12/10/2020

AI-REGULATION.COM

Biometric Mass Surveillance – Highlights from Greens/EFA Workshop

Maeva El Bouchikhi

To cite this article:

Maeva El Bouchikhi, Biometric Mass Surveillance – Highlights from Greens/EFA Workshop, Chair Legal and Regulatory Implications of Artificial Intelligence, MIAI Grenoble Alpes, 12/10/2020.

AI-Regulation.com

CHAIR LEGAL AND REGULATORY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE

On December 3, 2020, the Greens/EFA Group of the European Parliament hosted an online discussion on the risks of discrimination posed by biometric mass surveillance.
As facial recognition technology (FRT) is becoming more and more used in public places across the world, and especially during Covid19 pandemic, the European Digital Rights (EDRi), a European NGO defending fundamental rights and freedoms online, called for a ban on biometric mass surveillance in a paper published on May 13, 2020. This call was supported by Patrick Breyer, a Greens/EFA Member of the European Parliament (MEP), and by 44 civil society organizations. As biometric surveillance technologies did not stop to be deployed since their call, Patrick Breyer hosted and moderated this workshop to raise global awareness about the risks inherent to these surveillance technologies and the reasons motivating the group for a ban.

AI-Regulation Chair followed the discussions which focused on the legal issues raised by facial recognition. It presents hereafter some of the highlights.

1. Risks of discrimination: Claims of "Algorithmic Bias" in the United States

The first panelist, Mutale Nkonde**,** is an AI Policy advisor of the United Nations, member of the Tik Tok Advisory Board and CEO of AI for the People, a nonprofit communications firm that seeks to change tech neutrality narratives. She first explained how biometric technologies and specifically facial recognition work and how biometric measures and facial features are actually taken by the system before being integrated into a dataset. She raised two particular ''key issues'':

a) Legal protection for sensitive data such as biometric data is important because "data cannot be changed''. The person targeted by FRT ''will never be able to be forgotten'' once processed by the system, which enables this technology to be a very powerful surveillance tool.

b) With regard to the fight against discrimination in the US, a study found that facial recognition had ''a 40% error rate against people of dark skins''. This error rate has a significant impact on public services as, according to Mutale Nkonde, facial recognition is mostly used for security purposes (by police forces at a municipal level, for federal investigations and Immigration services) and can consequently marginalize and discriminate against certain ethnic groups.

Mutale Nkonde regretted that these technologies are being used to control and to track "the most marginalized communities", which "are already over-represented in this system of control''. Moreover, she affirmed that the Covid 19 pandemic demonstrated ''the reemerging of surveillance as a public health asset'' and that FRT could constitute ''a massive existential threat" to individual rights.

2. Cases of Biometric Surveillance in Europe: "Legislative Gap" in the EU

The second panelist was Ella Jakubowska, Policy and Campaigns Officer at EDRi. She leads the network's advocacy on biometric technologies (such as facial recognition) and is one of the coordinators of the recently launched pan-European "Reclaim Your Face" campaign to ban biometric mass surveillance. She claimed that massive surveillance technology is deployed in the EU even if it should not be possible. According to her, if the General Data Protection Regulation (GDPR) should

prevent the deployment of such technologies, there is however an ‘‘enormous legislative gap’’ surrounding FRT in the EU. She emphasized that European citizens are not having their‘‘biometric data protected’’ due to the massive deployment of this surveillance technology.

To illustrate her statement, she chose to focus on two examples that she characterized as “particularly chilling”:

a) Municipality of Como, Italy - Innovative Biometric Surveillance Systems

The first case occurred in the municipality of Como in Italy at the beginning of 2020. FRT, deployed in public spaces as part of an “experiment”, was claimed to be able to detect the face of passers-by as well as to detect ‘‘loitering’’. For achieving such a level of detection, Ella Jakubowska expressed concern that training data of the system might contain ‘‘some forms of discriminatory profiling and bias assumptions’’ as it was deployed ‘‘at the exact places’’ where migrants were held after having been turned away at the border. According to her, the place where Italian authorities chose to deploy these biometric technologies was not “a coincidence”. As a result of the above, journalists put pressure on the Italian Data Protection Authority (DPA) and questioned the legality of such system. The DPA took action in February 2020 against the municipality of Como and mandated the suspension of the FRT system. According to the Italian DPA, the processing of biometric data carried out by the municipality was illegal. If this decision is a first step towards a ban of biometric surveillance, Ella Jakubowska highlighted that at least two other Italian cities are currently experimenting FRT with ‘‘almost the same exact technologies’’ as the one used in the municipality of Como.

b) EU-Borders Control lie-detector systems

The second case relates to FRT and other algorithmic technologies which were deployed at EU external borders, under the framework of the Integrated Portable Control System (as reported by the European Agency for Fundamental Rights (FRA)), for lie-detection purposes. These systems are currently ‘‘part of the immigration process ’’but, according to Ella Jakubowska, ‘‘detecting if someone is lying is scientifically not valid’’. Given that this technology is used by those people who ‘‘have the power to grant or to deny people’s right of movement ’’this case should, according to her, act as a warning case of biometric surveillance.

3. UK Perspective: Focus on the Bridges v. South Wales Police Judgement

The third panelist was Gracie Mae Bradley, a human rights expert and campaigner. She is Interim Director of Liberty, an independent organization in the United-Kingdom (UK). During her presentation, she focused on the Bridges v. South Wales Police Judgement, a case in which the applicant found his face has been scanned by a FRT at least twice by the South Wales Police during a protest. In September 2019, the High Court decided that while FR does interfere with the privacy rights of everyone scanned, the current legal framework provided sufficient safeguards. Liberty appealed against the judgement and on August 11, 2020 the Court of Appeal agreed with Liberty’s submissions and found that the South Wales Police breached article 8 of the European Convention on Human Rights, the Data protection impact assessment requirements of the Data Protection Act and the Public Sector Equality Duty.

With specific regard to adequacy with the UK legal framework and fight against discrimination, the Court found that the South Wales Police failed to meet the Public Sector Equality Duty placed on them.

The latter requires public bodies and other people carrying out public functions to ‘‘have due regard to the need to eliminate discrimination’’ proactively. Consequently, the Court found that the South Wales Police, in deploying FRT, had never sought to satisfy, directly or by independent verification, the requirement that the system does not have an unacceptable bias on the grounds of race or sexual gender. The recall of this judgement was interesting as its main contribution invites police forces that intend to use FRT ‘‘to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias’’.

All panelists acknowledged that FRT’s accuracy was a main issue, in particular regarding minorities, vulnerable groups, or transgender people, and went on to focus on the legal consequences that biased algorithms may be generated.

4. Discriminatory and racial bias into the dataset

All the panelists agreed that besides the lack of legal provisions, current FRTs that rely on Artificial Intelligence (AI) might be biased, inaccurate and discriminatory towards minorities. Mutale Nkonde explained how facial recognition misidentified black people and more specifically black women as well as non-binary people. This discriminatory effect is due to the fact that algorithmic biases generate error rates and ‘‘red flags'' when the system analyzes category or group of people. According to her, these biases are mainly due to the lack of dynamism of these machines and to the fact that they learn from past tasks to make predictions about the future. In her vue, racial biases into the system are simply the reflection of human societal biases. She agreed with Ella Jakubowska regarding the places in which public authorities choose to deploy FR systems. She also argued that these machines are trained “to take a very euro-centric, very white-centric, very-male-centric view of who is a human’’ and they could ‘‘completely disregard everybody else’’.

Acquiescing to these issues, the moderator, Patrick Breyer asked if “these algorithms really deserve the name of Artificial Intelligence?’’

Mutale Nkone agreed and replied with a quotation from the book entitled *Artificial UnIntelligence, How Computers Misunderstand the World* written by Meredith Broussard, who explains that these (facial recognition) systems are deployed at a cost of billions of dollars all over the world and do not work, especially when used for law enforcement purposes.

5. Inaccuracy of the system and judicial consequences

As algorithmic biases are not purely theoretical assumptions but may lead to particular harmful judicial consequences for individuals, Mutela Nkonde referred to two particular cases that underline the potential threats at stake regarding inaccurate FRTs when used for law enforcement purposes:

a) Detroit police wrongfully arrested a black man based on false positives by FRT in 2020: By the means of CCTV Cameras, FRT used by the police misidentified a black man as being responsible for stealing approximately 4,000 USD worth of merchandise in a Shinola retail store. This case was brought to the public’s attention as it was the first case of misidentification and judicial charges due to FRT flaws. This case was also the first of this kind to, first attract public attention, and second, raise public awareness about the massive deployment of FRT and surveillance technology in public spaces across the US.

b) The use of FRT to track Black Lives Matter protestors in August 2020 : Police forces used FRT to track and charge protestors of the Black Live Matters movement which, according to Mutela Nkonde, breached American citizens' fundamental rights and freedom of speech.

These cases are of particular importance as Europe is also deploying more and more FRTs for law enforcement and criminal investigation purposes. This point was emphasized by Ella Jakubowska who explained that companies operating in the EU ''have invested interests in selling as much of these technologies as possible to customers including, law enforcement, to municipalities, schools'', etc. She underlined a certain political inadequacy between the fact that companies that claim to be able to detect ''people's age, race, for advertising purposes'' are also the ''very same companies that are selling biometric-surveillance-technologies'' to the EU, ''receiving seal of excellence'' and ''massively funded'' for their technology. For instance, she explained that the successful, massive deployment of Huawei technology for smart cities projects in Europe might be due to Huawei's campaign convincing governments that their technologies were both necessary and legally compliant, which, according to her, is not the case. To conclude, she said that, in her opinion, a 100% accurate FRT would probably be even worse as it might be used to "profile and target people and taking their rights and ability to live in privacy and dignity.''

6. If the Legal Framework is inadequate, is a ban needed?

Consequently, if the current legal framework governing these technologies is not ''enough'', according to the panelists, most of them supported the view that these technologies should be banned until adequate safeguards and measures have been implemented. However, they argued that better safeguards might not ensure an adequate level of legal certainty and prevent harmful consequences due to FRTs and other biometric surveillance. For instance, Gracie Mae Bradley explained that in the UK, people need to move on from speaking about bias to speak more broadly about the context in which the technology is actually being deployed and if the technology is actually desirable. As the ''technology gets better at recognizing certain faces'' and a greater diversity of faces as well, she wondered if a more effective surveillance tool was really desirable.

Most areas where FRTs are deployed in the Metropolitan Police of the UK are areas with ''high ethnic minorities populations'' and ''racially diverse and working-class''. According to her, the ''intended target'' of these biometric surveillance technologies are the most vulnerable ones and these technologies participate to construct intended targets as "generally'' perceived as "criminal or harmful in some ways". This example echoes Ella Jakubowska's case of FRTs deployed in areas where migrants were held in Italy. Consequently, FR system construction can be biased, discriminatory, and thus disproportionately affect certain communities. This concern should justify, according to Ella Jakubowska, Liberty, and other panelists, the ban of these technologies. As stated by Gracie Mae Bradley:

> *''The legal framework is absolutely not acceptable and it is very difficult to see what safeguards could be put in place that would sufficiently mitigate the right impacts of mass-surveillance-tools like Facial Recognition''.*

If some might think that there are already rules in place to protect individuals against abusive public surveillance, Ella Jakubowska also pointed out that some others might think that any additional legal framework may arrive ''too late'' as these systems are already massively deployed. According to her,

banning these technologies might be the best option so far. However, since this solution does not meet with unanimous approval, some other safeguards and alternatives should be put in place:

a) Additional Safeguards: the panelists proposed to more investigate the structure in which FRTs are deployed, to increase transparency of the system, introduce red lines regarding the location of FRTs, let the public know the motivations of surveillance biometric technologies's deployment and use alternative means when less intrusive measures can still achieve the same intended purpose.

b) Providing better resources to DPAs: during the question time between the panel and the audience, someone asked if the deployment of FRTs in Europe was a failure of national DPAs. According to Ella Jakubowska, DPAs did not failed as most of them were doing ''a great job with the resources they have". On the contrary, she stated that Member States should probably be the ones responsible as they might have failed to equip DPAs with adequate human, financial or political resources. As a solution, she said that DPAs would need more capacity ''to be able to hold various authorities and companies to account for their abuses of biometric data across Europe''. For supporting her statement, she mentioned for instance that the Belgium DPA found out that Brussels Airport deployed a system of mass recognition through the reading of a press article.

As a conclusion all the panelists agreed that the political and legal landscape framing biometric surveillance technology is unclear or inadequate so far, and that current FRTs are still biased and discriminatory at some extent. Each of them committed to continue to call for a ban on biometric surveillance technology, whether in the US, in Europe, or in the UK.

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