AI and Criminal Justice – Regulatory and Practical Challenges (28 April 2022)

Prepared by Lina Jasmontaite

On 28 April 2022, the Brussels Privacy Hub hosted a roundtable focusing on the implications of the draft AI Act for law enforcement authorities. The roundtable was part of Enforcing Europe Series 2. It was organised in cooperation with the University of Luxembourg within the framework of the FWO/FNR-funded MATIS project, and in partnership with EDRi. The event was followed by 62 participants, ranging from industry and civil society representatives to policy makers and academics, who actively engaged in the debate by posing questions in the meeting chat.

After the opening remarks of Juraj Sajfert, a researcher at VUB/University of Luxembourg, Eike Graef, Policy Officer for Fundamental Rights at the European Commission's Directorate General for Justice and Consumers, set the background for the discussions. He noted, the European Commission (EC) is aware of the lukewarm welcome of the draft AI proposal by the home affairs community and is interested in learning specific concerns that could be taken into account during the legislative deliberation stage. For example, the EC is aware of the fear that in markets with rather small demand, as might be the case for systems destined for the use by courts, there might be little supply that would satisfy the new requirements for a certain time. Eike emphasised that the proposed AI Act is part of many policy actions devoted to fostering and promoting AI development. It complements the funding for the EU's technological and industrial capacity and reach effort, in particular work of the Joint Research Centre, to prepare for socio-economic changes brought about by AI.

Eike recalled that the main objective of this proposal was to address the complexity and opacity of certain AI systems and in this way help ensure safety and compliance and effective enforcement of fundamental rights, including the rights to data protection and privacy, the freedom of expression, freedom of assembly, equal treatment, and procedural rights. The proposed AI Act should be regarded as a legislative measure that seeks to complement the existing legislative framework. It is not meant to govern any kind of action that could be performed by means of AI but instead strengthen the existing framework in place that governs the type of action at hand. For example, the AI Act should supplement the proposed new rules for consumer credits and people working through platforms, where systems used in areas governed by those rules are based on AI technology.

The proposed AI Act includes a broad definition of AI in order to increase legal certainty about which systems are covered. The idea behind having a broad definition, which covers not only machine learning but for example also expert systems, was considered to be a solution to avoid endless discussions on whether certain technologies would constitute "real" AI or not (which often emerge in relation to statistics). The choice of the EC was not to exclude systems from the scope because they are not complex enough, but to have a broad technical scope and to impose obligations depending on the types of risks that would be posed by AI systems in view of their purpose. Annex III of the proposal clarifies in which situations the use of AI systems in the areas of law enforcement (Annex III.6) and for administration of justice and democratic processes (Annex III. 8) are considered to result in high risk.

The AI proposal is in the legislative deliberation stage. The recently drafted amendments by the members of the European Parliament, namely Dragoș Tudorache and Brando Benifei suggested to exclude predictive policing from high-risk situations because they believe that it should be prohibited as such, in order to prevent discriminatory practices. Other political groups are still reviewing the proposal and are drafting the amendments to the articles that fall within their competence.

Eike, highlighted several articles that are of great interest for the debates concerning the AI use in the law enforcement area, namely Article 10 on data governance and Article 11 on technical documentation that require to test and document many dimensions of AI tools (e.g., what is optimised, the performance of the tool on different types of populations etc.). Article 13 is about informing the users of a high-risk AI system about characteristics, capabilities and limitations of the performance of the system. Article 64 empowers authorities in charge of fundamental rights in areas that fall under Annex III of the proposal to access any documentation that is created and maintained pursuant to the AI Act.

There are several provisions that provide specifications for the law enforcement area. For example, Article 52 on transparency and Article 70 on confidentiality are the provisions, where obligations of law enforcement authorities would be limited in order not to hamper investigations.

Julia Thorsøe Ballaschk, Data Protection Officer at the Danish National Police, highlighted that the police not only investigates crime but it is also an administrative body tasked with duties, such as issuing gun permits or preparing criminal records for certain types of job. With regards to the more traditional law enforcement tasks, the police witnesses a constant decrease in violent crimes while cybercrime is rapidly increasing. Cybercrime ranges from cyber harassment and distribution of content with illicit sexual images to online financial fraud. In order to solve these types of crimes, AI based systems could be used as they could facilitate work with large data sets. More specifically, the investigation of money laundering and the analysis of child sexual abuse material could be two use cases for AI systems. With regards to money laundering investigations, AI could help analyse very big data sets on transactions with regards to highlighting deviant behaviour and thus save a tremendous amount of ressources and help identify relevant cases. With regards to the analysis of child sexual abuse material, AI based systems allow i.a. to identify locations, where sexual abuse of children was recorded. These systems aid the work of police by analysing large datasets much faster and limit the exposure of personnel who have to watch through disturbing material.

At the same time, it should be recognised that there are certain limitations posed by AI systems. For example, it would be a challenge to use AI based systems to solve violent crimes in Denmark because there is no data set that would be big enough in order to make assumptions about the future. Additionally, law enforcement in smaller countries would often be forced to buy off the shelf-software solutions, due to budgetary restraints. Such solutions, however, may not be appropriate as they may be a poor fit in the existing legal and societal framework. On top of that they may include internal and external bias from previous actions or samples of data used to develop such tools. Finally, it should be considered that AI tools should be affordable to law enforcement authorities.

Teresa Quintel, a senior lecturer at the Maastricht European Centre on Privacy and Cybersecurity (ECPC), in her contribution, based on the recent publication, reflected on the European Data Protection Supervisor (EDPS) investigation and order concerning Europol's data processing practices. The order issued by the EDPS is an illustrative example of a situation where a law enforcement authority, Europol in this case, may no longer be able to effectively handle a large amount of data received from national law enforcement authorities without the help of AI technologies. The EDPS ordered Europol to delete data concerning individuals with no established link to a criminal activity. Europol's big data challenge underlines the violation of data protection principles by an EU agency.

It appeared that for over the period of several years, Europol processed datasets which it received from its national counterparts for purposes of strategic and operational analysis without defining the categories of data subjects. According to the Europol Regulation 2016/794 (Annex II, part B.1), Europol must categorize data subjects into 'suspects', 'potential future criminals', 'contacts and associates', 'victims', 'witnesses' and 'informants'. By failing to perform the data subject categorisation, Europol also infringed core principles of data protection such as the purpose limitation and the data minimization principles. It is noteworthy, that soon after the order, the recast Europol Regulation was adopted, and in essence it is going to allow for Europol to engage in data processing activities without performing data subject categorisation for operational analysis if that is relevant for a specific investigation (Article 18a of the recast Regulation). This development is worrisome because it is not going to enable different treatment of individuals in accordance with their status in a crime. The new processing capabilities of Europol that the Agency was granted under its recast Regulation facilitate processing and matching of personal data that the EDPS ordered the deletion of. In addition, the recast Europol Regulation retroactively legalises those processing operations that the EDPS ordered to be terminated. The question remains, whether more data and more matching of data can meaningfully facilitate law enforcement actions.

Laure Baudrihaye-Gérard, who leads Fair Trials' legal and policy work in Europe, shared insights from the research concerning the impact of AI on the law enforcement sector. It has been observed that large data sets are used by police and criminal justice authorities and increasingly used to develop AI systems, including predictive risk profiling assessments of future criminality (see Fair Trails, Automating Injustice. Artificial intelligence (AI) and automated decision-making (ADM) systems). For example, police data from stop and searches and arrests (even where they do not lead to charges) are fed into such systems. The data fed into these models also includes people who were affected or implicated by a crime into the same systems as well as non-police data, such as immigration status and welfare benefits. As a result, these systems reflect existing bias and discrimination in policing. One illustrative example in this regard is 'Top600', an automated risk modelling and profiling system, which was started by the Amsterdam Municipality in partnership with police and social services. It attempted to profile the 'top 600' young people, over the age of 16, who are most at risk of committing 'High Impact Crime' in the future. It affected not only policing decisions, but our research indicates that it also influenced criminal justice outcomes, including the decision to request pre-trial detention and the severity of punishments. While striving for greater efficiency, technological solutions are presented as "neutral" solutions but they are very harmful, by hardwiring existing discrimination, with very real consequences on people and their rights. Moreover, such predictive type of systems, that aim to detect "future" criminality, are depriving of substance the right of presumption of innocence.

Laure remarked that the proposed AI Act is a momentous opportunity, which provides for a possibility to stop currently highly worrisome practices through the implementation of a ban on such predictive types of systems, and impose transparency over how such systems function and are developed as well as effectives redress mechanisms for individuals.

During the discussion between the speakers and the audience, the following issues were pointed out:

- AI driven systems in law enforcement are fuelling racial profiling and have real consequences on marginalised groups (e.g., black people, Asian, or people living poverty). This is mostly because they are not based on objective data but on the historic data.
- AI based systems result in over-policing and often lack accuracy.
- The Europol's big data challenge demonstrates that there is tension between different types of regulation. The expansion of Europol's mandate is in stark contradiction with the European Parliament's view expressed in its resolution on banning the use of artificial intelligence by the police.