Executive Summary

Opinion on the implications of the exclusion from new binding European instruments on the use of AI in military, national security and transnational law enforcement contexts

by

Douwe Korff

Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

October 2022

European Center for
Not-for-Profit Law

Executive Summary[1]

It is increasingly recognised that the use of so-called "artificial intelligence" (**AI**), while promising benefits in many areas, can also pose serious threats to fundamental rights. To counter these threats and to protect those rights, binding rules on the use of "AI systems" are being proposed at both European Union (EU) and Council of Europe (CofE) level: in the EU, the Artificial Intelligence Act or AIA (an EU regulation) is already going through the legislative process, while in the Council of Europe, a so-called "zero draft" of a Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law[2] has been circulated.

EU context:

A recent judgment[3] of the EU Court of Justice (CJEU) on the compatibility of the EU Passenger Name Record (PNR) Directive with the EU Charter of Fundamental Rights (CFR) (Case C-817/19) is crucially important. Specifically, the Court made clear that **the use of opaque and unchallengeable AI systems is inherently incompatible with the EU Charter of Fundamental Rights.** In particular, the use of systems with such characteristics violates the very essence of the right to an effective remedy (*see Opinion* - *Conclusion 1*).

It follows from the PNR judgment of the CJEU that **the category of AI systems presenting "unacceptable" risks** as identified by the draft AI Act must be regarded as including the use of unexplainable, therefore unchallengeable, AI systems in any decision that significantly affects the rights of individuals (*see Opinion – Conclusion 4).*

It equally follows from the case-law of the CJEU (namely, *PNR* and *La Quadrature di Net*), that **even when EU Member States hold exclusive competence in some areas (such as national security), if the exercise of their competence affects another area that is within the EU competence and is covered by EU law** (e.g., data protection, internal market legislation), **the exercise of the Member State's exclusive competence may not impinge on the EU legal order or undermine the relevant EU legal rules**, such as the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED), the Europol Regulation or in future with

[1] This Executive Summary consists of an abbreviated and edited version of the Conclusions outlined across the text of the Opinion and listed altogether in the Annex. References are added to conclusions set out in the Opinion that address the relevant matters in more detail.

[2] The term "zero draft" indicates that it is not yet even a formal draft, but rather a first tentative attempt at a text.

[3] CJEU, Case C-817/19, 18 August 2022: https://curia.europa.eu/juris/document/document.jsf?text=&docid=264843&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1156470

the AI Act – and the CJEU is competent to assess compatibility with such EU laws and more generally with the CFR (*see Opinion - Conclusion 5*).

More specifically: irrespective of Article 4 of the Treaty of the EU (which excludes Member States' national security matters from the competence of the EU), **whenever an EU Member State, for national security purposes, imposes obligations on any entities that are, in their relevant activities, subject to any EU rules** (including, e.g., Europol, Frontex, EU missions and law enforcement agencies of EU Member States), **those obligations must be compatible with the Charter** – and the Court of Justice is competent to assess that compatibility (*See Opinion – Conclusion 5*). Therefore, any rules (including the AI Act) covering the links (e.g., exchanges of data) between private entities and EU entities (in particular Europol and Frontex) on the one hand, and EU Member States' national security agencies on the other hand, should be so drafted and applied as to prevent circumvention of EU law and, in the present case, of the AI Act (*See Opinion – Conclusion 6*).

More specifically, the European Data Protection Supervisor should urgently issue an opinion on the use of AI systems in processing of personal data subject to EU data protection rules in relation to which he is competent (Europol Regulation, Law Enforcement Directive, Regulation 2018/1725, etc.), in which he clarifies that the use of unexplainable and unchallengeable AI systems in any decision-making that significantly affects the fundamental rights of individuals is incompatible with the Charter and therefore also with each and every one of those instruments (*See Opinion – Conclusion 7*).

There is no justification for the exemption in the AI Act relating to AI systems developed or used for military purposes (or dual purposes) at all. They should be fully subject to the Act – and to the Charter as interpreted by the Court of Justice. The development and placing on the (internal) market of military (or dual-use) goods and services incorporating or using unexplainable and unchallengeable AI systems should consequently be prohibited. Further, the development and placing on the (internal) market of military (or dual-use) other AI systems should be subject to the same strict conditions as are provided for "high risk" systems in the AI Act, i.e., an *ex ante* conformity assessment, the establishment of a risk management and data and data governance system, the drawing up and having available for inspection of technical documentation and detailed records, post-market surveillance, etc. (*See Opinion – Conclusion 8)*.

Equally, all EU legal instruments and policies relating to the EU CFSP and the EU CSDP should be reviewed and revised to reflect and respect the prohibition on the use of unexplainable and unchallengeable AI systems in relation to decision-making that significantly affects the fundamental rights of individuals (especially any decisions on the use of force). (*See Opinion – Conclusion 9)*.

Council of Europe context:

Despite the provision of the Statute of the Council of Europe (Article 1(d)) excluding "matters of national defence" from its mandate, "military matters" and "national defence" (or "defense") issues are not excluded from the application of human- or digital rights-related Council of Europe treaties, and some explicitly apply to matters relating to such matters or to armed conflicts. (*See Conclusion 12*). Therefore, the proposed exemption from the AI Convention for "[*the] design, development and application of artificial intelligence systems used for purposes related to national defense*"[4], if accepted as necessary to comply with Article 1(d) of the Statute of the Council of Europe, would imply a fundamental retreat of Council of Europe-backed European treaty law – including the ECHR and ECtHR case-law – from military/defence activities in relation to which Council of Europe-issued treaties and the ECHR have until now fully applied. It is reprehensible and must be deleted. (*see Conclusion 12*).

If Article 13 of the European Convention on Human Rights (which guarantees the right to an effective remedy) is interpreted in the same way as Article 47 of the EU Charter by the CJEU, - as is to be expected – it follows that the use of unexplainable – hence unchallengeable – AI systems for decision-making also violates the Convention and indeed affects the very essence of that right. Therefore, the use of such AI systems must never be allowed under the proposed AI Convention, also not under the exception clause that is currently in the "zero draft" of that Convention (*See Conclusion 13).*

Practical implications under both the EU and the Council of Europe:

The only way to guard against erroneous or societally unacceptable outcomes of AI systems would be to have the relevant algorithms and data on their application and on the outcomes of their application continuously **rigorously tested and audited** by fully qualified, independent experts on the basis of **clear, peer-reviewed scientific standards** in order to limit, as far as possible: straight-forward errors, bias against certain groups (especially those defined by race, gender, religion, etc.), and excessive false positives and/or false negatives.

Moreover, in a democratic society the results of those tests and audits – and the underlying data and algorithms and methodologies – should be **open to external, independent scientific review**, not least also on behalf of any individuals affected by the programs. This information should not be kept from scrutiny on the bases of issues such as "commercial confidentiality" or "national security" (*See Conclusion 14*).

Douwe Korff,
Cambridge (UK), October 2022

[4] Language in the zero-draft of the AI Convention, restricted but viewed by the Author.

European Center for Not-for-Profit Law Stichting
5 Riviervismarkt, 2513 AM, The Hague, Netherlands
www.ecnl.org   twitter.com/enablingNGOlaw

European Center for
Not-for-Profit Law