"Impacts of the use of biometric and behavioural mass surveillance technologies on human rights and the rule of law"

Key findings of the study

European countries have been experimenting with increasingly intrusive technology for the last 20 years, without ever demonstrating its efficiency and added-value. If left unregulated, these technologies have the potential to change our societies fundamentally. It's time to acknowledge the adverse effect of biometric surveillance methods on our fundamental rights. We need to act now before it's too late.

The use of biometric mass surveillance in public places, like at the Winter Olympics in Beijing, has an impact on our human rights, including the violation of the right to private life, loss of personal autonomy, such as self-censorship and the infringement on the right to assembly, risks to self-determination and human dignity, among others.

EU member states are also increasingly using video-surveillance, which progressively includes facial and behavioural recognition technology. In addition, the public and private sectors increasingly propose authentication functions based on biometric recognition. Different sectors are using surveillance techniques based on biometric or behavioural criteria.

The EU plays a central role in the development of the use of biometric technology, seeking to favour a technical convergence of European systems that contain biometric data. This EU policy expands to the Western Balkans. This approach is sometimes presented as the result of pressure from the USA to make the recourse to biometry a priority objective in the fight against terrorism. However, the authors show that the European Union made choices that widely exceeded the demands made by the USA and rather seem to serve an EU domestic policy aiming to develop a registry of fingerprints and facial images of EU citizens and residents. Governmental practices tend to show a will to massively use surveillance technology under the justification of security, 'protection', and progress; such as fighting terrorism and addressing immigration. At the same time, public opposition and civil society action to the use of biometric surveillance is slowing down its implementation.

Enforcement and supervision mechanisms appear to remain weak. Transparency is also lacking regarding the use of all video-surveillance systems, in particular in relation to their purposes, and supervision appears widely of a declarative nature. The risks linked to errors and to the theft of biometric identifiers are numerous and widespread. Risks include technical errors - a striking example of errors is provided by an independent report, which concludes that the facial recognition system used by the London Metropolitan Police is "verifiably accurate in just 19%

of cases", which means that "81% of 'suspects' flagged by [the] technology [are] innocent". Human-based errors and weaknesses are another factor - the way in which technology is implemented may itself lead to unwanted impacts, such as the reinforcement of stereotypes. Simple biometric identifier theft can have very serious impacts on the human rights of individuals.

Case studies

In **France (pp.125-138),** the exact number of video surveillance cameras deployed in the country remains unknown. Available figures do show that there are 42,500 cameras in Paris - that's a ratio of 3.84 cameras for every 1,000 inhabitants.

- In 2008, the term 'video surveillance' was replaced by 'video protection' in an attempt to reframe the debate, with legislation following in 2009
- In general, facial recognition and other biometric surveillance tools are used by law enforcement and intelligence agencies, with a lack of transparency
- From February 2020, law enforcement and government-affiliated agencies used a software aiming to perform facial recognition based on photographs collected on social networks by Clearview AI - without managerial oversight and outside any legal framework
- Next INpact reports that, each month, new airports and border crossings are equipped with facial recognition technology.
- During the pandemic, the Ministry of Home Affairs was sanctioned by the French Data Protection Authority (CNIL) for police use of drones to monitor public protests, monitor behaviours and assist in investigations. There was no transparency, nor an impact assessment or a link to a law with appropriate safeguards.
- Facial recognition software was also used in a metro station in Paris, in which 6 cameras could identify citizens not wearing a mask - this experiment was also condemned by the CNIL
- Several projects including VOIE (Open and Integrated Video-protection) and S^2UCRE (Safety and Security of UrbanCrowded Environments) have been initiated, which use biometric and behavioural identification methods. Other projects in Nice have used facial recognition - for example at a Carnival in 2019 and in public transport to identify 'suspects'.
- The use of biometric technologies continues to grow in the private sector in France, including behavioural technology in a number of supermarkets

In the **United Kingdom (pp.142-155),** while ID cards do not exist, biometric immigration documents do.

- London installed more than 691,000 cameras for a ratio of 73.31 cameras for 1,000 inhabitants, which meant it was, at last count, the most surveilled city in Europe.
- In 2017 and 2018, the South Wales police implemented automated facial recognition technology, but this was overturned by the High Court in 2020.
- In 2020, right before this ruling, despite criticism, the London Metropolitan Police announced the deployment of facial recognition in the streets.

- Since 2016, the London Metropolitan Police has been testing a live facial recognition technology, and announced in 2020 its intention to deploy it across London. Tests revealed that "81% of matches made by the system were incorrect".
- Research on the use of biometric data by 96 countries during the pandemic observes that "the country with the worst number of facial recognition technologies in use/being developed for the pandemic is the United Kingdom".
- In October 2021, the UK government announced it would introduce a facial recognition app in 2022 enabling citizens to access over 300 government services through their smartphones. The app will either use facial recognition or fingerprint scanning to verify the user.
- The United Kingdom intelligence services have a long tradition of collecting information on their citizens and residents, and of information sharing with other services.
- We are all aware of the surveillance practices of GCHQ, as brought to light by Edward Snowden, but there are also other administrations in the UK that have used surveillance practices. In 2019, UK Data Protection Authority (ICO) issued an enforcement notice against Her Majesty Revenue & Customs (HRMC) for collecting the voices of 7 million users in order to obtain voice-ID as future means of authentication.
- In 2015, a report showed that '25% of UK retailers are using facial recognition technology in an effort to monitor customer activities at their stores'. The situation since then has worsened. Last year, the cafeterias of nine British schools in North Ayrshire implemented facial recognition for payment.

In **Romania (pp. 155-168),** activists suspect that the public authorities maintain a "facial recognition database with some 50-60 million facial images (such as ID cards or passports), to which the Romanian Intelligence Service (SRI) has unlimited and unsupervised access", without specific legislation providing for it.

- Recent research highlights the increasing use of CCTV including facial recognition in the country, in association with biometric databases, again with a lack of transparency
- Although it is difficult to estimate the overall number of surveillance cameras in Romania, there are many examples of the use of surveillance. In one district in Bucharest in 2019, at least 375 surveillance cameras were installed and used, with the aim of sending fines to people whose cars were caught to be at the scene of illegal waste dumping.
- In 2013, the Bucharest airport was used to test a system named Automated Virtual Agent for Truth Assessment in Real time (AVATAR), developed by the US National Centre for Border Security and Immigration. It enabled the conducting of automated interviews of travellers associated with the analysis of the latter's "nonverbal and verbal behaviour, such as eye movement, gestures and pitch". Romania's Border Police also uses unmanned aerial vehicle (UAV).
- The Romanian Intelligence Service (RSI) also completed a large-scale project in 2019, which has the potential for widespread surveillance of the entire Romanian population. Complaints were filed by civil society,

including to the European Commission, the European Anti-fraud Office (OLAF), the Romanian Data Protection Authority, and the Parliamentary Committee overseeing SRI's activity. The RSI maintains that its use does not infringe on citizens' fundamental rights, but concerns about the legal basis and lack of transparency still remain.
- In Romania, authorities express a strong desire to strengthen Romanian national security (e.g addressing terrorism and immigration) through surveillance. The Implementation of such surveillance technologies generally relies on a provider, the majority of which appear to be located in Europe. This is not in general matched by widespread opposition to the use of biometric surveillance technologies.

Key recommendations from this study include

- Declare an immediate ban on technology and practices that impact the right to hold a belief, the right to self-determination, the right to human dignity, and the right to resist oppression
- Implement human rights education in society and in the political sphere, at national and European Union levels
- Restore the conditions for democratic debate
- Convene a general forum on democracy, human rights, and the rule of law

More about the authors of the study commissioned by Greens/EFA

- **Dr. Estelle De Marco** - lead researcher for the Greens/EFA study on biometric surveillance and human rights, is a jurist specialising in legal and ethical aspects related to ICT, cybersecurity and action against crime, covering fundamental rights and personal data protection, including impact and risk assessment. She holds a Ph.D. in private law and criminal sciences and a Master II degree in ICT law. She is the founder and Director of Inthemis, a firm specialised in ICT legal ethics and data protection compliance and is the founder and administrator of jrgpd.fr. She regularly leads ethics-related tasks in EU co-funded research projects. In parallel, she is lecturer at three higher education establishments where she teaches legal ethics and personal data protection, legal aspects of cybersecurity and cybercrime and liability of Internet stakeholders. She also acts as an expert on cybercrime, electronic evidence and fundamental rights protection for the Council of Europe.

- **Aeris** is a computer engineer specialising in cybersecurity and cryptography. He holds an IT engineering degree from the French Advanced National College of Applied Science and Technology (ENSSAT). He is DevOps and safety and security advisor. He co-founded the Francilian Cryptoparty movement and is involved in several other projects focussing on privacy and security awareness, such as Exodus Privacy, a tool that enables discovering privacy trackers in Android applications. He is lecturer at the University of Technology of Troyes where he teaches cybersecurity.

He is involved in several related research activities, such as third party detection in webpages and TLS scoring.

Contributors to the study

- **Célie Zamora** is a jurist specialising in ICT law and fundamental rights protection. She holds a Master II degree in digital economy related law and is a PhD candidate in private law and criminal science at the Institut de Droit Européen des Droits de l'homme (IDEDH), of the University of Montpellier. Her research focusses on public policies addressing hatred and discrimination and on fundamental rights preservation, including personal data protection.

- **Valentina Pavel** is a jurist specialising in digital rights, privacy and data protection. She holds a Master II degree in law and technology. She is a legal advisor and researcher and her current work on the Rethinking Data project at the Ada Lovelace Institute focuses on changes in the data governance ecosystem that can enable countervailing visions for data use and regulation. She is also a member of ApTI Romania and a 2018-2019 Mozilla Fellow.