European Parliament
2019-2024

Plenary sitting

A9-0232/2021

13.7.2021

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: Petar Vitanov

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 on European Union (TEU), in particular Articles 2 and 6 thereof, and to the Treaty on the Functioning of the European Union (TFEU), in particular Article 16 thereof,

– having regard to the Charter of Fundamental Rights of the European Union (the Charter), in particular Articles 6, 7, 8, 11, 12, 13, 20, 21, 24 and 47 thereof,

– 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), and its amending protocol (Convention 108+),

– having regard to the European Ethical Charter on the use of artificial intelligence in judicial systems and their environment of the European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe,

– having regard to the Commission communication of 8 April 2019 entitled ‘Building Trust in Human-Centric Artificial Intelligence’ (COM(2019)0168),

– having regard to the Ethics Guidelines for Trustworthy AI published by the Commission’s High-Level Expert Group on Artificial on 8 April 2019,

– having regard to the Commission white paper of 19 February 2020 entitled ‘Artificial Intelligence – A European approach to excellence and trust’ (COM(2020)0065),

– having regard to the Commission communication of 19 February 2020 entitled ‘A European strategy for data’ (COM(2020)0066),

– 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)[1],

– 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

[1] OJ L 119, 4.5.2016, p. 1.

penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[2],

– 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[3],

– 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)[4],

– 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[5],

– having regard to its resolution of 19 June 2020 on the anti-racism protests following the death of George Floyd[6],

– having regard to its resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement[7],

– having regard to the hearing in the Committee on Civil Liberties, Justice and Home Affairs (LIBE) on 20 February 2020 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters,

– having regard to the report of the LIBE mission to the United States in February 2020,

– 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 (A9-0232/2021),

A. whereas digital technologies in general and the proliferation of data processing and analytics enabled by artificial intelligence (AI) in particular, bring with them extraordinary promises and risks; whereas AI development has made a big leap forward

[2] OJ L 119, 4.5.2016, p. 89.
[3] OJ L 295, 21.11.2018, p. 39.
[4] OJ L 201, 31.7.2002, p. 37.
[5] OJ L 135, 24.5.2016, p. 53.
[6] Texts adopted, P9_TA(2020)0173.
[7] OJ C 263, 25.7.2018, p. 82.

in recent years, making it one of the strategic technologies of the 21st century, with the potential to generate substantial benefits in efficiency, accuracy, and convenience, and thus bringing positive change to the European economy and society, but also great risks for fundamental rights and democracies based on the rule of law; 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, human capabilities and safety;

B. whereas despite continuing advances in computer processing speed and memory capacity, there are as yet no programs that can match human flexibility over wider domains or in tasks requiring understanding of context or critical analysis; whereas, some AI applications have attained the performance levels of human experts and professionals in performing certain specific tasks (e.g. legal tech), and can provide results at a drastically higher speed and wider scale;

C. whereas some countries, including several Member States, make more use of AI applications, or embedded AI systems, in law enforcement and the judiciary than others, which is partly due to a lack of regulation and regulatory differences which enable or prohibit AI use for certain purposes; whereas the increasing use of AI in the criminal law field is based in particular on the promises that it would reduce certain types of crime and lead to more objective decisions; whereas these promises, however, do not always hold true;

D. whereas fundamental rights and freedoms enshrined in the Charter should be guaranteed throughout the life cycle of AI and related technologies, notably during their design, development, deployment and use, and should apply to the enforcement of the law in all circumstances;

E. whereas AI technology should be developed in such a way as to put people at its centre, be worthy of public trust and always work in the service of humans; whereas AI systems should have the ultimate guarantee of being designed so that they can always be shut down by a human operator;

F. whereas AI systems need to be designed for the protection and benefit of all members of society (including consideration of vulnerable, marginalised populations in their design), be non-discriminatory, safe, their decisions be explainable and transparent, and respect human autonomy and fundamental rights, in order to be trustworthy, as described in the Ethics Guidelines of the High-Level Expert Group on Artificial Intelligence;

G. whereas the Union together with the Member States bears a critical responsibility for ensuring that decisions surrounding the life cycle and use of AI applications in the field of the judiciary and law enforcement are made in a transparent manner, fully safeguard fundamental rights, and in particular do not perpetuate discrimination, biases or prejudices where they exist; whereas the relevant policy choices should respect the principles of necessity and proportionality in order to guarantee constitutionality and a fair and humane justice system;

H. whereas AI applications may 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, online sexual abuse and exploitation of children as well as certain types of cybercrime, thereby contributing to the safety and security of EU citizens, while at the same time they may entail significant risks for the fundamental rights of people; whereas any blanket application of AI for the purpose of mass surveillance would be disproportionate;

I. whereas the development and operation of AI systems for police and judicial authorities involves the contribution of multiple individuals, organisations, machine components, software algorithms, and human users in often complex and challenging environments; whereas the applications of AI in law enforcement and the judiciary are in different stages of development, ranging from conceptualisation through prototyping or evaluation to post-approval use; whereas new possibilities for use may arise in the future as technologies become more mature owing to ongoing scientific research worldwide;

J. whereas a clear model for assigning legal responsibility for the potential harmful effects of AI systems in the field of criminal law is imperative; whereas regulatory provisions in this field should always maintain human accountability and must aim, first and foremost, to avoid causing any harmful effects to begin with;

K. whereas it is ultimately the responsibility of the Member States to guarantee the full respect of fundamental rights when AI systems are used in the field of law enforcement and the judiciary;

L. whereas the relationship between protecting fundamental rights and effective policing must always be an essential element in the discussions on whether and how AI should be used by the law enforcement sector, where decisions may have long-lasting consequences on the life and freedom of individuals; whereas this is particularly important as AI has the potential to be a permanent part of our criminal justice ecosystem providing investigative analysis and assistance;

M. whereas AI is in use by law enforcement in applications such as facial recognition technologies, e.g. to search suspect databases and identify victims of human trafficking or child sexual exploitation and abuse, 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, advanced virtual autopsy tools to help determine cause of death, autonomous tools to identify financial fraud and terrorist financing, social media monitoring (scraping and data harvesting for mining connections), and automated surveillance systems incorporating different detection capabilities (such as heartbeat detection and thermal cameras); whereas the aforementioned applications, alongside other potential or future applications of AI technology in law enforcement, can have vastly varying degrees of reliability and accuracy and impact on the protection of fundamental rights and on the dynamics of criminal justice systems; whereas many of these tools are used in non-EU countries but would be illegal under the Union data protection aquis and case law; whereas the routine deployment of algorithms, even with a small false positive rate, can result in false alerts outnumbering correct alerts by far;

N. whereas AI tools and applications are also used by the judiciary in several countries worldwide, including to support decisions on pre-trial detention, in sentencing, calculating probabilities for reoffending and in determining probation, online dispute resolution, case law management and the provision of facilitated access to the law; whereas this has led to distorted and diminished chances for people of colour and other minorities; whereas at present in the EU, with the exception of some Member States, their use is limited mainly to civil matters;

O. whereas 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, as well as risks for the freedom and security of individuals;

P. whereas AI systems used by law enforcement and the judiciary are also vulnerable to AI-empowered attacks against information systems or data poisoning, whereby a wrong data set is included on purpose in order to produce biased results; 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;

Q. whereas, the deployment of AI in the field of law enforcement and the judiciary should not be seen as a mere technical feasibility, but rather a political decision concerning the design and the objectives of law enforcement and of criminal justice systems; whereas modern criminal law is based on the idea that authorities react to an offence after it has been committed, without assuming that all people are dangerous and need to be constantly monitored in order to prevent potential wrongdoing; whereas AI-based surveillance techniques deeply challenge this approach and render it urgent that legislators worldwide thoroughly assess the consequences of allowing the deployment of technologies that diminish the role of human beings in law enforcement and adjudication;

1. Reiterates that, as processing large quantities of personal 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; recalls, therefore that the EU has already established data protection standards for law enforcement, which form the foundation for any future regulation in AI for the use of law enforcement and the judiciary; recalls that processing of personal data should be lawful and fair, the purposes of processing should be specified, explicit and legitimate, processing should be adequate, relevant and not excessive in relation to the purpose for which is it processed, it should be accurate, kept up to date and inaccurate data should, unless restrictions apply, be corrected or erased, data should not be kept longer than is necessary, clear and appropriate time limits should be established for erasure or for periodic review of the need for storage of such data, and it should be processed in a secure manner; underlines also that possible identification of individuals by an AI application using data that was previously anonymised, should be prevented;

2. Reaffirms 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; stresses that use of AI applications must be prohibited when incompatible with fundamental rights;

3. Acknowledges that the speed at which AI applications are being developed around the world does not allow for an exhaustive listing of applications and thus necessitates a clear and coherent governance model guaranteeing both the fundamental rights of individuals and legal clarity for developers, considering the continuous evolution of technology; considers, however, given the role and responsibility of police and judicial authorities, and the impact of decisions they take for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, that 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;

4. Considers, in this regard, that 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, and that 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; highlights that trust among citizens in the use of AI developed, deployed and used in the EU is conditional upon the full fulfilment of these criteria;

5. Acknowledges the positive contribution of certain types of AI applications to the work of law enforcement and judicial authorities across the Union; highlights, as an example, the enhanced case law management achieved by tools allowing for additional search options; believes that there is a range of other potential uses for AI for law enforcement and the judiciary which could be explored while taking into consideration the five principles of the Ethical Charter on the use of artificial intelligence in judicial systems and their environment, adopted by the CEPEJ, and paying particular attention to the ‘uses to be considered with the most extreme reservation’, identified by the CEPEJ;

6. Underlines that any technology can be repurposed and therefore calls for strict democratic control and independent oversight of any AI-enabled technology in use by law enforcement and judicial authorities, especially those that can be repurposed for mass surveillance or mass profiling; notes, thus, with great concern the potential of certain AI technologies used in the law enforcement sector for mass surveillance purposes; highlights the legal requirement to prevent mass surveillance by means of AI technologies, which by definition does not fulfil the principles of necessity and proportionality, and to ban the use of applications that could result in it;

7. Emphasises that the approach taken in some non-EU countries regarding the development, deployment and use of mass surveillance technologies disproportionately interferes with fundamental rights and thus is not to be followed by the EU; stresses

therefore that safeguards against the misuse of AI technologies by law enforcement and judicial authorities also need to be regulated uniformly across the Union;

8. Stresses the potential for bias and discrimination arising from the use of AI applications such as machine learning, including the algorithms on which such applications are based; 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; points out that the results provided by AI applications are necessarily influenced by the quality of the data used, and that such inherent biases are inclined to gradually increase and thereby perpetuate and amplify existing discrimination, in particular for persons belonging to certain ethnic groups or racialised communities;

9. Underlines the fact that 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; recalls that individuals not only have the right to be correctly identified, but they also have the right not to be identified at all, unless it is required by law for compelling and legitimate public interests; stresses that AI predictions based on characteristics of a specific group of persons end up amplifying and reproducing existing forms of discrimination; considers that strong efforts should be made to avoid automated discrimination and bias; calls for robust additional safeguards where AI systems in law enforcement or the judiciary are used on or in relation to minors;

10. Highlights the power asymmetry between those who employ AI technologies and those who are subject to them; stresses that it is imperative that use of AI tools by law enforcement and judicial authorities does not become a factor of inequality, social fracture or exclusion; underlines the impact of the use of AI tools on the defence rights of suspects, the difficulty in obtaining meaningful information on their functioning and the consequent difficulty in challenging their results in court, in particular by individuals under investigation;

11. Takes note of the risks related in particular to data leaks, data security breaches and unauthorised access to personal data and other information related to, for example. criminal investigations or court cases that is processed by AI systems; underlines that security and safety aspects of AI systems used in law enforcement and by the judiciary need to be considered carefully and be sufficiently robust and resilient to prevent the potentially catastrophic consequences of malicious attacks on AI systems; stresses the importance of security by design, as well as specific human oversight before operating certain critical applications and therefore calls for law enforcement and judicial authorities only to use AI applications that adhere to the privacy and data protection by design principle in order to avoid function creep;

12. Stresses that no AI system used by law enforcement or the judiciary should be enabled to harm the physical integrity of human beings, nor to distribute rights or impose legal obligations on individuals;

13. Recognises the challenges to the correct location of legal responsibility and liability for

potential harm, given the complexity of development and operation of AI systems; considers it necessary to create a clear and fair regime for assigning legal responsibility and liability for the potential adverse consequences produced by these advanced digital technologies; underlines, however, that the aim must, first and foremost, be to prevent any such consequences materialising to begin with; calls, therefore, for the application of the precautionary principle in all applications of AI in the context of law enforcement; underlines that legal responsibility and liability must always rest with a natural or legal person, who must always be identified for decisions taken with the support of AI; emphasises, therefore, the need to ensure the transparency of the corporate structures that produce and manage AI systems;

14. Considers it essential, both for the effectiveness of the exercise of defence rights and for the transparency of national criminal justice systems, that a specific, clear and precise legal framework regulates the conditions, modalities and consequences of the use of AI tools in the field of law enforcement and the judiciary, as well as the rights of targeted persons, and effective and easily available complaint and redress procedures, including judicial redress; underlines the right of the parties to a criminal proceeding to have access to the data collection process and the related assessments made by or obtained through the use of AI applications; underlines the need for executing authorities involved in judicial cooperation, when deciding on a request for extradition (or surrender) to another Member State or non-EU country, to assess whether the use of AI tools in the requesting country might manifestly compromise the fundamental right to a fair trial; calls on the Commission to issue guidelines on how to conduct such an assessment in the context of judicial cooperation in criminal matters; insists that Member States, in accordance with applicable laws, should ensure that individuals are informed when they are subject to the use of AI applications by law enforcement authorities or the judiciary;

15. Points out that if humans only rely on the data, profiles and recommendations generated by machines, they will not be able to conduct an independent assessment; highlights the potentially grave adverse consequences, specifically in the area of law enforcement and justice, when individuals overly trust in the seemingly objective and scientific nature of AI tools and fail to consider the possibility of their results being incorrect, incomplete, irrelevant or discriminatory; emphasises that over-reliance on the results provided by AI systems should be avoided, and stresses the need for authorities to build confidence and knowledge to question or override an algorithmic recommendation; considers it important to have realistic expectations on such technological solutions and not to promise perfect law enforcement solutions and detection of all offences committed;

16. Underlines that in judicial and law enforcement contexts, the decision giving legal or similar effect always needs to be taken by a human, who can be held accountable for the decisions made; considers that those subject to AI-powered systems must have recourse to remedy; recalls that, under EU law, a person has the right not to be subjected to a decision which produces legal effects concerning them or significantly affects them and is based solely on automated data processing; underlines further that automated individual decision-making must not be based on special categories of personal data, unless suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place; stresses that EU law prohibits profiling that results in discrimination against natural persons on the basis of special categories of personal

data; highlights that decisions in the field of law enforcement are almost always decisions that have a legal effect on the person concerned, owing to the executive nature of law enforcement authorities and their actions; notes that the use of AI may influence human decisions and have an impact on all phases of criminal procedures; takes the view, therefore, that authorities making use of AI systems need to uphold extremely high legal standards and ensure human intervention, especially when analysing data deriving from such systems; requires therefore the sovereign discretion of judges and decision-making on a case-by-case basis to be upheld; calls for a ban on the use of AI and related technologies for proposing judicial decisions;

17. Calls 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, and that there is transparency on the source data and how the system arrived at a certain conclusion; points out that in order to ensure technical transparency, robustness, and accuracy, only such tools and systems should be allowed to be purchased by law enforcement or judiciary authorities in the Union whose algorithms and logic is auditable and accessible at least to the police and the judiciary as well as the independent auditors, to allow for their evaluation, auditing and vetting, and that they must not be closed or labelled as proprietary by the vendors; points out, furthermore, that documentation should be provided in clear, intelligible language about the nature of the service, the tools developed, the performance and conditions under which they can be expected to function and the risks that they might cause; calls therefore on judicial and law enforcement authorities to provide for proactive and full transparency on private companies providing them with AI systems for the purposes of law enforcement and the judiciary; recommends therefore the use of open source software where possible;

18. Encourages law enforcement and judicial authorities to identify and assess the areas where some tailor-made AI solutions might be beneficial and to exchange best practices on AI deployment; calls for the adoption by Member States and EU agencies of appropriate public procurement processes for AI systems when used in a law enforcement or judicial context, so as to ensure their compliance with fundamental rights and applicable legislation, including ensuring that software documentation and algorithms are available and accessible to the competent and supervisory authorities for review; calls, in particular, for binding rules requiring public disclosure on public-private partnerships, contracts and acquisitions and the purpose for which they are procured; stresses the need to provide the authorities with the necessary funding, as well as to equip them with the necessary expertise to guarantee full compliance with the ethical, legal and technical requirements attached to any AI deployment;

19. Calls for traceability of AI systems and the decision-making process that outlines their functions, defines the capabilities and limitations of the systems, and keeps track of where the defining attributes for a decision originate, through compulsory documentation; underlines the importance of keeping full documentation of training data, its context, purpose, accuracy and side effects, as well as its processing by the builders and developers of the algorithms and its compliance with fundamental rights;

highlights that it must always be possible to reduce the computations of an AI system to a form that is comprehensible to humans;

20. 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 the judiciary, in order to assess any potential risks to fundamental rights; recalls that the prior data protection impact assessment is mandatory for any type of processing, in particular, using new technologies, that is likely to result in a high risk to the rights and freedoms of natural persons and is of the opinion that this is the case for most AI technologies in the area of law enforcement and judiciary; underlines the expertise of data protection authorities and fundamental rights agencies in assessing these systems; stresses that these fundamental rights impact assessments should be conducted as openly as possible and with the active engagement of civil society; demands that the impact assessments also clearly define the safeguards necessary to address the identified risks and that they be made, to the greatest extent possible, publicly available before the deployment of any AI system;

21. Stresses that only robust European AI governance with independent evaluation can enable the necessary operationalisation of fundamental rights principles; calls 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, by an independent authority, to test and evaluate algorithmic systems, their context, purpose, accuracy, performance and scale, and, once they are in operation, in order to detect, investigate, diagnose and rectify any unwanted and adverse effects and to ensure the AI systems are performing as intended; calls therefore for a clear institutional framework for this purpose, including proper regulatory and supervisory oversight, to ensure full implementation and to guarantee a fully informed democratic debate on the necessity and proportionality of AI in the field of criminal justice; underlines that the results of these audits should be made available in public registers so that citizens know the AI systems being deployed and which measures are taken to remedy any violation of fundamental rights;

22. Stresses that the datasets and algorithmic systems used when making classifications, assessments and predictions at the different stages of data processing in the development of AI and related technologies may also result in differential treatment and both direct and indirect discrimination of groups of people, especially as data used to train predictive policing algorithms reflects ongoing surveillance priorities and consequently may end up reproducing and amplifying current biases; emphasises therefore that AI technologies, especially when deployed for the use of law enforcement and the judiciary, require inter-disciplinary research and input, including from the fields of science and technology studies, critical race studies, disability studies, and other disciplines attuned to social context, including how difference is constructed, the work of classification, and its consequences; stresses the need therefore to systematically invest in integrating these disciplines into AI study and research at all levels; stresses also the importance for the teams that design, develop, test, maintain, deploy and procure these AI systems for law enforcement and judiciary of reflecting, where possible, the diversity of society in general as a non-technical means to reduce the risks of discrimination;

23. Highlights further that adequate accountability, responsibility, and liability require significant specialised training with regard to the ethical provisions, potential dangers, limitations, and proper use of AI technology, especially for police and judiciary personnel; emphasises that suitable professional training and qualifications should ensure that decision-makers are trained about the potential for bias, as the data sets may be based on discriminatory and prejudiced data; supports the establishment of awareness-raising and educational initiatives to ensure that individuals working in law enforcement and the judiciary are aware of and understand the limitations, capabilities and risks that the use of AI systems entails, including the risk of automation bias; recalls that the inclusion in AI training data sets of instances of racism by police forces in fulfilling their duties will inevitably lead to racist bias in AI-generated findings, scores, and recommendations; reiterates its call on Member States, therefore, to promote anti-discrimination policies and to develop national action plans against racism in the field of policing and the justice system;

24. Notes that predictive policing is among the AI applications used in the area of law enforcement, but warns that while predictive policing can analyse the given data sets for the identification of patterns and correlations, it cannot answer the question of causality and cannot make reliable predictions on individual behaviour, and therefore cannot constitute the sole basis for an intervention; points out that several cities in the United States have ended their use of predictive policing systems after audits; recalls that during the LIBE Committee's mission to the United States in February 2020, Members were informed by the police departments of New York City and Cambridge, Massachusetts, that they had phased out their predictive policing programmes due to a lack of effectiveness, discriminatory impact and practical failure, and had turned instead to community policing; notes that this has led to a decline in crime rates; opposes, therefore, the use of AI by law enforcement authorities to make behavioural predictions on individuals or groups on the basis of historical data and past behaviour, group membership, location, or any other such characteristics, thereby attempting to identify people likely to commit a crime;

25. Notes the different types of use of facial recognition, such as, but not limited to, verification/authentication (i.e. matching a live face to a photo in an ID document, e.g. smart borders), identification (i.e. matching a photo against a set database of photos) and detection (i.e. detecting faces in real time from sources such as CCTV footage, and matching them to databases, e.g. real-time surveillance), each of which carry different implications for the protection of fundamental rights; strongly believes that the deployment of facial recognition systems by law enforcement should be limited to clearly warranted purposes in full respect of the principles of proportionality and necessity and the applicable law; reaffirms that as a minimum, the use of facial recognition technology must comply with the requirements of data minimisation, data accuracy, storage limitation, data security and accountability, as well as being lawful, fair and transparent, and following a specific, explicit and legitimate purpose that is clearly defined in Member State or Union law; is of the opinion verification and authentication systems can only continue to be deployed and used successfully if their adverse effects can be mitigated and the above criteria fulfilled;

26. Calls, furthermore, 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;

27. Calls, however, 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, results derived are non-biased and non-discriminatory, the legal framework provides strict safeguards against misuse and strict democratic control and oversight, and there is empirical evidence of the necessity and proportionality for the deployment of such technologies; notes that where the above criteria are not fulfilled, the systems should not be used or deployed;

28. Expresses its great concern over the use of private facial recognition databases by law enforcement actors and intelligence services, such as Clearview AI, a database of more than three billion pictures that have been collected illegally from social networks and other parts of the internet, including from EU citizens; calls on Member States to oblige law enforcement actors to disclose whether they are using Clearview AI technology, or equivalent technologies from other providers; recalls the opinion of the European Data Protection Board (EDPB) that the use of a service such as Clearview AI by law enforcement authorities in the European Union would 'likely not be consistent with the EU data protection regime'; calls for a ban on the use of private facial recognition databases in law enforcement;

29. Takes note of the Commission's feasibility study on possible changes to the Prüm Decision[8], including regarding facial images; takes note of earlier research that no potential new identifiers, e.g. iris or facial recognition, would be as reliable in a forensic context as DNA or fingerprints; reminds the Commission that any legislative proposal must be evidence based and respect the principle of proportionality; urges the Commission not to extend the Prüm Decision framework unless there is solid scientific evidence of the reliability of facial recognition in a forensic context compared to DNA or fingerprints, after it has conducted a full impact assessment, and taking into account the recommendations of the European Data Protection Supervisor (EDPS) and EDPB;

30. Stresses that the use of biometric data relates more broadly to the principle of the right to human dignity forming the basis of all fundamental rights guaranteed by the Charter; considers that the use and collection of any biometric data for remote identification purposes, for example by conducting facial recognition in public places, as well as at automatic border control gates used for border checks at airports, may pose specific risks to fundamental rights, the implications of which could vary considerably depending on the purpose, context and scope of use; further highlights the contested scientific validity of affect recognition technology, such as cameras detecting eye movements and changes in pupil size, in a law enforcement context; is of the view that the use of biometric identification in the context of law enforcement and the judiciary should always be considered 'high risk' and therefore be subjected to additional requirements, as per the recommendations of the Commission's High-Level Expert Group on AI;

31. Expresses strong concern over research projects financed under Horizon 2020 that

[8] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. OJ L 210, 6.8.2008, p. 1.

deploy artificial intelligence on external borders, such as the iBorderCtrl project, a ‘smart lie-detection system’ profiling travellers on the basis of a computer-automated interview taken by the traveller’s webcam before the trip, and an artificial intelligence-based analysis of 38 microgestures, tested in Hungary, Latvia and Greece; calls on the Commission, therefore, to implement, through legislative and non-legislative means, and if necessary through infringement proceedings, a ban on any processing of biometric data, including facial images, for law enforcement purposes that leads to mass surveillance in publicly accessible spaces; calls further on the Commission to stop funding biometric research or deployment or programmes that are likely to result in indiscriminate mass surveillance in public spaces; highlights, in this context, that special attention should be paid, and a strict framework applied, to the use of drones in police operations;

32. Supports the recommendations of the Commission’s High-Level Expert Group on AI advocating for a ban on AI-enabled mass scale scoring of individuals; considers that any form of normative citizen scoring on a large scale by public authorities, in particular within the field of law enforcement and the judiciary, leads to the loss of autonomy, endangers the principle of non-discrimination and cannot be considered in line with fundamental rights, in particular human dignity, as codified in EU law;

33. Calls for greater overall transparency in order to form a comprehensive understanding regarding the use of AI applications in the Union; requests that Member States provide comprehensive information on the tools used by their law enforcement and judicial authorities, the types of tools in use, the purposes for which they are used, the types of crime they are applied to, and the names of the companies or organisations that developed those tools; calls on law enforcement and judicial authorities also to inform the public and provide sufficient transparency as to their use of AI and related technologies when implementing their powers, including disclosure of false positive and false negative rates of the technology in question; requests that the Commission compile and update the information in a single place; calls on the Commission to also publish and update information concerning the use of AI by the Union agencies charged with law enforcement and judicial tasks; calls on the EDPB to assess the legality of these AI technologies and applications in use by law enforcement authorities and the judiciary;

34. Recalls that AI applications, including those used in the context of law enforcement and the judiciary, are being developed globally at a rapid pace; urges all European stakeholders, including the Member States and the Commission, to ensure, through international cooperation, the engagement of partners outside the EU in order to raise standards at international level and to find a common and complementary legal and ethical framework for the use of AI, in particular for law enforcement and the judiciary, that fully respects the Charter, the European data protection acquis and human rights more widely;

35. Calls for the EU Fundamental Rights Agency, in collaboration with the EDPB and the EDPS, to draft comprehensive guidelines, recommendations and best practices in order to further specify the criteria and conditions for the development, use and deployment of AI applications and solutions for use by law enforcement and judicial authorities; undertakes to conduct a study on the implementation of the Law Enforcement

Directive[9] in order to identify how the protection of personal data has been ensured in processing activities by law enforcement and judicial authorities, particularly when developing or deploying new technologies; calls on the Commission, furthermore, to consider whether specific legislative action on further specifying the criteria and conditions for the development, use and deployment of AI applications and solutions by law enforcement and judicial authorities is needed;

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

[9] 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. OJ L 119, 4.5.2016, p. 89.

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.

3.9.2020

OPINION OF THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION

for the Committee on Civil Liberties, Justice and Home Affairs

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

Rapporteur for opinion: Marcel Kolaja

SUGGESTIONS

The Committee on the Internal Market and Consumer Protection calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to incorporate the following suggestions into its motion for a resolution:

A. whereas, in view of both the positive societal potential and the inherent risks of artificial intelligence (AI), the functioning of the digital single market should be improved by reinforcing legal certainty for providers of AI systems, and also reinforcing consumer trust and security by strengthening safeguards to ensure the rule of law and respect for fundamental rights, in particular the right to privacy and protection of personal data, the right to equality and non-discrimination, the right to good administration, the right to a fair trial, and the right to a high level of consumer protection; whereas a common European approach to AI and the regulation of its use in criminal matters by police and law enforcement is necessary in order to avoid fragmentation in the single market;

B. whereas the testing and use of AI by police and judicial authorities is widespread, entailing different types of uses, consequences and risks, namely facial recognition systems, DNA profiling, predictive crime mapping, mobile phone data extraction, advanced case-law search engines, online dispute resolution, and machine learning for the administration of justice;

C. whereas the use of AI can represent a paradigm shift in the administration of criminal justice;

D. whereas according to the report by the Fundamental Rights Agency there is still only limited information currently available on the possible use or testing of facial recognition technologies in Member States[1];

E. whereas in those Member States where some information was available on the use of facial recognition technologies, data protection authorities found that the use of these technologies did not comply with data protection law and lacked a legal basis for their deployment;

F. whereas in the field of the internal market, by reforming public procurement procedures the Union can make a fundamental difference in aligning government actions and behaviour with secondary policy objectives such as data protection and non-discrimination;

G. whereas discrimination in data-driven algorithmic decision-making can occur during the design, testing, and implementation phase, through the biases that are incorporated in the datasets or the algorithms;

H. whereas a principle-based technical development and application of AI is necessary to ensure compliance with human and fundamental rights;

I. whereas on 4 December 2018 the European Commission for the Efficiency of Justice of the Council of Europe published the Ethical Charter for the Use of Artificial Intelligence in Judicial Systems, which sets out ethical principles for the use of AI in judicial systems;

J. whereas certain uses of AI technologies are particularly sensitive and prone to abuse, and this has recently led some technology companies to decide to stop offering related software;

1. Considers that AI used by police and judicial authorities has to be generally categorised as high-risk and treated with the utmost care and the highest standards of data protection, given the role of these authorities in defending the public interest and in view of the nature of their responsibilities; considers that there is an urgent need for a common European regulatory framework for AI in the internal market; believes that the EU should take the lead in laying down regulation at Union level, including on public procurement, based on clear rules and fundamental rights and ethics, in the development and use of AI so as to ensure the same high level of consumer protection and uniform industry standards across the EU, with a view to enabling a better functioning of the internal market while encouraging innovation and fostering legal certainty for businesses, especially SMEs; calls on the Commission to scrutinise the application of existing legislation and its enforcement prior to initiating any possible new legislative proposals;

2. Recognises that the use of AI in the field of justice can help improve the efficiency and quality of proceedings; stresses in this context that in particular it is necessary to respect the rules laid down in the European Convention for Human Rights and in the Council of Europe Convention for the Protection of Individuals with regard to Automatic

[1] European Union Agency for Fundamental Rights: Facial recognition technology: fundamental rights considerations in the context of law enforcement (FRA Focus), 27 November 2019 - https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

Processing of Personal Data;

3. Calls on the Commission to assess the AI technology available on the market and the level of use by police and judicial authorities on a country-by-country basis;

4. Stresses that AI should help to ease the administrative burden on public authorities and increase the efficiency of their decision-making, and that AI systems should always rely on human oversight, collaboration and coordination; in this regard, highlights that humans should always bear the ultimate responsibility for any decision-making in criminal matters; stresses the importance of accurate data sets, when these are used to assist related e-government processes and administrative decision-making across the Union;

5. Emphasises the importance of enabling innovation, transparency, traceability and verification; stresses that open-source AI could contribute to this while also strengthening cooperation and fostering a culture of exchanging ideas and experiences relating to the use and creation of algorithms;

6. Considers that AI used by police and law enforcement in criminal matters should be released as open source software where possible under the public procurement procedure, in compliance with the applicable legislation, including Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market, with software documentation and algorithms being accessible and thus allowing competent authorities to review how the AI system arrived at a certain conclusion; emphasises that a fundamental rights audit should be part of a prior conformity assessment; believes that, while ensuring respect for EU law and values and the applicable data protection rules, and without jeopardising investigations or criminal prosecutions, explainable and unbiased algorithms that meet the obligation of sufficient transparency, as well as the use of open data for training in compliance with the applicable legislation, including Directive (EU) 2019/1024 on open data and the re-use of public sector information without prejudice to Regulation (EU) 2016/679, are essential to ensure that businesses and citizens including consumers can trust in, and benefit from, better, accessible, non-discriminatory and reliable public services at a fair cost;

7. Emphasises that AI-based data collection and the monitoring of individuals should be limited to criminal suspects and court-approved surveillance in accordance with applicable national laws, taking into account respect for private life and the presumption of innocence, including that of other users and consumers who may be inadvertently affected by such systems and practices; emphasises that where decision-making is assisted by statistical calculations, suitable professional training and qualifications should ensure that decision-makers are trained about the potential for bias, as data sets may be based on discriminatory and prejudiced data; highlights in this regard the importance of the quality of algorithms and original data, and recalls that the use of AI must be based on the principle of non-discrimination in data entry and analyses; calls for procurement procedures for such applications to contain safeguards against possible biases; calls for exchanges of information and best practices regarding the application of AI techniques and tools by judicial and police authorities in Member States, in order to avoid a fragmented approach in the single market and ensure the protection of

consumers and citizens across the Union;

8. Insists that Member States, in accordance with applicable criminal laws, should ensure that citizens and consumers are informed when they are subject to the use of AI and that simple, effective and easily accessible complaint and redress procedures, including judicial redress, should be made available to citizens in order to allow them to effectively defend their rights;

9. Recalls the high risk of certain types of AI, including facial recognition technologies in public spaces, automated behaviour detection and profiling to divide people into risk categories at borders, biometric detection and recognition for mass surveillance, mass-scale citizen scoring, and predictive policing, and calls on the Commission to regulate the procurement and use thereof in order to eliminate the risk of abuse; in this regard, welcomes the Commission’s ongoing work to assess the use of biometric technologies and consider regulatory options, including a risk-based approach and a ban on them in specific circumstances, as well as introducing necessary safeguards where their use is justified;

10. Underlines that the sovereign discretion of judges and case-by-case decision-making have to be upheld in order to avoid the standardisation of decisions based on purely statistical calculations.

INFORMATION ON ADOPTION IN COMMITTEE ASKED FOR OPINION

Date adopted	3.9.2020
Result of final vote	+: 40 –: 4 0: 0
Members present for the final vote	Alex Agius Saliba, Andrus Ansip, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoş, Markus Buchheit, Dita Charanzová, Deirdre Clune, David Cormand, Petra De Sutter, Carlo Fidanza, Evelyne Gebhardt, Sandro Gozi, Maria Grapini, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Marcel Kolaja, Kateřina Konečná, Andrey Kovatchev, Jean-Lin Lacapelle, Maria-Manuel Leitão-Marques, Morten Løkkegaard, Adriana Maldonado López, Antonius Manders, Beata Mazurek, Leszek Miller, Dan-Ștefan Motreanu, Kris Peeters, Anne-Sophie Pelletier, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Kim Van Sparrentak, Marion Walsmann, Marco Zullo
Substitutes present for the final vote	Maria da Graça Carvalho, Anna Cavazzini, Krzysztof Hetman

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

40	+
EPP	Maria da Graça Carvalho, Deirdre Clune, Krzysztof Hetman, Arba Kokalari, Andrey Kovatchev, Antonius Manders, Dan-Ştefan Motreanu, Kris Peeters, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Marion Walsmann
S&D	Alex Agius Saliba, Brando Benifei, Biljana Borzan, Evelyne Gebhardt, Maria Grapini, Maria-Manuel Leitão-Marques, Adriana Maldonado López, Leszek Miller, Christel Schaldemose
RENEW	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Sandro Gozi, Svenja Hahn, Morten Løkkegaard
ID	Hynek Blaško
GREENS/EFA	Anna Cavazzini, David Cormand, Petra De Sutter, Marcel Kolaja, Kim Van Sparrentak
ECR	Adam Bielan, Carlo Fidanza, Eugen Jurzyca, Beata Mazurek
EUL/NGL	Kateřina Konečná, Anne-Sophie Pelletier
NI	Marco Zullo

4	-
ID	Alessandra Basso, Markus Buchheit, Virginie Joron, Jean-Lin Lacapelle

0	0

Key to symbols:
+ : in favour
- : against
0 : abstention

15.9.2020

OPINION OF THE COMMITTEE ON LEGAL AFFAIRS

for the Committee on Civil Liberties, Justice and Home Affairs

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

Rapporteur for opinion: Angel Dzhambazki

SUGGESTIONS

The Committee on Legal Affairs calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to incorporate the following suggestions into its motion for a resolution:

A. whereas the right to fair trial is a fundamental and legally binding right enshrined in the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights for the purposes of law enforcement; whereas it applies throughout the entirety of criminal proceedings, including in law enforcement, and its safeguarding rules out, at all stages of the procedure, the taking of measures, including technical measures, whose direct or indirect consequence is to deprive the rights of the defence of their substance; whereas the guarantees attaching to this principle, in particular those of an ‘independent court’, ‘equality before the law’ and the presumption of innocence, are more stringent in the area of criminal law; whereas these rights must be upheld in all circumstances, in particular in the context of the use of artificial intelligence (AI), especially given that AI-based technologies could have an impact on various human rights;

B. whereas the protection of personal data, in accordance with the General Data Protection Regulation (GDPR)[1] and other relevant legislation where applicable, applies at all times;

C. whereas AI and related technologies, including their self-learning abilities, always involve a certain level of human intervention;

[1] 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 (OJ L 119, 4.5.2016, p. 1).

D. whereas AI has the potential to become a permanent part of criminal law systems;

E. whereas AI and related technologies are a priority for the Union, given the fast-paced advances in the technology sector and the importance of being vigilant about their current and future impact on the unique European intellectual property rights system; whereas a variety of sectors are already implementing AI and related technologies, such as the robotics, transport and healthcare sectors to name but a few;

F. whereas technologies such as AI and related technologies could be used in the area of criminal law with the aim of reducing crime rates, facilitating certain procedures through their use in statistical data analytics in crime analysis and prevention, and detecting and investigating criminal cases; whereas the Union should further develop its capacities with regard to software, data storage and AI technologies in order to improve insufficiencies when it comes to data protection and privacy;

G. whereas these technologies can be used to create anonymised statistical databases that help authorities, academics and legislators to analyse figures and efficiently design policies to prevent criminality and help offenders to successfully reintegrate into society;

H. whereas the legal framework of AI and its application to criminal law should include legislative actions where required, starting with mandatory measures to prevent practices that would undoubtedly undermine fundamental rights and freedoms;

I. whereas owing to the intrinsically opaque nature of AI systems, the new tools used in criminal justice contexts might conflict with some fundamental freedoms;

J. whereas possible risks linked to the application of AI systems in criminal justice matters need to be prevented and mitigated in order to safeguard the fundamental rights of suspects and accused persons in criminal proceedings;

1. Emphasises the crucial importance of duly assessing the risks of using AI systems, such as discrimination and breaches of privacy, and of considering all the ethical and operational implications of the use of AI and related technologies in our society, in particular by state authorities, the police and judicial authorities in criminal justice systems, as well as liability and evidentiary issues in the case of potential errors associated with the operation of AI systems; considers that a clear regulatory framework is necessary for setting limits and providing the necessary safeguards; considers that ethical principles, such as those laid down in the Council of Europe’s European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment, should be taken into account and adhered to by public and private entities responsible for the initial design and development of AI tools and services, so that all social stakeholders can have comprehensive information on the corporate structures of companies that produce AI programmes; stresses the importance of the human factor, which must always be the final decision-maker in the use of AI technology-based software and within the criminal system, whether in police enforcement or criminal justice; reiterates that biometric recognition software should only be deployed in situations in which it is clearly warranted;

2. Stresses the need to establish and maintain a balance between the use of AI systems in

criminal proceedings and respect for all fundamental rights and procedural guarantees provided for under European and international law;

3. Emphasises the importance of AI being used with due respect for the principles of the rule of law and the independence of the judiciary in the decision-making process;

4. Calls on the Commission to further clarify the rules on the protection and sharing of the data collected through AI and related technologies by authorities authorised to collect and/or process such data, including non-personal and anonymised data that directly or indirectly identify individuals, with full respect for the GDPR and the ePrivacy Directive[2]; underlines, furthermore, that the right to a fair trial should encompass the right of citizens and litigants to access these data, especially when collected from their personal devices or equipment, in accordance with the GDPR, but also for the purposes of their right of defence as soon as their legal liability is engaged;

5. Underlines the importance of increasing the transparency of AI systems that are used in criminal justice matters in order to enable judicial oversight and of ensuring that developers of AI and related technologies provide for a sufficient level of transparency of algorithms and algorithmic decisions for the benefit of competent authorities and citizens; emphasises the general right of parties to be given access to processes relating to data collection, prognostic assessments used for crime prevention, the cataloguing and evaluation of criminal evidence and the determining of whether a suspect might be a danger to society if not restricted by existing EU law, such as Directive (EU) 2016/680[3]; underlines, in addition, the importance of being able to access AI-produced or AI-assisted outputs and, ultimately, of defining responsibility for notification procedures and the role of AI and related technologies in criminal matters, in particular with regard to the analysis of large amounts of evidence in criminal investigations and the identification of suspects or victims of crime; recalls the importance of questions related to governance, fundamental rights and procedural guarantees, non-discrimination, accountability, transparency, impartiality, fairness and the intellectual integrity of AI and related technologies, while stressing the need to ensure human oversight at all times; insists that judicial authorities must be obligated to justify their decisions, including when using elements of proof provided by AI-assisted technologies, which require a high level of judicial scrutiny and strict admissibility criteria, in keeping with its resolution of 16 February 2017 on robotics[4] which stresses that it should always be possible to supply the rationale behind any decision taken with the aid of AI that can have an impact on one or more persons' lives; recalls the distinction between the use of AI and related technologies in crime prevention and criminal justice; stresses that AI technologies must fulfil a subordinate role at all times;

6. Recalls that the most severe misuses of AI and related technologies, such as mass

[2] 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 (OJ L 201, 31.7.2002, p. 37).

[3] 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 (*OJ L 119, 4.5.2016, p. 89).*

[4] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (OJ C 252, 18.7.2018, p. 239).

surveillance, profiling and predictive policing programmes which could assess where crime is likely to occur, where suspects are likely to be located, a person's chances of victimisation, vulnerability, being reported missing or being the victim or the perpetrator of domestic violence or a sexual offence, and breaches of due process rights, can come from public authorities acting in law enforcement;

7. Underlines the importance of using auto-generated data in evidence collection and analysis; recalls that, in both crime prevention and criminal justice, errors in or the possible misuse of data-input and -output analysis, as well as interpretation thereof, may be rooted in the human factor involved and calls, therefore, for a cautious approach when analysing the effectiveness and appropriateness of using AI technologies in all decision-making processes;

8. Calls on all competent public authorities, particularly law enforcement authorities such as the police and the judiciary, to inform the public about and ensure sufficient transparency as to their use of AI and related technologies when implementing their powers, especially in criminal law matters;

9. Considers it vital that the application of AI systems in the context of criminal proceedings should ensure respect for the fundamental principles of criminal proceedings, including the right to a fair trial, the principle of the presumption of innocence and the right to an effective remedy, as well as ensuring monitoring and independent control of automated decision-making systems;

10. Underlines the importance of the human-in-command principle and verification of AI-produced or AI-assisted outputs; recalls the importance of questions related to governance, transparency, explainability and accountability to ensure respect for fundamental rights and avoid potential faults in the AI;

11. Stresses its cautious approach to the use of biometric recognition software; highlights the ambiguity resulting from an inherent insufficiency when it comes to data protection, as well as infringements of data privacy; notes with concern the amalgamation of personal data on citizens in the European Union by foreign countries, through private sector developers and providers;

12. Recalls that, in accordance with the current EU data protection rules and the Charter of Fundamental Rights of the European Union, AI can only be used for remote biometric recognition purposes, where such use is duly justified, proportionate and subject to adequate safeguards; welcomes the recommendations of the Commission's High-Level Expert Group on AI for a proportionate, considerate and risk-based use of biometric recognition technology in compliance with the legislation on the protection of personal data; suggests that the application of such technology must be clearly warranted under existing laws and suggests that the Commission assess how to effectively incorporate these recommendations, with particular regard to the right to privacy and the protection of personal data;

13. Strongly believes that decisions issued by AI or related technologies, especially in the areas of justice and law enforcement, that have a direct and significant impact on the rights and obligations of natural or legal persons should be subject to strict human verification and due process;

14. Considers it necessary to analyse whether it is expedient for law enforcement decisions to be partly delegable to AI and if so, under what conditions and in what regard such a use of AI could be allowed; considers that AI and related technologies that can replace public authority decisions should be treated with the utmost precaution; stresses the need to develop strong ethical principles and specific codes of conduct for the design and use of AI to help law enforcers and judicial authorities in the event that law enforcement decisions are delegated to AI; refers to the ongoing work in the Committee on Legal Affairs.

INFORMATION ON ADOPTION IN COMMITTEE ASKED FOR OPINION

Date adopted	10.9.2020
Result of final vote	+: 22 –: 3 0: 0
Members present for the final vote	Manon Aubry, Gunnar Beck, Geoffroy Didier, Angel Dzhambazki, Ibán García Del Blanco, Jean-Paul Garraud, Esteban González Pons, Mislav Kolakušić, Gilles Lebreton, Karen Melchior, Jiří Pospíšil, Franco Roberti, Marcos Ros Sempere, Liesje Schreinemacher, Stéphane Séjourné, Raffaele Stancanelli, Marie Toussaint, Adrián Vázquez Lázara, Axel Voss, Marion Walsmann, Tiemo Wölken, Lara Wolters, Javier Zarzalejos
Substitutes present for the final vote	Heidi Hautala, Emil Radev

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

22	+
EPP	Geoffroy Didier, Esteban González Pons, Jiří Pospíšil, Emil Radev, Axel Voss, Marion Walsmann, Javier Zarzalejos
S&D	Ibán García Del Blanco, Franco Roberti, Marcos Ros Sempere, Tiemo Wölken, Lara Wolters
RENEW	Karen Melchior, Liesje Schreinemacher, Stéphane Séjourné, Adrián Vázquez Lázara
ID	Gunnar Beck, Jean-Paul Garraud, Gilles Lebreton
ECR	Angel Dzhambazki, Raffaele Stancanelli
NI	Mislav Kolakušić

3	-
VERTS/ALE	Heidi Hautala, Marie Toussaint
GUE/NGL	Manon Aubry

0	0

Key to symbols:
+ : in favour
- : against
0 : abstention

INFORMATION ON ADOPTION IN COMMITTEE RESPONSIBLE

Date adopted	29.6.2021
Result of final vote	+: 36 –: 24 0: 6
Members present for the final vote	Magdalena Adamowicz, Konstantinos Arvanitis, Malik Azmani, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Joachim Stanisław Brudziński, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Jean-Paul Garraud, Maria Grapini, Sylvie Guillaume, Andrzej Halicki, Evin Incir, Sophia in 't Veld, Patryk Jaki, Marina Kaljurand, Fabienne Keller, Peter Kofod, Łukasz Kohut, Moritz Körner, Alice Kuhnke, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Sara Skyttedal, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Tomas Tobé, Dragoş Tudorache, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Elissavet Vozemberg-Vrionidi, Jadwiga Wiśniewska, Elena Yoncheva, Javier Zarzalejos
Substitutes present for the final vote	Tanja Fajon, Miguel Urbán Crespo

FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE

36	+
NI	Laura Ferrara, Martin Sonneborn
Renew	Malik Azmani, Anna Júlia Donáth, Sophia in ‘t Veld, Fabienne Keller, Moritz Körner, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu, Dragoş Tudorache
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Tanja Fajon, Maria Grapini, Sylvie Guillaume, Evin Incir, Marina Kaljurand, Łukasz Kohut, Juan Fernando López Aguilar, Javier Moreno Sánchez, Birgit Sippel, Bettina Vollath, Elena Yoncheva
The Left	Konstantinos Arvanitis, Pernando Barrena Arza, Cornelia Ernst, Miguel Urbán Crespo
Verts/ALE	Patrick Breyer, Saskia Bricmont, Damien Carême, Alice Kuhnke, Terry Reintke, Diana Riba i Giner, Tineke Strik
24	**-**
ID	Nicolas Bay, Nicolaus Fest, Jean-Paul Garraud, Marcel de Graaff, Peter Kofod, Annalisa Tardino, Tom Vandendriessche
NI	Milan Uhrík
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Andrzej Halicki, Jeroen Lenaers, Lukas Mandl, Roberta Metsola, Nadine Morano, Paulo Rangel, Ralf Seekatz, Sara Skyttedal, Tomas Tobé, Elissavet Vozemberg-Vrionidi, Javier Zarzalejos
6	**0**
ECR	Joachim Stanisław Brudziński, Jorge Buxadé Villalba, Patryk Jaki, Nicola Procaccini, Jadwiga Wiśniewska
PPE	Emil Radev

Key to symbols:
+ : in favour
- : against
0 : abstention