Committee on Civil Liberties, Justice and Home Affairs

2020/2013(INI)

23.11.2020

OPINION

of the Committee on Civil Liberties, Justice and Home Affairs

for the Committee on Legal Affairs

on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI))

Rapporteur for opinion: Patryk Jaki

PA_NonLeg

EN

SUGGESTIONS

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

–   having regard to Articles 2 and 3 of the Treaty on European Union (TEU),

–   having regard to Articles 10, 19, 21 and 167 of the Treaty on the Functioning of the European Union (TFEU),

–   having regard to the right to petition enshrined in Articles 20 and 227 of the TFEU and Article 44 of the Charter of Fundamental Rights of the European Union (EUCFR),

–   having regard to Articles 21 and 22 of the EUCFR,

–   having regard to the preamble to the TEU,

–   having regard to the Council of Europe's Framework Convention for the Protection of National Minorities, Protocol No 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms, and the European Charter for Regional or Minority Languages,

–   having regard to Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin[1] (Racial Equality Directive),

–   having regard to Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation[2] (Equal Treatment in Employment Directive),

–   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)[3] (GDPR), and 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[4],

–   having regard to the communication of 11 December 2019 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Green Deal,

---

[1] OJ L 180, 19.7.2000, p. 22.
[2] OJ L 303, 2.12.2000, p. 16.
[3] OJ L 119, 4.5.2016, p. 1.
[4] OJ L 119, 4.5.2016, p. 89.

EN

– having regard to its resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics[5],

– having regard to the OECD Council Recommendation on Artificial Intelligence adopted on 22 May 2019,

– having regard to its resolution of 12 September 2018 on autonomous weapon systems[6],

A. whereas the development and design of so-called 'artificial intelligence', robotics and related technologies are done by humans, and their choices determine the potential of technology to benefit society;

B. whereas ethical guidance, such as the principles adopted by the High-Level Expert Group on Artificial Intelligence, provides a good starting-point but is not enough to ensure that businesses act fairly and guarantee the effective protection of individuals;

1. Acknowledges the potentials and the risks offered by the development, deployment and use of artificial intelligence (AI) for security both within the EU and in its external relations; draws attention to the fact that many Member States use AI in both the civil and the military field, and underlines the importance of the EU playing a significant and adequate role in the future international discussions on this topic;

2. Notes the regulatory advances that some Member States have already made in the AI area; emphasises the importance of a common European approach which harmonises the legal situation across Member States and gives legal certainty to those developing and deploying AI;

3. Stresses the fact that the development, deployment, use and management of AI must respect the fundamental rights, values and freedoms expressed in the EU Treaties, and calls on Member States to refrain from deploying high-risk AI systems that pose threats to fundamental rights; takes note of the publication of the Commission's White Paper on Artificial Intelligence and encourages deeper research into the potential risk to fundamental rights of the use of AI by state authorities and by agencies, bodies and institutions of the European Union;

4. Stresses that in order to harness the opportunities offered by AI the EU should adopt an appropriate framework to mitigate the risks, ensure its ethical use, and prevent its use for malicious purposes; considers that such a framework should clearly determine appropriate liability, accountability, security and traceability regimes; underlines the importance of the EU helping to develop much-needed investment, data infrastructure, research and common ethical norms;

5. Stresses that the EU must be in the forefront of the creation of an international legal and ethical framework governing research and development, creation, use and maintenance in the area of AI that is rooted in the principles of human rights and counteracts and remedies potential risks; considers it necessary to create a clear and fair international regime for assigning legal responsibility for adverse consequences produced by these

---

[5] OJ C 252, 18.7.2018, p. 239.
[6] OJ C 433, 23.12.2019, p. 86.

EN

advanced digital technologies; underlines that first and foremost the aim must be to pre-empt such consequences;

6. Calls on the Commission to facilitate research into and discourse on opportunities of using AI in disaster relief, crisis prevention, and upholding peace;

7. Points to the clear risks in decisions made by humans if solely relying on the data, profiles and recommendations generated by machines; points out that the overall design of AI systems should also include guidelines on human supervision and oversight; calls for an obligation to be imposed regarding transparency and explainability of AI applications and the necessity of human intervention, as well as other measures, such as independent audits and specific stress tests to assist and enforce compliance; stresses that such audits should be conducted periodically by an independent authority, to supervise high-risk AI applications used by state authorities or the military;

8. Notes concerns that AI, when improperly designed and developed, may lead to bias and discrimination; commits to finding regulatory and policy solutions to ensure that discrimination, rather than being reinforced, is eliminated, through the use of existing and emerging technologies;

9. Underlines that making predictions from the processing of sharing of, access to and use of data must be governed in accordance with the requirements of quality, integrity, transparency, security, privacy and control; stresses the need, throughout the development, deployment and use of AI, robotics and related technologies, to respect the EU legal framework on data protection and privacy in order to increase citizens' safety and their trust in those technologies;

10. Observes the rapid development of AI applications to recognise unique characteristic elements, such as facial characteristics, movements and attitudes; warns about issues of invasion of privacy, non-discrimination and the protection of personal data related to the use of automated recognition applications;

11. Underlines that any decision about a natural person that is based solely on automated processing, including profiling, and which produces an adverse legal effect concerning the data subject or significantly affects that person, is prohibited under the GDPR unless authorised by Union or Member State law, subject to suitable measures to safeguard the data subject's rights and freedoms and legitimate interests;

12. Calls for explainability of algorithms, transparency and regulatory oversight when artificial intelligence is used by public authorities, and for impact assessments to be conducted before tools resorting to AI technologies are deployed by state authorities; calls on the Commission and the European Data Protection Board to issue guidelines, recommendations and best practices in order to further specify the criteria and conditions for decisions based on profiling and the use of AI by public authorities;

13. Calls for transparent and risk-reducing measures at international level regarding the development and use of military AI, in particular with regard to the principles of territorial integrity and non-intervention and concerning the use of force; stresses the importance of taking account of the military aspects when addressing legal and ethical issues in the European framework on AI; recalls its position on a ban on the

development, production and use of lethal autonomous weapons systems; regrets that no explicit conventions exist on a global scale on the use of such weapons;

14. Notes that certain AI technologies enable the automation of information processing and action to an unprecedented scale, as in the case of mass surveillance in the civil and military domains, which poses a threat to fundamental rights and paves the way for unlawful interference with national sovereignty; calls for the scrutiny of mass surveillance activities under international law jurisdiction and enforcement standards; expresses strong concerns about some highly intrusive social scoring applications that have been developed, as being highly dangerous for respect for fundamental rights; calls for an explicit ban on the use of mass-scale social scoring by public authorities to restrict the rights of citizens; considering the decisional hegemony and control of certain private actors over the development of such technologies, calls for strengthening the accountability of such private actors under international law;

15. Invites the Commission to assess the consequences of a moratorium on the use of facial recognition systems, and, depending on the results of such an assessment, to consider a moratorium on the use of those systems by public authorities in the public space and in premises meant for education and healthcare, and on the use of facial recognition systems by law enforcement authorities in semi-public spaces such as airports, until the technical standards can be considered fully fundamental rights-compliant, the results derived are non-biased and non-discriminatory, and there are strict safeguards against misuse and that ensure the necessity and proportionality of using such technologies;

16. Considers that artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies, regardless of the field in which they are used, should be developed in a secure and technically rigorous manner;

17. Stresses the importance of enabling the proper deployment and use of AI; calls on the Member States to provide their civil and military personnel with appropriate training in order to allow them to accurately identify and avoid discrimination and bias in datasets;

18. Notes that the use of AI in fighting crime and cybercrime could bring a wide range of possibilities and opportunities, while at the same time the principle that what is illegal offline is illegal online should continue to prevail;

19. Is deeply concerned about the deepfake technologies that allow increasingly realistic photo, audio and video forgeries to be produced that could be used to blackmail, to generate false news reports, or to erode public trust and influence public discourse; believes such practices have the potential of destabilising countries, spreading disinformation and influencing elections; calls, therefore, for an obligation for all deepfake material or any other realistically made synthetic videos to be labelled as 'not original' by the creator, with strict limits on their use for electoral purposes and strong enforcement; calls for adequate research in this regard to ensure that countering technologies keep pace with the malicious use of AI;

20. Stresses that the use of AI in justice could improve the analysis and collection of data and the protection of victims, and that this could be explored in research and development and accompanied by impact assessments, in particular regarding

safeguards for due process and against bias and discrimination, with the precautionary principle being applied; recalls, however, that this is no substitute for human beings in terms of sentencing or decision-making;

21. Emphasises the importance of cybersecurity for AI, in both offensive and defensive scenarios; notes in this regard the importance of international cooperation and of the publication and sharing of IT security vulnerabilities and remedies; calls for international cybersecurity cooperation for effective AI use and deployment, and for safeguards against misuse of AI and cyberattacks; notes in addition the dual-use nature of IT systems (i.e. use for civil and military purposes), and of AI, and calls for its effective regulation;

22. Calls on the Member States to consider the need to provide safeguards for the use of AI, such as rules on professional ethics; calls on the Commission to establish a clear set of criteria to determine the various levels of risk in domains for which AI technologies are designed or to which they are deployed, taking into consideration existing EU legislation;

23. Emphasises the importance of verifying how high-risk AI technologies arrive at a decision; recalls that the principle of proportionality needs to be respected and that questions of causality and liability need to be clarified;

24. Recalls the importance of the principles of governance, transparency, impartiality, accountability, fairness and intellectual integrity in the use of AI in criminal justice;

25. Urges the Member States to assess the risks related to AI-driven technologies before automating activities connected with the exercise of state authority, especially in the area of justice; calls on them to consider the need to provide safeguards, such as supervision by a qualified professional and rules on professional ethics.

INFORMATION ON ADOPTION IN COMMITTEE ASKED FOR OPINION

Date adopted	17.11.2020
Result of final vote	+: 56 –: 4 0: 0
Members present for the final vote	Malik Azmani, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Clare Daly, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Jean-Paul Garraud, Maria Grapini, Sylvie Guillaume, Andrzej Halicki, Evin Incir, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Peter Kofod, Łukasz Kohut, Alice Kuhnke, Moritz Körner, Jeroen Lenaers, Juan Fernando López Aguilar, Nuno Melo, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Birgit Sippel, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Tomas Tobé, Dragoş Tudorache, Tom Vandendriessche, Bettina Vollath, Jadwiga Wiśniewska, Elena Yoncheva, Javier Zarzalejos, Sophia in 't Veld, Michal Šimečka
Substitutes present for the final vote	Malin Björk, Delara Burkhardt, Klára Dobrev, Rasa Juknevičienė, Kris Peeters, Karlo Ressler

EN

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

56	+
PPE	Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Andrzej Halicki, Rasa Juknevičienė, Jeroen Lenaers, Nuno Melo, Kris Peeters, Emil Radev, Karlo Ressler, Ralf Seekatz, Tomas Tobé, Javier Zarzalejos
S&D	Pietro Bartolo, Delara Burkhardt, Caterina Chinnici, Klára Dobrev, Maria Grapini, Sylvie Guillaume, Evin Incir, Marina Kaljurand, Łukasz Kohut, Juan Fernando López Aguilar, Javier Moreno Sánchez, Birgit Sippel, Bettina Vollath, Elena Yoncheva
Renew	Malik Azmani, Anna Júlia Donáth, Fabienne Keller, Moritz Körner, Maite Pagazaurtundúa, Ramona Strugariu, Dragoş Tudorache, Sophia in 't Veld, Michal Šimečka
ID	Nicolas Bay, Nicolaus Fest, Jean-Paul Garraud, Peter Kofod, Annalisa Tardino, Tom Vandendriessche
Verts/ALE	Patrick Breyer, Saskia Bricmont, Damien Carême, Alice Kuhnke, Terry Reintke, Diana Riba i Giner, Tineke Strik
ECR	Jorge Buxadé Villalba, Patryk Jaki, Assita Kanko, Nicola Procaccini, Jadwiga Wiśniewska
NI	Laura Ferrara

4	-
PPE	Nadine Morano
GUE/NGL	Malin Björk, Clare Daly, Cornelia Ernst

0	0

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

EN