European Parliament
2019-2024

Committee on Civil Liberties, Justice and Home Affairs

2020/2016(INI)

8.6.2020

DRAFT REPORT

on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters
(2020/2016(INI))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Tudor Ciuhodaru

PR_INI

CONTENTS

Page

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters
(2020/2016(INI))

The European Parliament,

– having regard to the Treaty of the European Union, in particular Articles 2 and 6, and the Treaty on the Functioning of the European Union,

– having regard to the Charter of Fundamental Rights of the European Union,

– having regard to the Convention for the Protection of Human Rights and Fundamental Freedoms,

– having regard to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108),

– having regard to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee or Regions entitled 'Building Trust in Human-Centric Artificial Intelligence' of 8 April 2019[1],

– having regard to the Commission White Paper entitled 'Artificial Intelligence - A European approach to excellence and trust' of 19 February 2020[2],

– having regard to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee or Regions entitled 'A European strategy for data' of 19 February 2020[3],

– having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[4],

– having regard to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[5],

---

[1] COM(2019)0168.
[2] COM(2020)0065.
[3] COM(2020)0066.
[4] OJ L 119, 4.5.2016, p. 1.
[5] OJ L 119, 4.5.2016, p. 89.

– having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC[6],

– having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[7],

– having regard to Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA[8],

– having regard to Rule 54 of its Rules of Procedure,

- having regard to the opinions of the Committee on the Internal Market and Consumer Protection and the Committee on Legal Affairs,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A9-0000/2020),

A. whereas digital technologies in general and artificial intelligence (AI) in particular bring with them extraordinary promise; whereas AI is one of the strategic technologies of the 21st century, generating substantial benefits in efficiency, accuracy, and convenience, and thus bringing positive change to the European economy; whereas AI should not be seen as an end in itself, but as a tool for serving people, with the ultimate aim of increasing human well-being;

B. whereas the development of AI must respect the values on which the Union is founded, in particular human dignity, freedom, democracy, equality, the rule of law, and human and fundamental rights;

C. whereas trustworthy AI systems need to be accountable, designed for all (including consideration of vulnerable, marginalised populations in their design), be non-discriminatory, safe and transparent, and respect human autonomy and fundamental rights;

D. whereas the Union together with the Member States bear a critical responsibility for ensuring that policy choices surrounding the development, deployment and use of AI applications in the field of the judiciary and law enforcement are made in a transparent manner, respect the principles of necessity and proportionality, and guarantee that the policies and measures adopted will fully safeguard fundamental rights within the Union;

[6] OJ L 295, 21.11.2018, p. 39.
[7] OJ L 201, 31.7.2002, p. 37.
[8] OJ L 135, 24.5.2016, p. 53.

E. whereas AI applications offer great opportunities in the field of law enforcement, in particular in improving the working methods of law enforcement agencies and judicial authorities, and combating certain types of crime more efficiently, in particular financial crime, money laundering and terrorist financing, as well as certain types of cybercrime;

F. whereas a clear model for assigning legal responsibility for the potential harmful effects of AI systems in the field of criminal law is imperative;

G. whereas AI applications in use by law enforcement include applications such as facial recognition technologies, automated number plate recognition, speaker identification, speech identification, lip-reading technologies, aural surveillance (i.e. gunshot detection algorithms), autonomous research and analysis of identified databases, forecasting (predictive policing and crime hotspot analytics), behaviour detection tools, autonomous tools to identify financial fraud and terrorist financing, social media monitoring (scraping and data harvesting for mining connections), international mobile subscriber identity (IMSI) catchers, and automated surveillance systems incorporating different detection capabilities (such as heartbeat detection and thermal cameras); whereas the aforementioned applications have vastly varying degrees of reliability and accuracy;

H. whereas AI tools and applications are also used by the judiciary worldwide, including in sentencing, calculating probabilities for reoffending and in determining probation;

I. whereas use of AI in law enforcement entails a number of potential risks, such as opaque decision-making, different types of discrimination, and risks to the protection of privacy and personal data, the protection of freedom of expression and information, and the presumption of innocence;

J. whereas AI systems used by law enforcement are also vulnerable to AI-empowered attacks; whereas in these situations the resulting damage is potentially even more significant, and can result in exponentially greater levels of harm to both individuals and groups;

1. Reiterates that, as processing large quantities of data is at the heart of AI, the right to the protection of private life and the right to the protection of personal data apply to all areas of AI, and that the Union legal framework for data protection and privacy must be fully complied with;

2. Reaffirms that all AI solutions for law enforcement and the judiciary also need to fully respect the principles of non-discrimination, freedom of movement, the presumption of innocence and right of defence, freedom of expression and information, freedom of assembly and of association, equality before the law, and the right to an effective remedy and a fair trial;

3. Considers, in this regard, that any AI tool either developed or used by law enforcement or judiciary should, as a minimum, be safe, secure and fit for purpose, respect the principles of fairness, accountability, transparency and explainability, with their deployment subject to a strict necessity and proportionality test;

4. Highlights the importance of preventing mass surveillance by means of AI technologies, and of banning applications that would result in it;

5. Stresses the potential for bias and discrimination arising from the use of machine learning and AI applications; notes that biases can be inherent in underlying datasets, especially when historical data is being used, introduced by the developers of the algorithms, or generated when the systems are implemented in real world settings;

6. Underlines the fact that many algorithmically driven identification technologies disproportionately misidentify non-white people, children, the elderly, as well as women;

7. Highlights the power asymmetry between those who develop and employ AI technologies and those who interact and are subject to them;

8. Underlines that security and safety aspects of AI systems used in law enforcement need to be carefully considered, and be sufficiently robust and resilient to prevent the potentially catastrophic consequences of malicious attacks on AI systems;

9. Considers it necessary to create a clear and fair regime for assigning legal responsibility for the potential adverse consequences produced by these advanced digital technologies;

10. Underlines that in judicial and law enforcement contexts, the final decision always needs to be taken by a human, who can be held accountable for the decisions made, and include the possibility of a recourse for a remedy;

11. Calls for algorithmic explainability and transparency in order to ensure that the development, deployment and use of AI systems for judiciary and law enforcement comply with fundamental rights, and are trusted by citizens, as well as in order to ensure that results generated by AI algorithms can be rendered intelligible to users and to those subject to these systems, and that there is transparency on the source data and how the system arrived at a certain conclusion;

12. Calls for traceability of AI systems that defines the capabilities and limitations of the systems, and keeps track of where the defining attributes for a decision originate;

13. Calls for a compulsory fundamental rights impact assessment to be conducted prior to the implementation or deployment of any AI systems for law enforcement or judiciary, in order to assess any potential risks to fundamental rights;

14. Calls for periodic mandatory auditing of all AI systems used by law enforcement and the judiciary to test and evaluate algorithmic systems once they are in operation, in order to detect, investigate, diagnose and rectify any unwanted and adverse effects;

15. Calls for a moratorium on the deployment of facial recognition systems for law enforcement, until the technical standards can be considered fully fundamental rights compliant, results derived are non-discriminatory, and there is public trust in the necessity and proportionality for the deployment of such technologies;

16. Calls for greater overall transparency from Member States, and for a comprehensive understanding of the use of AI applications in the Union, broken down by Member State law enforcement and judicial authority, the type of tool in use, the types of crime they are applied to, and the companies whose tools are being used;

17. Instructs its President to forward this resolution to the Council and the Commission.

EXPLANATORY STATEMENT

Artificial Intelligence (AI) is one of the strategic technologies of the 21st century, generating substantial benefits in efficiency, accuracy, and convenience, and thus contributing positively to the European economy. Among others, AI applications have improved healthcare, increased the efficiency of farming, contributed to climate change mitigation and adaptation, and improved the efficiency of production.

AI is one of the main priorities of the current Commission. Commission President Ursula von der Leyen announced in her political Guidelines, a coordinated European approach on the human and ethical implications of AI as well as a reflection on the better use of big data for innovation. The endorsement of AI as an EU-level issue has been accompanied by a reflection on how to guarantee trust in AI technologies, and how to make sure AI does not compromise EU fundamental rights.

However, AI has been addressed by the European Parliament several years before the Commission decided to make it a high priority. Several resolutions on big data, robotics and artificial intelligence, adopted by the Parliament since 2016, show the importance given to this topic by the Parliament. The resolutions have looked at different implications raised by AI and how it affects welfare, education, technology, legal and fundamental rights and well as industry at large. These resolutions have stressed the need to adopt a "human centric" approach based on the respect of fundamental rights, namely the EU Charter and EU data protection framework.

As a "collection of technologies that combine data, algorithms and computing power", the "advances in computing and the increasing availability of data are therefore key drivers of the current upsurge of AI"[1]. At the core of AI is the fact it is based on the collection, analysis and the recurring accumulation of large amounts of data, including personal data, from a variety of sources, which are subject to automated processing by computer algorithms and advanced data-processing techniques. These techniques use both stored and streamed data in order to generate certain correlations, trends and patterns (big data analytics). Data used for AI do not only come from individuals themselves; AI applications mostly use data coming from industry, business and the public sector, processed for a variety different of purposes. Even if data used by AI applications may sometimes be non-personal data, very often the AI activity entails processing of personal data, as often the AI activity leads to automated decisions having a direct effect on individuals. These features of AI therefore demands us to pay a particular attention in this area to the respect of the basic principles of data protection and privacy.

AI offers great opportunities also in the law enforcement area and criminal justice, in particular in improving the working methods of the law enforcement agencies and judicial authorities and in the fight against certain types of crimes more efficiently, especially in the field of financial crime, money laundering and terrorist financing, and certain types of cybercrime. In this sector, AI applications include *i.a*. facial recognition technologies, automated number plate recognition, speaker identification, speech identification, lip reading technologies, aural surveillance (i.e. gunshot detection algorithms), autonomous research and analysis of identified databases, forecasting (predictive policing and crime hotspot analytics), behaviour detection tools, autonomous tools to identify financial fraud and terrorist financing, social media

[1] COM(2020) 65 final.

monitoring (scraping and data harvesting for mining it for connections), IMSI catchers, and automated surveillance systems incorporating different detection capabilities (such as heartbeat detection and thermal cameras). In judiciary, AI tools may be used in calculating probabilities for reoffending and in determining probation or deciding on the sentencing.

Notwithstanding the benefits brought by AI, the fact is that simultaneously AI entails a number of potential risks, such as opaque decision-making, different types of discrimination, intrusion into our private lives, challenges to the protection of personal data, human dignity, and the freedom of expression and information. These potential risks are aggravated in the sector of law enforcement and criminal justice, as they may affect the presumption of innocence, the fundamental rights to liberty and security of the individual and to an effective remedy and fair trial.

This report seeks to address the issues raised by the use of AI in Criminal Law and its use by the Police and Judicial Authorities in Criminal Matters. While acknowledging the potential opportunities and advantages that AI may imply, it also highlights the significant risks and effects it may entail.

The report stresses the need to fully respect fundamental rights as enshrined in the EU Charter of Fundamental rights, Union privacy and data protection law, namely Directive (EU) 2016/680 (police directive), and the necessity to implement several core principles in the life-cycle of AI, such as algorithmic explainability and transparency, traceability, the carrying out of compulsory fundamental rights impact assessments prior to the implementation or deployment of any AI system and mandatory audits. All these requirements are not only necessary to ensure the lawfulness of AI systems but also to achieve trust of individuals on their use by the law enforcement and criminal judicial authorities.

Last your rapporteur calls for a moratorium for the deployment of facial recognition systems for law enforcement purposes. The current state of play of these technologies, the significant impacts on fundamental rights, calls for an in depth and open societal debate in order to consider the different questions posed and the justification for their deployment.