Basic information

2020/2016(INI) INI - Own-initiative procedure	Procedure completed
Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters **Subject** 3.30.06 Information and communication technologies, digital technologies 3.40.06 Electronics, electrotechnical industries, ICT, robotics 7.30.05 Police cooperation 7.40.04 Judicial cooperation in criminal matters	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
LIBE Civil Liberties, Justice and Home Affairs	VITANOV Petar (S&D)	15/10/2020
	Shadow rapporteur VANDENKENDELAERE Tom (EPP) TUDORACHE Dragoş (Renew) BREYER Patrick (Greens /EFA) BUXADÉ VILLALBA Jorge (ECR) VANDENDRIESSCHE Tom (ID)	

Committee for opinion	Rapporteur for opinion	Appointed
EMPL Employment and Social Affairs	The committee decided not to give an opinion.	
IMCO Internal Market and Consumer Protection	KOLAJA Marcel (Greens/EFA)	18/02/2020
JURI Legal Affairs	DZHAMBAZKI Angel (ECR)	18/02/2020

European Commission

Commission DG	Commissioner
Justice and Consumers	REYNDERS Didier

Key events

Date	Event	Reference	Summary
16/01/2020	Committee referral announced in Parliament		
29/06/2021	Vote in committee		
13/07/2021	Committee report tabled for plenary	A9-0232/2021	Summary
04/10/2021	Debate in Parliament		
05/10/2021	Results of vote in Parliament		
06/10/2021	Decision by Parliament	T9-0405/2021	Summary

Technical information

Procedure reference	2020/2016(INI)
Procedure type	INI - Own-initiative procedure
Procedure subtype	Initiative
Legal basis	Rules of Procedure EP 55
Stage reached in procedure	Procedure completed
Committee dossier	LIBE/9/02284

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE652.625	08/06/2020	
Amendments tabled in committee		PE655.659	17/07/2020	
Committee opinion	IMCO	PE648.565	09/09/2020	
Committee opinion	JURI	PE652.371	14/09/2020	
Committee report tabled for plenary, single reading		A9-0232/2021	13/07/2021	Summary
Text adopted by Parliament, single reading		T9-0405/2021	06/10/2021	Summary

European Commission

Document type	Reference	Date	Summary
Commission response to text adopted in plenary	SP(2021)791	26/01/2022	

Meetings with interest representatives published in line with the Rules of Procedure

Rapporteurs, Shadow Rapporteurs and Committee Chairs

Transparency				
Name	Role	Committee	Date	Interest representatives
VANDENKENDELAERE Tom	Shadow rapporteur	LIBE	11/06/2021	Eurofedop

Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters

2020/2016(INI) - 06/10/2021 - Text adopted by Parliament, single reading

The European Parliament adopted by 377 votes to 248, with 62 abstentions, a resolution on artificial intelligence (AI) in criminal law and its use by the police and judicial authorities in criminal matters.

This resolution addresses the issues raised by the use of AI in criminal law and its use by police and judicial authorities in criminal matters. While recognising the potential opportunities and benefits that AI can bring, it also highlighted the significant risks and consequences that it can bring. It also highlighted the risks it may entail for the protection of people's fundamental rights.

Respect for fundamental rights

Given that the processing of large amounts of data is at the heart of AI, Members believe that the **EU legal framework on data protection and privacy** must be fully respected and should form a basis for any future regulation of AI for law enforcement and judicial use. The use of AI applications must be prohibited when incompatible with fundamental rights. Moreover, the use of AI applications should be categorised as high-risk in instances where there is the potential to significantly affect the lives of individuals.

Parliament reaffirmed that all AI solutions for law enforcement and the judiciary also need to fully respect the principles of human dignity, non-discrimination, freedom of movement, the presumption of innocence and right of defence, including the right to silence, freedom of expression and information, freedom of assembly and of association, equality before the law, the principle of equality of arms and the right to an effective remedy and a fair trial, in accordance with the Charter and the European Convention on Human Rights.

Risk of discrimination

Many algorithmically driven identification technologies currently in use disproportionately misidentify and misclassify and therefore cause harm to racialised people, individuals belonging to certain ethnic communities, LGBTI people, children and the elderly, as well as women.

Parliament called for **algorithmic explainability, transparency, traceability and verification** as a necessary part of oversight, in order to ensure that the development, deployment and use of AI systems for the 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.

Members considered that strong efforts should be made to **avoid automated discrimination** and bias and they called for safeguards against the misuse of AI technologies by law enforcement and judicial authorities also need to be regulated uniformly across the Union.

Mandatory impact assessments

Members called for a compulsory fundamental rights impact assessment to be conducted prior to the implementation or deployment of any AI system for law enforcement or the judiciary, in order to assess any potential risk to fundamental rights. These impact assessments should be conducted with the active participation of civil society. They should clearly define the safeguards needed to address the identified risks and be made public, as far as possible, before the deployment of any AI system.

Parliament called for periodic mandatory auditing of all AI systems used by law enforcement and the judiciary where there is the potential to significantly affect the lives of individuals. It also highlighted the need for specialised training regarding the ethical provisions, potential dangers, limitations, and proper use of AI technology, especially for police and judiciary personnel.

Guarantee human intervention

Members called for the precautionary principle to be respected in all law enforcement applications of AI and stressed that in judicial and law enforcement settings, the decision giving legal or similar effect always needs to be taken by a human, who can be held accountable for the decisions made. Those subject to AI-powered systems must have recourse to remedy.

Surveillance and mass profiling

Parliament called for the **permanent prohibition** of the use of automated analysis and/or recognition in publicly accessible spaces of other human features, such as gait, fingerprints, DNA, voice, and other biometric and behavioural signals. It also called for a ban on the use of private facial recognition databases (such as the Clearview AI system).

Members called for a **moratorium** on the deployment of law enforcement facial recognition systems for identification purposes, unless they are only used for the purpose of identifying victims of crime, until technical standards can be considered fully respectful of fundamental rights.

Members also supported a **ban on mass-scale scoring** of individuals using AI.

Lastly, Parliament expressed concern about research projects funded under Horizon 2020 that deploy artificial intelligence at **external borders**, such as the iBorderCtrl project, a 'smart lie detection system' for travellers entering the EU. It called on the Commission to implement, if necessary through infringement procedures, the ban on any processing of biometric data for law enforcement purposes leading to mass surveillance in publicly accessible areas.

Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters

2020/2016(INI) - 13/07/2021 - Committee report tabled for plenary, single reading

The Committee on Civil Liberties, Justice and Home Affairs adopted an own-initiative report by Petar VITANOV (S&D, BG) on artificial intelligence (AI) in criminal law and its use by the police and judicial authorities in criminal matters.

The use of AI in law enforcement entails a number of potentially high, and in some cases unacceptable, risks for the protection of fundamental rights of individuals, such as opaque decision-making, different types of discrimination and errors inherent in the underlying algorithm which can be reinforced by feedback loops, as well as risks to the protection of privacy and personal data, the protection of freedom of expression and information, the presumption of innocence, the right to an effective remedy and a fair trial.

This report addresses the issues raised by the use of AI in criminal law and its use by police and judicial authorities in criminal matters. While recognising the potential opportunities and benefits that AI can bring, it also highlighted the significant risks and consequences that it can bring.

Respect for fundamental rights

Given that the processing of large amounts of data is at the heart of AI, Members believe that the EU legal framework on data protection and privacy must be fully respected and should form a basis for any future regulation of AI for law enforcement and judicial use. **The use of AI applications must be prohibited when incompatible with fundamental rights**. Moreover, the use of AI applications has to be categorised as high-risk in instances where there is the potential to significantly affect the lives of individuals.

The report reaffirmed that all AI solutions for law enforcement and the judiciary also need to fully respect the principles of human dignity, non-discrimination, freedom of movement, the presumption of innocence and right of defence, including the right to silence, freedom of expression and information, freedom of assembly and of association, equality before the law, the principle of equality of arms and the right to an effective remedy and a fair trial, in accordance with the Charter and the European Convention on Human Rights.

Any AI tools either developed or used by law enforcement or the judiciary should, as a minimum, be safe, robust, secure and fit for purpose, respect the principles of fairness, data minimisation, accountability, transparency, non-discrimination and explainability. Furthermore, their development, deployment and use should be subject to risk assessment and strict necessity and proportionality testing, where safeguards need to be proportionate to the identified risks.

Surveillance and mass profiling

Many algorithmically driven identification technologies currently in use disproportionately misidentify and misclassify and therefore cause harm to racialised people, individuals belonging to certain ethnic communities, LGBTI people, children and the elderly, as well as women.

Members considered that safeguards against the misuse of AI technologies by law enforcement and judicial authorities should be regulated uniformly across the EU.

The report stressed the legal obligation to **prevent mass surveillance using AI technologies** and to prohibit the use of applications that could lead to it. It called for increased efforts to avoid automated discrimination and automation bias.

Risks of data leaks

The report stressed that the safety and security aspects of AI systems used by law enforcement and judicial authorities must be carefully considered and sufficiently robust and resilient to prevent the consequences of malicious attacks against AI systems. It stressed the importance of **safety by design** , as well as **specific human oversight** before the use of certain critical applications and called for law enforcement and judicial authorities to use only those AI applications that respect the principle of privacy and data protection by design so as to avoid misuse.

Members called for the **precautionary principle** to be respected in all law enforcement applications of AI and stressed that in judicial and law enforcement settings, the decision giving legal or similar effect always needs to be taken by a **human**, who can be held accountable for the decisions made.

Mandatory impact assessments

The report called for the **algorithmic explicability, transparency, traceability and verification** as a necessary part of oversight, in order to ensure that the development, deployment and use of AI systems for the judiciary and law enforcement comply with fundamental rights and are trusted by citizens.

Members called for a compulsory fundamental rights impact assessment to be conducted prior to the implementation or deployment of any AI system for law enforcement or the judiciary, in order to assess any potential risk to fundamental rights. These impact assessments should be conducted with the active participation of civil society. They should clearly define the safeguards needed to address the identified risks and be made public, as far as possible, before the deployment of any AI system.

The report called for periodic mandatory auditing of all AI systems used by law enforcement and the judiciary where there is the potential to significantly affect the lives of individuals. It also highlighted the need for specialised training regarding the ethical provisions, potential dangers, limitations, and proper use of AI technology, especially for police and judiciary personnel.

Facial recognition

Members called for a **moratorium** on the deployment of facial recognition systems for law enforcement purposes that have the function of identification, unless strictly used for the purpose of identification of victims of crime, until the technical standards can be considered fully fundamental rights compliant.