2021.01.05

AI-REGULATION.COM

The Surveillance Camera Commissioner's new guidance on the use of Live Facial Recognition

BECUYWE Mathias

To cite this article:

BECUYWE Mathias, The Surveillance Camera Commissioner's new guidance on the use of Live Facial Recognition, Chair Legal and Regulatory Implications of Artificial Intelligence, MIAI Grenoble Alpes, 2021, January 5th.

AI-Regulation.com

CHAIR LEGAL AND REGULATORY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE

The UK Surveillance Camera Commissioner (SCC)[1] released a new report in November 2020 entitled "Facing the Camera". It aims to provide "good practice and guidance for the police use of overt surveillance camera systems incorporating Facial Recognition Technology to locate persons on a watchlist, in public places in England & Wales". It is an important report as it represents the first guidelines issued by a governmental body since the Bridges decision. Indeed, just as the deployment of Live Facial Recognition (LFR) is increasing in the UK, the London Court of Appeal has ruled that an operation using LFR conducted by the South Wales Police was unlawful. As Tony Porter, the Surveillance Camera Commissioner, noted, the Court made it clear in its judgment that the use of LFR in this case was adjudged to be unlawful, but this did not mean that the technology is generally unlawful. The SCC's new report therefore proposes measures that intend to establish good practice to ensure that future use of Live Facial Recognition in England and Wales is in accordance with the law.

After presenting the main features of the report, the focus will be on the answers it provides to the specific questions raised by the Court of Appeal in London in August 2020.

1. What does this guidance contain?

In Tony Porter's own words, these guidelines are more detailed than those contained in the previous version of the SCC document dated March 2019, and are not limited to what is required by law but go further in terms of providing guidelines for best practice. This substantial document consists of six parts, subdivided into forty-three more specific sections:

1. Biometrics, Equality and Ethics
2. Human Rights, 'In Accordance with the Law' and The Legal Framework
3. Governance, Approval, Watchlists, Protected Characteristics and the Human Decision Maker
4. Integrity, Use of Material as Evidence and Handling of Material
5. Public Engagement, Provision of Information, Performance
6. Accountability and Certification

The intention here is not to repeat all the points highlighted by the SCC report, but it is interesting nevertheless to look at the notion of necessity, which is clarified from point 3.75 onwards (page 33). The document duly states that in order to meet the requirements of the European Human Rights Convention (ECHR), the ways in which LFR is used must take into account the protection of human rights where deployments are likely to interfere with protected rights. Therefore, to meet such requirements, deployments must be "convincingly established and transparently set out". In order to abide by good practice, there must therefore always be a legitimate interest in, and pressing need for, the use of LFR.

[1] The SCC is a government authority responsible for encouraging compliance with the Camera Code of Practice. It is part of the oversight mechanisms provided for in the Protection of Freedoms Act 2012 along with the Information Commissioner Office which is the UK's data protection authority.

It is therefore recommended that for each deployment, the reasons for the need to use the LFR for the identified problem should be stated. Going further, the report considers it important that the police explain why "operational conduct is considered necessary rather than simply desirable, convenient, or is otherwise borne out of no other reason than having the technical capability at their disposal".

After a detailed analysis of all the elements that the SCC considers to be crucial, the document provides a summary of its 11 recommendations in its annex:

1. The establishment by the Home Office of:
    a. A national procurement strategy which provides the right tools and engenders public confidence;
    b. A means by which the credentials of LFR technology can be suitably analysed and assessed so as to determine risks;
    c. National standards for future procurement, decision-making around acquisition and deployment of equipment, and the empowerment of police to comply with risk assessment obligations.
2. The development by the police of mechanisms which provide for meaningful and independent 'ethical oversight' of police decision-making and operational conduct.
3. The development by the Home Office and Other Stakeholders of a single 'integrated impact assessment' process which provides for a comprehensive approach.
4. The assessment of procured or deployed or planned systems with regard to known vulnerabilities, or a history of vulnerabilities that may lead to a risk that the equipment could be 'hacked'.
5. A review of the laws which govern the conduct of overt surveillance by the police where such surveillance employs biometric or similarly intrusive technology.
6. A review and update of the Surveillance Camera Code of Practice.
7. The inclusion in the two aforementioned reviews of clear provisions for ethical standards, equality, legality and the governance and accountability of operational and intrusive conduct.
8. The development by the National Police Chiefs Council (NPCC) and the Home Office of consistent approval and decision-making structures which approve the conduct of police operations that specifically use LFR. This strategic and operational decision-making should be provided by an officer of an appropriately senior rank who is not engaged in the day-to-day direction of the operation in which LFR is used.
9. The consideration by the College of Policing and the NPCC of whether at a national level, the role of the human decision maker should be better defined, "structured" within a surveillance camera system, and/or would benefit from further nationally produced guidance or training.
10. The development by the NPCC of a meaningful and national suite of relevant performance indicators which demonstrate at a minimum, the purpose, outcome, nature and extent of intrusion, accuracy and diversity of impact of their LFR operations, and whether or not they were successful.
11. The development by the police of a nationally consistent terminology that can be applied to the use of LFR systems.

2. Cross-referencing this guide with the 'Bridges' decision

In the 'Bridges' decision of August 11, 2020, the Court of Appeal in London considered that there were three factors which established that the use of LFR by the South Wales Police was unlawful: the lack of legal basis for the processing of data [2.1], non-compliance with the data protection impact assessment (DPIA) obligations contained in the Data Protection Act [2.2] and finally non-compliance with the non-discrimination obligation laid down by the Public Sector Equality Duty (PSED)[2.3]. An analysis of the differences between the guidelines provided by the SCC's report and the main points raised by the Court of Appeal could be interesting since the SCC explicitly references it to explain the new guidelines.

2.1 The legal basis for the processing of data

The Court noted in its decision that the legal basis for the processing of data was insufficient because the use of LFR conferred too much discretion to police officers both in terms of drawing up watchlists of the intended targets (the Who question) and determining exactly where the LFR would be deployed (the Where question).

The 'Who Question'

The SCC guide highlights that, in order to ensure appropriate safeguards for the rights of individuals, policies should be implemented that explain "decisions as to how additions to and removals from the watchlist are managed" (page 41). It also proposes that these policies should be made public and updated over time.

Whilst reminding us that it would prefer not to have a watchlist reused in different deployments, the SCC draws up a list of individuals who would be likely to be placed on a watchlist:

- Individuals wanted by the police for arrest on suspicion of an offence;
- Individuals wanted for arrest because of a warrant issued by the courts;
- Vulnerable persons who are sought by the police because of the risk they pose;
- 'Persons of specific police interest', information about whom the police refer to as being 'for intelligence purposes.'

It is the latter category of individuals that poses the greatest risk in terms of the police taking discretionary action, which is the main reason why the SCC provides more details about this issue. The SCC points out that these 'specific interest' individuals are likely to be unaware that information is being collected about them because a 'positive match' may not result in immediate action by the officers. There is therefore a risk of moving from 'overt' to 'covert' surveillance, which would require a surveillance authorization. This is why the SCC is strongly in favour of legal advice being provided each time that LFR technology is deployed. This approach would consequently ensure that the surveillance in question does not fall within the scope of 'covert' surveillance. The SCC therefore states that policies should be transparent and provide appropriate safeguards to determine "whether or not there is a legitimate information requirement the nature of which makes the use of LFR necessary and proportionate in those circumstances".

Finally, the SCC acknowledges that LFR may sometimes be used to locate an individual who is not suspected of committing a crime yet locating them would prevent or detect a crime, or protect an individual from harm. For this type of use, the SCC supports case-by-case assessment in which “the relevant circumstances should be of such seriousness as to justify the intended police conduct as being lawful, necessary and proportionate to what the police are seeking to achieve by means of LFR”.

The ‘Where Question’

Although the SCC recognises that officers' discretion in the choice of deployment location is a key issue, the guidelines are not as detailed for the 'Where Question' as they are for the 'Who Question'. It should be noted, however, that according to the SCC, the decision on where, or whether, to deploy LFR must be based on transparent policies and the establishment of appropriate safeguards by the police authorities (page 41), while at the same time relying on the advice of legal advisers to the police in the field. This 'Where Question' therefore appears to be part of the development of an approval structure for LFR deployments suggested in recommendation 11 of the guide.

Finally, in terms of 'overt' surveillance, the guide stresses the importance of informing the public about the deployment in progress. This information and transparency about the use of LFR is, according to the guidelines, of major importance in creating trust between individuals and the equipment used by the police (point 6.6). Whilst recognising that the police may need to act with a certain degree of confidentiality, this need “should be based on reasonable grounds and not on grounds of operational convenience”. The SCC also states “that decisions as to confidentiality are capable of being held to account by relevant third-party scrutiny where necessary” (point 6.7) and that information on arrangements “which enable the public to challenge any aspect of the police conduct” should be provided.

2.2 Data Protection Impact Assessment (DPIA)

In its 'Bridges' decision, the Court of Appeal in London identified that the DPIA had been incorrectly carried out for LFR deployment since it “failed properly to assess the risks to the rights and freedoms of data subjects and failed to address the measures envisaged to address the risks” (para. 153).

The SCC reaffirms the need to carry out a DPIA before each deployment of the technology (point 3.3). Given the risks to a number of fundamental rights, the SCC advocates that an “assessment of risk, including an assessment of intended and collateral intrusion, together with the identification and implementation of risk management measures, should be conducted and documented as part of police policy”. To put this into practice, the paper calls for the “creation of publicly available policies which set out the safeguards for police discretion”.

In order to ensure that a proper assessment is carried out that takes into account the risks of, and adequate protection measures needed for the deployment of LFR , the SCC refers in particular to the guide and template it provides on its website. In this DPIA implementation guide, the SCC highlights in point 14 which rights may be threatened by the use of cameras in general and facial recognition in particular (for instance, the right to freedom of assembly or freedom of thought, belief and religion). The guide also highlights that risk assessments must be conducted in accordance with two criteria: the likelihood of damage occurring and the likely seriousness of this damage. Consequently, "high risk could result from either a high probability of some harm, or a lower possibility of serious harm".

The template proposed by the SCC provides practical support for carrying out DPIAs and addresses the issue of risks and ways to reduce them. The last three sections of the template help to identify the risks, then to address them and finally, in the event that the risks cannot be mitigated, a procedure is foreseen for approval of the DPIA by the Information Commissioner Office (English Data Protection Authority).

2.3 Public Sector Equality Duty (PSED)

The Court of Appeal in London highlighted in August 2020 that although there was no evidence that the algorithm used in the challenged deployment of the LFR was biased (in particular in terms of race or gender), it was incumbent on the authorities to take a proactive approach to tackling discrimination. Indeed, in accordance with the obligations laid down by the Public Sector Equality Duty (PSED), the Court had noted that this obligation "requires the taking of reasonable steps to make enquiries about what may not yet be known to a public authority about the potential impact of a proposed decision".

The Court considered that a human review of algorithmic decisions before any intervention with an individual was not a sufficient guarantee of compliance with the PSED (para. 185). The Court also relied on the expertise of Dr Jain, Professor at the Department of Computer Science and Engineering at Michigan State University, who highlighted the necessity of accessing the technical training characteristics of the deployed algorithm in order to assess its possible biases (para. 198). The Court of Appeal therefore linked compliance with the PSED to proactive action, notably with regard to the technical characteristics of the algorithm used, to ensure that certain groups were not being discriminated against before and during LFR deployment.

The SCC guide therefore addresses this issue in section 2. The SCC begins by welcoming the evolution of datasets used for training of Facial Recognition Technologies, which is, according to him, showing positive results in eliminating bias. Subsequently, it echoes the reasoning of the Court by reminding us that a human review alone cannot constitute a guarantee of the kind proposed by the PSED, whilst highlighting that the PSED applies not only to LFR software but also to human agents monitoring the system. The guide continues to follow the reasoning of the Court of Appeal by highlighting that the PSED is a constant process and highlights the 6 principles that govern it:

a) The PSED must be fulfilled before and during the time when a particular policy is being considered
b) The duty must be exercised in substance, with rigour, and with an open mind. It is not a question of ticking boxes
c) The duty is non-delegable
d) The duty is ongoing
e) If the relevant material is not available, there is be a duty to acquire it and this will frequently mean that some further consultation with appropriate groups is required
f) Providing that the court is satisfied that there has been a rigorous consideration of the duty, so that there is a proper appreciation of the potential impact of the decision on considerations around equality, then it is for the decision-maker to decide how

The SCC points out that compliance with the PSED with regard to LFR takes place in particular at the time of acquisition of the technology (point 2.14). This recommendation calls on police authorities to negotiate with suppliers to acquire access to the relevant data necessary to carry out and perform system auditing. Noting the difficulties that may arise out of opposition between the PSED and the protection of intellectual property, the SCC insists that police authorities should not limit its action to the manufacturer's refusal to provide technical information on the algorithm. When audits cannot be completed and have taken "all reasonable steps to understand any risks of inconsistency which occurs within the software", the SCC states that "the police should be able to justify how their policies, decision making and conduct takes account of such risks and how they are to be satisfactorily mitigated". In the end, "if the technology cannot be deployed in a manner whereby the PSED has not or cannot be discharged then it should not be used".

It is therefore in this context, and in order to ensure the effectiveness of the PSED within the framework of LFR, that the SCC formulates proposal number 1:

The establishment by the Home Office of:

a. A national procurement strategy which provides the right equipment and engenders public confidence;
b. A means by which the credentials of LFR technology can be suitably analysed and assessed so as to determine risks;
c. National standards for future procurement, decision-making around acquisition and deployment of equipment, and the empowerment of the police to comply with risk assessment obligations.

These statements are attributable only to the author, and their publication here does not necessarily reflect the view of the other members of the AI-Regulation Chair or any partner organizations.

This work has been partially supported by MIAI @ Grenoble Alpes, (ANR-19-P3IA-0003)