February 20th, 2020

AI-REGULATION.COM

Assessing the Use and Impact of Facial Recognition Technologies (CPDP 2020 Highlights)

BECUYWE Mathias

To cite this article:

BECUYWE Mathias, *Assessing the Use and Impact of Facial Recognition Technologies (CPDP 2020 Highlights)*, February 20th, 2020, https://ai-regulation.eu/assessing-the-use-and-impact-of-facial-recognition-technologies/

AI-Regulation.com
CHAIR LEGAL AND REGULATORY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE

Facial recognition technologies have become central to the interests and concerns of governments, citizens and the private sector alike. In Europe, many countries are seriously considering the use of facial recognition technologies, with the United Kingdom leading the way. The use of live facial recognition in the public space provides a dense legal agenda. It is for this reason that a panel on the issue was organized at the CPDP 2020. This panel, made up of both institutional actors and human rights organizations, addressed the issue by focusing on the impact that facial recognition technologies can have on citizens based on the use made by the police in the United Kingdom.

1. ACCORDING TO THE SCC: LEGITIMATE USE BUT INSUFFICIENT LEGAL FRAMEWORK

The first panelist was **Tony Porter, the Surveillance Camera Commissioner (SCC) in the United-Kingdom (UK).** He recalled the context in which facial recognition was introduced in the UK. He declined to discuss the general issue of banning, or not, this technology and focused instead on specific issues such as: surveillance, data protection or data transfer.

He recalled that, as legal advisor, he had defended the use of facial recognition by the South Wales Police. Indeed, on the occasion of a case before the High Court, he had argued that in this particular case, the use of this technology was justified and permitted by law. According to him, the use of facial recognition in this case complied with all relevant rules (Data Protection Act, Protection of Freedoms Act and Common Law). He welcomed the fact that the High Court validated this reasoning but, nevertheless, he emphasized that this decision only applied to the facts in this specific case: the legality of the use of facial recognition has to be **assessed on a case-by-case basis** without presuming global authorization.

Indeed, his main concerns were that **the legislation is not clear enough** but also that police officers find themselves into situations where they do not know whether their actions were legal or not. In his view, the use of facial recognition by the police is legitimate, but the underlying infrastructure – such as police training, transparency of algorithms, or legal framework – is not sufficient enough. This framework is crucial as citizens are mistrustful of this surveillance technology that threatens their privacy.

He acknowledged the fact that the decision in Bridges case set out guidelines. Tony Porter mentioned, without further details, that courts had ordered to “stop the use of facial recognition at five occasions when they considered it necessary”.

He concluded his intervention by relaying a discussion he had had with various government’s politicians. The Commissioner thus pleaded for a change in legislation in favour of clearer and more transparent texts that would take into account three major points: a fundamental review of oversurveillance, a judicial oversight and the need of confidence of the public.

2. THE ICO SEES ITSELF AS AN AUTHORITY BOTH IN CONTROL AND IN GUIDANCE

The next speaker was **Steven Wright**, who works in the **Information Commissioner's office (ICO)**, which is the UK's Data Protection Authority. He reviewed the state of usage and legislation of FRTs in the United Kingdom. Facial recognition is used by the public and private sectors, for law enforcement purposes, in shopping centers or football stadiums but also in public spaces. This diversity means that many different legal bases have to be taken into account.

For the private sector, this technology is attractive for commercial purposes. Nonetheless, **it must be legal, necessary, justified and proportionate**. For police forces using these technologies to fulfill their duty, **a balance between privacy protection and surveillance technologies must be reached**. For this reason, police must provide strong evidence that Automated Facial Recognition (AFR) is strictly necessary, balanced and effective in each specific context.

While recognising that processing of sensitive data is, in principle, prohibited, he stressed that the Data Protection Act 2018 provides for exceptions, notably for law enforcement, as allowed by EU Directive 2016/680. In concrete terms, he indicated that ICO's recent work has been to provide means to comply with legislation to law enforcement authorities. He then called for good information governance not to be seen as an obstacle to innovation, but instead as a help.

ICO expects that **a clear legal basis should be put in place** in order to require that the process is fair, legal, transparent and appropriate. He stressed the need for a risk assessment prior to processing as well as data protection by design. He also recalled that the ICO had the authority to fine a company up to 4% of its turnover.

He concluded his intervention by saying that the ICO was following very closely the uses of facial recognition, particularly in the field of law enforcement. The ICO carried out investigations, researches and monitoring on the uses of facial recognition and published a report on this topic in October 2019. Finally, he reaffirmed that the Data Protection Act 2018 applied to all stages of the use of personal data (collection, storage, use, etc.) while insisting on the need to assess all applicable texts comparatively.

3. FOR LIBERTY, THE FUTURE OF FACIAL RECOGNITION MUST BE ITS PROHIBITION

After two institutional actors, the floor was given to a member of the **Liberty organization**: **Hannah Couchman**. She recalled her association's commitment to a campaign in favor of banning facial recognition and focused on a human rights approach while emphasizing the central issue of the protection of minorities.

Her starting point was the definition of privacy as: "the ability of individuals to determine what they want to be and what they want to share with others", hence pointing out that facial recognition is a threat to privacy.

She went on to demonstrate that surveillance technologies such as FRTs are changing the way we act, which affects the very symbolic **right to protest**. For instance, taking the first facial recognition test deployed during a folk festival (in Notting Hill Carnival, 2016) as proof, she regretted that we have to change our lifestyles to escape this surveillance.

Concerning **discrimination:** she argued that even with perfect and 100% reliable technology, its use was likely to discriminate against people of color through police over-surveillance. She expressed indignation at the possibility of increasing surveillance of certain categories of people in order to perfect facial recognition. And she expressed concern about the increase of police surveillance capabilities offered by this new cloud of technology.

According to her, one problem was the **collusion between states and the private sector**. She denounced the fact that police admitted sharing sensitive data with private actors, which led some companies to build an economic business based on surveillance. Finally, in terms of transparency, she deplored the fact that transparency systematically comes up against trade secrets.

She ended her plea by **calling for a ban** on facial recognition:

"Even if we address all the questions raised: it will always be disproportionate, it will always threaten our ability to live freely and it will always be use in a discriminatory way. This kind of tools is about oppression and control: it has no place in our schools, in our train stations, in our football stadiums or our shopping centers. It has no place in our streets."

4. FOR THE FRA, THE CURRENT CONDITIONS DO NOT ALLOW A SUFFICIENT ASSESSMENT OF THE RISKS TO FUNDAMENTAL RIGHTS

The last speaker was a member of the Research and Data Unit of the **European Union Agency for Fundamental Rights:** **David Reichel**. He presented an overview of the Agency's research and analysis related to the uses of facial recognition in the United Kingdom but also in France and Germany that led to a report released on November 2019.

The Agency was thus able to make three major observations which – according to him – should guide the legal analysis.

The first stems from the fact that there is **no truly comprehensible review** of who is using facial recognition – nor a review of the exact purposes of FRTs uses.

The second issue was **a lack of transparency** with regard to the rules governing the drawing up of watch lists. The purpose of the processing – and therefore its legality – is assessed in particular in the light of the database used. That is why he explained that beyond technology-specific regulation, the rules governing watch lists are also a crucial issue. For example, the use of existing but very large databases – such as immigration or security databases – to run facial recognition raises questions. As much as using a database that would be specific to facial recognition technology but with unknown, broad or discretionary rules of drawing up.

The third issue he raised was that **the private sector is a major** user of facial recognition.

Returning to fundamental rights considerations, he highlighted the fact that, despite the absence of any significant study on that topic, **citizens seemed, a priori, uncomfortable with the use of facial recognition**.

He explained that the possibility to restrict some human rights, was subject to strict compliance with three conditions: **provision by law, necessity and proportionality**. In the absence of precise rules governing the establishment of watch lists, he therefore deplored the difficulty of being able to assess if these conditions were met, and therefore the legality of limitations.

At some point, he **agreed with Hannah Couchman** by underlying that we need to think beyond the issue of the problems of accuracy of facial recognition, because even a perfect technology raises important problems for fundamental rights. That is why the Agency has placed the protection of privacy and the protection of personal data at the center of its concerns.

He also expressed concern about the violation of other fundamental rights by facial recognition. Beyond privacy and data protection, it is the right to non-discrimination, freedom of expression and association or the right to good administration that are threatened by this technology.

Finally, he suggested minimum guarantees by calling for the **implementation of Fundamental Rights Impact Assessments** separate from Data Protection Impact Assessments as well as the creation of **independent supervisors**.

In conclusion, this panel, which focused on the implications of facial recognition for citizens, showed that many issues require significant legal reflection in terms of the protection of civil liberties and fundamental rights. Consequently, the eagerness of certain stakeholders to generalize facial recognition seems to have to be tempered.

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)