procedural safeguards. In particular, effective legal safeguards place demands on control, use, sharing and deletion of personal data.

These safeguards apply regardless of whether the surveillance concerns one specific person under reasonable suspicion, or whether the technology is used for general surveillance of citizens in public spaces (mass surveillance).

The European Court of Human Rights has established that, as a general rule, secret surveillance by the state should be subject to judicial control or other effective supervision in order not to violate Article 8 of the European Convention on Human Rights.[11]

The Court has stated that, in the absence of effective safeguards for surveillance, depending on the circumstances, the mere risk of being surveilled may cause interference with the right to respect for private life, without the citizen having to prove that he or she has actually been subject to surveillance.[12]

It also follows from the Article 8(3) of the EU Charter on Fundamental Rights that compliance with the rules on protection of personal data must be subject to control by an independent authority.

Any use of facial recognition will aggravate the due-process concerns associated with increased use of CCTV surveillance. In this connection, see the Institute's memo on the government's recent proposal on safety and security in public spaces which involves increasing access to CCTV surveillance.[13]

The use of biometric data brings into play other issues related to legal safeguards. For example, the risk of data on citizens "floating" across different purposes. There is a problem if data collected for the purpose of one - serious - type of crime is used to investigate another - less serious - type of crime. Similarly, legal safeguards must be in place to ensure that data collected in connection with tasks other than combatting crime cannot automatically be used in police investigations.

The European Court of Human Rights has stressed that any use of video footage or other photographic material used by the police must have a clear legal basis, in particular if the police use the material for purposes other than the purpose for which the material was originally collected.[14]

Challenges regarding rule of law caused by facial recognition should be seen in light of the increased use by the police of intelligence-led policing. An example of this is the use of POL-INTEL, an intelligence platform enabling the police to process massive volumes of data about individuals.[15] Data analysed using such tools cannot only be used for actual investigations; potentially, data can also be used for predictive policing, a technique by which the police can analyse data to predict potential criminal activity or unrest without any prior suspicion of a criminal offence.[16]

Furthermore, risks of security breaches and abuse increase when data is shared by police services across national borders, or when private players develop and sell surveillance technologies. In the worst case scenario, this may lead to sensitive data on citizens being sent to players other than the state.

These challenges have caused the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to propose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime is in place.[17]

FREEDOM OF ASSEMBLY AND FREEDOM OF EXPRESSION

Intensive surveillance by the police may potentially affect the freedom of assembly and, to some extent, the freedom of expression.[18]

Use of facial recognition technology, for example during a demonstration, can potentially reveal information about individuals, including sensitive data such as their political affiliation.

Freedom of assembly
The freedom of assembly is protected under Article 11 of the European Convention on Human Rights and in section 79 of the Constitutional Act of Denmark. It gives everyone the right to freedom of peaceful assembly with others for any lawful purpose.

UN WARNINGS AGAINST FACIAL RECOGNITION

The UN Special Rapporteur on the rights to freedom of peaceful assembly and of association as well as the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression[19] have warned against the use of facial recognition technology.

The 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 citizens' willingness to take part in public assemblies.[20] 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.[21]

Today, it is legal for the police to stay informed about how a demonstration is proceeding and to maintain a certain control. In this connection, the police use video footage, for example to document police intervention and suspicious behaviour of individuals in large assemblies.[22] Furthermore, in Denmark, wearing masks during demonstrations is illegal according to section 134b of the Danish Penal Code.

However, facial recognition implies such an intensification of surveillance that, in the assessment of the Danish Institute for Human Rights, it differs fundamentally from usage of regular video footage or the intention behind the ban on face covering in section 134b

of the Danish Penal Code. The technology reveals sensitive information and affects far more people than is permitted by the legislation currently in force. This challenges the principle of proportionality.

END NOTES

1 See in particular: https://fra.europa.eu/sites/default/files/fra_uploads/ fra-2019-facial-recognition-technology-focus-paper.pdf , https://rm.coe. int/0900001680973a5d and https://undocs.org/A/HRC/41/35

2 Reply to section 20 question no. S 190, 31 October 2019, available (in Danish) here: https:// www.ft.dk/samling/20191/spoergsmaal/s190/index.htm

3 Reply to section 20 question no. S 288, 20 November 2019, available (in Danish) here: https:// www.ft.dk/samling/20191/spoergsmaal/s288/index.htm

4 B 46 Proposal for parliamentary resolution to ban public authorities' use of facial recognition technology in public spaces, presented on 27 November 2019, available (in Danish) here: https://www.ft.dk/samling/20191/beslutningsforslag/B46/som_fremsat.htm

5 See in particular the final reply to question 926 from the Legal Affairs Committee, 21 August 2018, available (in Danish) here: https://www.ft.dk/samling/20171/almdel/reu/spm/926/index. htm and the final reply to question 927 from the Legal Affairs Committee, 21 August 2018, available (in Danish) here: https://www.ft.dk/samling/20171/almdel/reu/spm/927/index. htm

6 See for example the Essex University report from June 2019 available here: https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/ uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report. pdf and the European Union Agency for Fundamental Rights report on facial recognition technology, December 2019, available here: https://fra.europa.eu/sites/ default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper. pdf

7 See Act no. 410 of 27 April 2017 on the processing of personal data by law enforcement authorities, available (in Danish) here: https://www.retsinformation.dk/ Forms/R0710.aspx?id=189891#id4f473848-6de6-4956-bd58-2252db5363a7.

8 Judgment by the European Court of Justice in Joined Cases C-203/15 and C-698/15, Tele2 Watson, 21 December 2016, paragraph 100, available here: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5417450

9 See judgment by the European Court of Human Rights in the case of Rotaru v. Romania, 4 May 2000, paragraph 47, available here: http: //hudoc.echr.coe.int/eng?i=001-58586

10 See for example judgment by the European Court of Justice in Joined Cases C-203/15 and C-698/15, Tele2 Watson, 21 December 2016, available here: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5417450 or the Council of Europe factsheet on mass surveillance, available here: https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e

11 See judgment by the European Court of Human Rights in the case of Rotaru v. Romania, 4 May 2000, paragraph 57ff, available here: http://hudoc.echr.coe.int/eng?i=001-58586

12 See judgment by the European Court of Human Rights in the case of Klass v. Germany, 6 September 1978, paragraph 38, available here: http://hudoc.echr.coe.int/eng?i=001-57510

13 The Institute's memo and news article are available (in Danish) here: https://menneskeret.dk/nyheder/regeringens-sikkerhedsudspil-begraenser-borgernes-frihedsrettigheder.

14 See judgment by the European Court of Human Rights in the case of Peck v. the United Kingdom, 28 January 2003 (44647/98), paragraphs 61-62 available here: https://hudoc.echr.coe.int/eng#{"itemid":["001-60898"]} as well as Perry v. the United Kingdom, 17 July 2003, paragraphs 47-48, available here: https://hudoc.echr.coe. int/eng#{"itemid":["001-61228"]}

15 See consultation response from the Danish Institute for Human Rights of 9 March 2017 about police use of tools for data analysis, etc., available (in Danish) here: https://menneskeret.dk/sites/menneskeret.dk/files/03_marts_17/hoeringssvar_til_udkast_til_forslag_til_lov_om_aendring_af_politiets_virksomhed_og_toldloven. pdf

16 See the final reply to question no. 52 from the Legal Affairs Committee, including a review of intelligence-led and predictive policing, 25 November 2016, available (in Danish) here: https://www.ft.dk/samling/20161/almdel/reu/spm/52/svar/1362234/1693008/index.htm

17 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, available here: https:// undocs.org/A/HRC/41/35

18 See for example the United Nations Human Rights Council, "The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights", 30. June 2014, A/HRC/27/37, available here: https://www.ohchr. org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_ en.pdf

19 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, available here: https:// undocs.org/A/HRC/41/35

20 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, available here: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/ HRC/41/41

21 Ibid.

22 Final reply to question 388 from the Legal Affairs Committee, 29 October 2019, available (in Danish) here: https://www.ft.dk/samling/20182/almdel/reu/spm/388/index.htm