European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2021)0405

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

European Parliament resolution of 6 October 2021 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, in particular Articles 2 and 6 thereof, and to the Treaty on the Functioning of the European Union, 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 Intelligence 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 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,

---

1 OJ L 119, 4.5.2016, p. 1.
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 OJ C 362, 8.9.2021, p. 63.
7 OJ C 263, 25.7.2018, p. 82.

– 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 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[1], 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 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;

---

[1] 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).

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[1] 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.

---

[1] 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).