18 October 2021

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

"Human After All: Data Protection in Policing"

7th EDEN Event on Data Protection in Law

Wojciech Wiewiórowski
European Data Protection Supervisor

Human After All: Data Protection in Policing.

I am delighted to address the EDEN conference again and regret that I cannot be with you in person.

As we have many interesting keynote speakers today, let's get down to business. Let's talk Artificial Intelligence - a central topic of the last few years across many fields, and the law enforcement community is no exception.

Let me say upfront: as the head of a data protection authority, I welcome and support the responsible development and deployment of AI and other new technologies, as long as we are satisfied that they do not endanger [the essence of] our fundamental rights.

[AI - need for a regulation]

I recognise, however, that AI, with all its complexity, requires more specific rules based on a human-centric and risk-based approach, in line with EU fundamental values. Therefore, I supported, in principle, the European Commission's proposal for an AI Regulation because I believe that it sets certain necessary requirements. But, I also expressed my doubts as to certain solutions.

I am deeply convinced that we should be very aware that while the use of data and AI technologies may undoubtedly have its benefits, these are by no means a "silver bullet" and can never be a substitute for the human factor, **especially in the field of law enforcement and criminal justice.**

I do not see, nor can I imagine, any applications of AI in law enforcement that could be considered as meeting the test of necessity and proportionality.

[Three risks with AI]

There are several use cases of AI that are a source of high concern, such as

- **facial recognition in public spaces;**
- **AI to classify people based on their biometrics;**
- **AI to infer emotions.**

I believe that the use of facial recognition in public spaces does not have its place in a democratic society as, by nature, this entails mass surveillance.

The resulting interference with fundamental rights and freedoms goes much further than privacy and data protection. It affects, for example, the freedom of movement, freedom of assembly, but more importantly, encroaches on basic human dignity.

After all, we are talking about an IT infrastructure working 24/7, processing everybody's biometric data permanently - comparisons with an Orwellian world come naturally to all of us, I believe.

[Emotional AI]

Let me give you another example of the use of AI that I find very difficult to accept: Emotional AI

For emotional Artificial Intelligence, such as Facial Emotion Recognition, we consider that this clearly touches a part of peoples' most private and intimate data.

Any technology that is used to infer information from human emotions raises - in addition to cold legal concerns, such as legality, necessity and proportionality - serious ethical concerns, because of the sensitivity of the human emotions and their effect on human dignity.

[AI in public spaces]

I am not saying one cannot envisage a role for such technology. Certain well-specified use cases for heath or research purposes (e.g. patients where emotion recognition is important), with the appropriate safeguards, could exceptionally, under conditions, justify the necessity and proportionality test. However**, I definitely do not see a place for AI-powered emotion recognition in law enforcement** or in any related activity in the public sphere.

[AI development - how?]

I feel personally encouraged that the EDPS is not alone in this effort for our democracy: on 6 October, the European Parliament called for a ban on police use of facial recognition technology in public places, and on predictive policing. In their resolution, the Members of the European Parliament have, amongst other considerations, highlighted the problem of private facial recognition databases, like the one offered by the controversial company, Clearview AI.

It may sound like a paradox but I am convinced that by raising a red flag and banning the most controversial applications**, we are actually helping the development and deployment of AI in law enforcement**. As the supervisor of the EU institutions, bodies and agencies, the EDPS has actually developed some experience in the field of AI deployment and its supervision.

I acknowledge the fact that today **criminal investigations increasingly include the collection and analysis of large and complex datasets**, which may necessitate new IT tools.

I also understand that law enforcement authorities, both at EU and national level, would like to **benefit from the best possible legal and technical instruments** to accomplish their tasks, while not being forced to rely on external vendors.

Therefore, in our recent Opinion on the reform of Europol, I supported the **proposed new role of Europol in research and innovation,** including my support for the development of algorithms for the analysis of large and complex datasets, provided that all necessary safeguards are put in place.

At the same time, while digital tools may contribute to the greater efficiency and effectiveness of combatting serious crime, their **use in the law enforcement and criminal justice sector remains highly sensitive**. Therefore, it is crucial that their deployment fully complies with privacy and the data protection legislation and meets the state-of-the-art standards with regard to information and cyber security

[Role of supervision]

This is why one of the priorities of my mandate is to closely monitor the use of new tools involving data analytics and artificial intelligence by Europol and other agencies operating in the Area of Freedom Security and Justice, such as Frontex, eu-LISA, EPPO, or Eurojust.

In view of the new operational reality and the new tasks given to Europol in that area, in the context of the review of the Europol Regulation, **the EDPS has put specific emphasis this year on making sure that Europol was implementing strong data protection safeguards when using AI tools.** I understand that this is a challenge as Europol is at the forefront of innovation in the field of law enforcement, and specific legislation is still in the making. My role as supervisor is to monitor that Europol defines in a concrete way the technical and organisational measures to be put in place.

I believe Europol should be an example of how AI-based solutions are developed alongside highly advanced data protection impact assessments. **Europol should be able to lead by example in this area.** To lead globally.

[Conclusion]

To conclude, while I remain committed to assisting and providing guidance to the EU institutions, bodies and agencies, I will - as an enforcer of data protection and privacy rules, not only an advisor - continue to monitor and, whenever necessary, intervene in order to ensure that their powers are used with full respect for the legal framework and fundamental rights.

I am convinced that the long tradition of EDEN conferences proves that, at EU level, our law enforcement authorities can not only lead by example, but also show the way globally on how to achieve its aims, hand in hand with fundamental rights and respect for human dignity.