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

> "The attempts to exclude from the new protections, in sweeping terms, anything to do with AI in national security, defence and transnational law enforcement contexts, including research into as well as the "design, development and application of" artificial intelligence systems used for those purposes, also by private companies, are pernicious: if successful, they would make the entire military-industrial-political complex a largely digital rights-free zone."

About the European Center for Not-for-Profit Law (ECNL): ECNL is an independent European non-governmental organisation, based in The Hague, Netherlands. It is the only regional organisation in Europe focused entirely on law and policy that affect civil society. ECNL's mission is to create legal and policy environments that enable individuals, movements and organisations to exercise and protect their civic freedoms and to put into action transformational ideas that address national and global challenges. It responds to both continuing challenges to public participation and the right of peaceful assembly and to new trends impacting on the non-profit sector, such as securitisation, counter-terrorism, and the use of artificial intelligence, also in relation to national security and defence. https://ecnl.org/

About the author: Douwe Korff is a Dutch comparative and international lawyer specialising in human and digital rights. He is emeritus professor of international law at London Metropolitan University and visiting professor at the universities of Zagreb and Rijeka in Croatia; an Associate of the Oxford Martin School of the University of Oxford, a Visiting Fellow at Yale University (Information Society Project), and a Fellow at the Centre for Internet and Human Rights of the European University of Viadrina, Berlin.

Douwe Korff has carried out many studies relating to digital rights, data protection and surveillance for the EU, the Council of Europe, the UN (ITU), the British Commonwealth, and the UK authorities. He works closely with civil society and digital rights groups including European Digital Rights (EDRi).

Contents

Copyright © 2022 by the European Center for Not-for-Profit Law Stichting (ECNL). All rights reserved.

Abbreviations & Glossary

AI	Artificial Intelligence
AIA/AI Act	(pending) EU Artificial Intelligence Act
AI Convention	(proposed) CoE Convention on Artificial Intelligence, Human Rights, Democracy and the Rule Of Law
AI system	Software that is developed with one or more of the techniques and approaches listed in Annex I to the AI Act and that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with. (Article 3(1) AIA)* *See footnote 26 of the opinion for further detail.
AFJS	EU Area of Freedom, Justice and Security
CETS	Council of Europe Treaty Series
CFR/Charter	EU Charter of Fundamental Rights
CoE	Council of Europe
CFSP	EU Common Foreign and Security Policy
CSDP	EU Common Security and Defence Policy (part of the CFSP)
CJEU	Court of Justice of the European Union
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDAP	EU European Defence Action Plan
EU	European Union
Europol	EU Agency for Law Enforcement Cooperation
Europol Regulation	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), as last updated by Regulation (EU) 2022/991 of 8 June 2022
Frontex	EU Border and Coast Guard Agency
GDPR	EU General Data Protection Regulation* *Full title: 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

ICCPR	UN International Covenant on Civil and Political Rights
ICESCR	UN International Covenant on Economic, Social and Cultural Rights
IHL	International Humanitarian Law
LED	EU Law Enforcement Directive* *Full title: 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
MI5	UK domestic intelligence agency
MI6	UK foreign intelligence agency
ML	Machine learning* *See the definition of ML/AI system.
ML/AI system	A self-learning (or "machine learning" [ML]) artificial intelligence system that is capable of modifying without human intervention or review the assessment processes for which the system is used and, in particular, the assessment criteria on which the result of the application of those processes are based as well as the weighting of those criteria.* *(Cf. the CJEU PNR judgment, discussed in section 2.2, para. 194, quoted in that section. For a discussion, see also section 2.3.
NATO	North Atlantic Treaty Organisation
Non-ML-based AI system	An AI system that does not use machine- (self)learning.* *See the definition of ML/AI system.
NSA	US national security agency
OECD	Organisation for Economic Cooperation and Development
PIU	Passenger Information Unit (established under the PNR Directive)
PNR	Passenger Name Records
PNR Directive	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

RBI	Remote biometric identification
SMEs	Small and medium-sized companies
TEU	EU Treaty on European Union
TFEU	EU Treaty on the Functioning of the European Union
UDHR	United Nations Universal Declaration of Human Rights
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organisation

1. Introduction

It is increasingly recognised that the use of so-called "artificial intelligence", while promising benefits in many areas, can also pose serious threats to fundamental rights.[1] To meet these threats and to protect those rights, binding rules on the use of "AI systems" are therefore proposed at both European Union (EU) and Council of Europe (CoE) level. In the EU, the **Artificial Intelligence Act** or **AIA** (an EU regulation) is already going through the legislative process,[2] 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** (hereafter: "the proposed AI Convention") has been circulated. The term "zero draft" indicates that it is not yet even a formal draft, but rather a first tentative attempt at a text.[3] The text is still confidential, but some aspects of it have been leaked, as discussed at 3.2 and 4.2, below.

[1] In this opinion, I am using the terms "fundamental rights" and "human rights" interchangeably. The EU tends to use the former (as in the title of its main rights instrument, the EU Charter of Fundamental Rights) while the Council of Europe tends to use the term "human rights" (as in the title of its seminal rights instrument, the European Convention on Human Rights and Fundamental Freedoms). The UN also uses "human rights" (as in the "mother" instrument of all modern rights treaties, the Universal Declaration of Human Rights).

[2] European Commission, Proposal for an Artificial Intelligence Act (AIA (COM(2021) 206 final), Brussels, 21 April 2021, which includes the text as proposed by the European Commission as well as the explanatory memorandum on the proposed text: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206

There have been several revised Council texts, the latest drafted by the Czech Presidency in July 2022, and several committees of the European Parliament have adopted positions on the text. The so-called "trilogues" in which the final text will be agreed will probably not start until next year. But as noted in this opinion, the overall approach is broadly agreed (in spite of criticism).

[3] The proposed AI convention fits in with a wide range of activities undertaken by the Council of Europe in relation to AI, see the long list at: https://www.coe.int/en/web/artificial-intelligence/work-in-progress#02EN

The United Nations High-level Committee on Programmes (HLCP) produced a discussion paper on AI that in 2019 led to a UN "system-wide strategic approach and road map for supporting capacity development on artificial intelligence":

https://unsceb.org/united-nations-system-wide-strategic-approach-and-road-map-supporting-capacity-development

In the same year, UNESCO established an Ad Hoc Expert Group with the aim to elaborate a non-binding Recommendation on the Ethics of AI. A first draft version of this recommendation was published in May 2020 and the final text was adopted in November 2021. https://unesdoc.unesco.org/ark:/48223/pf0000381137 (text of the recommendation)

Background information is available here: https://en.unesco.org/artificial-intelligence/ethics#recommendation

On 12 August 2022, the UN Human Rights Council Advisory Committee (the HRC's "Think Tank") announced it had decided to submit for consideration and for approval by the Human Rights Council two updated research proposals including one on *"Human rights implications of the use of new and emerging digital technologies developed in the military domain used for law enforcement and security purposes"*. See: https://www.ohchr.org/en/press-releases/2022/08/hrc-advisory-committee-concludes-its-28th-session-advances-work-new

But there are no moves at UN level towards a binding instrument (a treaty).

Note also the OECD Council Recommendation on Artificial Intelligence of 21 May 2019: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

However, **the European legislators are seeking to exclude from the application of the proposed instruments the use of AI in the contexts in which they arguably pose the greatest threats to fundamental rights: national security, defence and transnational law enforcement**. To some extent, in the EU, this is the result of the exclusion of national security from the scope of Union law and from the competence of the EU legislator, and of the need for different instruments for different areas in which the EU is competent. However, the proposed exemptions to the AI Act in fact – and indefensibly – go well beyond what is required. In relation to the proposed Council of Europe instrument, it is reportedly suggested that there is a general limitation on the competence of the Council of Europe to create treaties that may affect human rights in relation to "matters relating to national defence". As I will explain in this opinion, this poses a fundamental threat to the much-lauded system of human rights protection by the Council generally.

In section 2, I discuss the risks to fundamental rights posed by AI systems generally, with reference to acknowledgments of those threats in the proposed new instruments. I will also discuss a recent judgment of the Court of Justice of the European Union (CJEU) that linked those threats to specific fundamental rights, and to an earlier opinion I wrote on the issues raised in that case. I note that while the judgment can and rightly has been criticised, it also sets important standards of general application in relation to the use of AI.

In section 3, I note the general approach taken to counter these threats in the proposed new European instruments. In particular, I note that both the Act and, reportedly, the "zero draft" AI Convention identify (or will provide a methodology for identifying) AI systems that pose "unacceptable" risks – and that therefore should be banned and never developed or used – and "high risk"/"significant risk" systems that should be tightly regulated. In fact, as I will show, in the light of the above-mentioned CJEU judgment, that the restrictions, in at least the AI Act, will have to be further tightened.

In Section 4, I discuss the proposed exemptions and exceptions provided in the EU AI Act and reportedly proposed for the CoE AI Convention, and in particular the (dubious) rationales given for these exemptions. In relation to each of the exemptions and exceptions, I spell out the implications in the light of the standards adduced in section 3.

For practical reasons, this opinion has been kept brief. I have tried wherever possible, to provide footnote references to more elaborate exposés of the relevant issues (some of which I have written). I hope this opinion will assist in

While influential, with some 46 countries signing it as "adherents", this recommendation, too, is non-binding.

There have also been developments in relation to the use of AI (and similar technologies) for military and national security purposes within NATO, to which I will come in sections 3 and 4.

informing policy makers and legislators involved in the drafting of the new instruments – and that they will avoid creating the above-mentioned danger: a digital rights-free zone for national security and defence activities by states and private companies.

2. The risks to fundamental rights posed by AI systems

2.1 The risks in general terms

The Explanatory Memorandum to the AI Act rightly stresses that while AI:[4]

> can bring a wide array of economic and societal benefits across the entire spectrum of industries and social activities… **the same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences for individuals or the society**.

The proposed EU rules must therefore:[5]

> [be] **based on EU values and fundamental rights** and aims[ ] to give people and other users the confidence to embrace AI-based solutions, while encouraging businesses to develop them. AI should be a tool for people and be a force for good in society with the ultimate aim of increasing human well-being. **Rules for AI available in the Union market or otherwise affecting people in the Union should therefore be** human centric, so that people can trust that the technology is used in a way that is safe and **compliant with the law, including the respect of fundamental rights**.

Potential harms include the use of AI for mass surveillance, misinformation or electoral interference, and effects such as discrimination, digital exclusion and a general weakening of human agency.

Edwards notes more specifically that:[6]

> [t]wo categories of requirements seem particularly germane to the principal worries in the literature around AI in our society making decisions that affect humans, namely: **algorithmic error, bias and discrimination**; **automated decision-making as contrary to human dignity**; and **opacity/lack of explanations**.

I have elaborated on some of these potential risks and dangers in an earlier opinion on the use of passenger name record data (PNR data) for profiling and analyses in order to "identify" (read: single out), by means of sophisticated,

[4] Explanatory Memorandum to the proposed AI Act (footnote 2, above) section 1.1, *Reasons for and objectives of the proposal*, first paragraph.

[5] *Idem*, second paragraph, emphases added.

[6] Lilian Edwards, The EU AI Act: a summary of its significance and scope, Ada Lovelace Institute, April 2022, p. 16, emphases added, available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf

Presumably, the final worry, about lack of transparency and explanations, is seen by her as part of the second category: automated decision-making as contrary to human dignity. Otherwise, there would be three categories.

self-learning algorithms, individuals who "may be" involved in terrorism or serious crime.[7] There, I discuss, in particular, the risks stemming from the so-called "**base-rate fallacy**" (the mathematically inevitability that algorithmic/AI-based searches for rare phenomena or categories of persons – such as terrorists – in a wide population will result in excessive numbers of "false positives" and "false negatives", or both, and are therefore fundamentally unsuited for such uses); **built-in biases** in algorithmic/AI-based systems, leading to discriminatory outputs and outcomes; and the **opaqueness and unchallengeability of algorithm-based decisions** (even if subject to human oversight).

Here, it will suffice to simply note two matters. First, these risks are not disputed by the proponents of the new instruments; on the contrary, as shown above with reference to the AI Act, they explicitly acknowledge them and, as noted in the next section, make extensive and elaborate proposals on how those risks should be countered or minimised. Indeed, they make clear that AI systems that pose "unacceptable risks" should be banned.

Second, these risks are especially serious in relation to activities of states relating to (or purported to relate to and claimed to be necessary for) the protection of their national security, for national (or collective) defence, and for law enforcement (and international cooperation in law enforcement). This makes the exclusions of these activities from the proposed international instruments, all the more problematic, as discussed in section 3.

2.2 The risks spelled out further and linked to the Charter in the EU Court of Justice PNR judgment

On 21 June 2022, the Court of Justice of the European Union (CJEU or "the Court") issued a judgment on the compatibility of the EU PNR Directive[8] with the EU Charter of Fundamental Rights.[9] The PNR Directive mandates the large-scale collection and screening of airline passenger data by EU Member States against

[7] Douwe Korff, Opinion on Core Issues in the PNR CJEU Case, prepared at the request of the Fundamental Rights European Experts Group (FREE Group), November 2021, available at:

https://www.ianbrown.tech/wp-content/uploads/2021/12/KORFF-FREE-Paper-on-Core-Issues-in-the-PNR-Case.pdf (full opinion, 147 pages) (hereafter: "my earlier opinion)

https://www.ianbrown.tech/wp-content/uploads/2021/12/KORFF-PNR-Case-Executive-Summary.pdf (executive summary, 27 pages)

See in particular section 4.9(f), sub-section (fe) of the full opinion, on *The limitations of and flaws in the technologies*.

[8] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4 May 2016, p. 132–149, available at:

https://eur-lex.europa.eu/eli/dir/2016/681/oj

[9] CJEU judgment of 21 June 2022 in case C-817/19 on the *PNR Directive*, ECLI:EU:C:2022:491, available at: https://curia.europa.eu/juris/documents.jsf?num=C-817/19 (hereafter: "the PNR judgment")

"relevant" databases and "pre-determined criteria", with the aim of "identifying" (read: singling out), through analysis, individuals who "may be" terrorists or serious criminals. "Initial hits" (matches) are produced by automated means, and those are then reviewed manually and converted to an actual "hit" if the human reviewer confirms the computer-generated result. As explained in my earlier opinion, the system was specifically tailored to allow the use of sophisticated algorithms and AI in this endeavour.[10] It has also become clear that the system in practice results in a great many "false positives", i.e., automated results that suggest that the person concerned "may be" a terrorist or serious criminal, but where the "initial hit" is not subsequently confirmed.[11]

In crucial passages that will have broad implications, the Court **prohibited** the use of certain self- or machine-learning (i.e., self-modifying) AI systems ("**ML/AI systems**") in the taking of decisions under the PNR Directive.

The Court imposed this prohibition, partly because the term "pre-determined criteria" excluded the use of criteria that modified themselves in deployment, but also because ML/AI systems[12] can be untransparent and unexplainable – and thus unchallengeable, meaning they are then incompatible with the Charter:

> … [T]he processing of PNR data against pre-determined criteria is intended, in essence, to identify persons who may be involved in a terrorist offence or serious crime. …
>
> As noted by the Advocate General in point 228 of his Opinion,[13] **that requirement [of the criteria to be used in PNR screening having to**

[10] See my earlier opinion (footnote 8, above), section 4.9(f), Matching of data in the PNRs against more complex "pre-determined criteria" or profiles.

[11] See the judgment at paras. 106 and 206, but note that neither the Court nor the Advocate-General addressed the far from easy question of what should be, and what should not be, regarded as a "true" or "false positive". On that point, see my earlier opinion (footnote 8, above), section 5.2(a), at (ab), *When a (confirmed) "hit can be said to constitute a "positive" result (and when not)*.

[12] As noted in footnote 225 to the Advocate-General's opinion in the case (referenced in the next footnote), according to Section 1.1(g) of the Appendix to the 2021 Council of Europe (updated) Profiling Recommendation, '*machine learning processing*' refers to '*processing using particular methods of AI based on statistical approaches to give computers the ability to "learn" from data, that is, to improve their performance in solving tasks without being explicitly programmed for each of them*'. Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted by the Committee of Ministers on 3 November 2021, available at:

https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a46147

In this light and in the light of the paragraphs in the judgment quoted, an ML/AI system can be defined as "A self-learning (or 'machine learning' [ML]) artificial intelligence system that is capable of modifying without human intervention or review the assessment processes for which the system is used and, in particular, the assessment criteria on which the result of the application of those processes are based as well as the weighting of those criteria." In this opinion, I will hereafter use the term "ML/AI system" as shorthand for such systems.

[13] Opinion of Advocate-General Pitruzzella, delivered on 27 January 2022, available here:

> **be 'pre-determined'] precludes the use of artificial intelligence technology in self-learning systems ('machine learning'), capable of modifying without human intervention or review the assessment process and, in particular, the assessment criteria on which the result of the application of that process is based as well as the weighting of those criteria.**
>
> It is important to add that **use of such [machine learning] technology would be liable to render redundant the individual review of positive matches and monitoring of lawfulness required by the provisions of the PNR Directive**. As observed, in essence, by the Advocate General in point 228 of his Opinion[14], **given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match. In those circumstances, use of such technology may deprive the data subjects also of their right to an effective judicial remedy enshrined in Article 47 of the Charter**, for which the PNR Directive, according to recital 28 thereof, seeks to ensure a high level of protection, in particular in order to challenge the non-discriminatory nature of the results obtained.
>
> (CJEU *PNR* judgment, paras. 193 – 195, emphases added)

As the words "might" and "may" in the above quote indicate, strictly speaking this paragraph does not lay down a permanent prohibition on the use of self-learning algorithms for surveillance purposes, should they become easy to interpret/review by a human and therefore explainable and challengeable.

https://curia.europa.eu/juris/document/document.jsf;jsessionid=B4A49BBF05F595B9B70F39DE31BEA945?text=&docid=252841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1429667

At 228, the A-G writes:

"[T]*he requirement that the criteria on the basis of which that analysis is carried out must be 'pre-determined' means that they must not be modifiable without human intervention and, therefore, precludes the use of 'machine learning' artificial intelligence technology, which, whilst it may be more precise, is difficult to interpret, even for the operators who carried out the automated processing*."

The A-G added*: "On the effects of the opacity of algorithmic systems on the feasibility of human control to prevent the detrimental effects of those systems and their negative human rights impacts, see Recommendation CM/Rec(2020)1 of the Committee of Ministers of the Council of Europe to member States on the human rights impacts of algorithmic systems."* (footnote 226 to the A-G opinion)

[14] To quote again from point 228 of the Opinion:
"[I]f it is to be effective, the safeguard set out in Article 6(5) and (6) of the PNR Directive, according to which any positive match resulting from the automated processing of PNR data under Article 6(2)(a) must be individually reviewed by non-automated means, requires – in relation to the analysis under Article 6(3)(b) of the PNR Directive – that it must be possible to understand why the program arrived at that match, which cannot be guaranteed when, for example, self-learning systems are used. The same is true as regards monitoring the lawfulness of the analysis – including in relation to the fact that the results obtained must be non-discriminatory, which is the responsibility of the data protection officer and the national supervisory authority, under Article 6(7) and Article 15(3)(b) of the PNR Directive respectively. Transparency in the functioning of the algorithms used is also a necessary precondition for the data subjects to be able to exercise their rights to complain and their right to an effective judicial remedy."

Rather, as Thönnes puts it,[15] "*[p]aragraphs 194-195 contain prohibitions on self-learning algorithms which (1) are capable of modifying their assessment criteria without any human intervention of review (this notably open logical distinction does not matter much at the moment), and/or (2) are too opaque to allow for effective judicial remedy against their recommendations.*" In that regard, he notes that:

> This may cover most of today's available AI software. It is not inconceivable, however, that AI software could, in the future, provide satisfactory reasons for their recommendations (see for example *Wischmeyer*, Artificial Intelligence and Transparency: Opening the Black Box).[16] Also, there are methods of supervised and reinforced learning where autonomous learning is intertwined with human interventions (see *Binns/Veale*, IDPL 11 (4), 319-332).[17] Therefore, the prohibition on self-learning algorithms is a positive step forward – but without further legal elaboration security agencies could circumvent this prohibition if they just use the right AI systems.

For the sake of argument, I will allow for the possibility that transparent and explainable ML/AI systems, the outputs of which can be effectively challenged, may be developed in future. When, in the remainder of this opinion, I refer to to-be-banned AI systems, this refers to *unexplainable and unchallengeable AI systems in general* (as often expressly reaffirmed in the text). If there are, or at some stage will be, ML/AI systems (or any other type of AI systems developed in the future) that are explainable and therefore challengeable, any developer claiming to have developed a system with these characteristics would have to provide serious, openly peer-reviewed evidence to that effect. Equally, any user of such a purportedly explainable and challengeable system would have to also collect the relevant data and make them available for independent expert review (as noted in section 4.3).

[15] Christian Thönnes, A Directive altered beyond recognition: On the Court of Justice of the European Union's PNR decision (C-817/19), *Verfassungsblog*, 23 June 2022, available at:

https://verfassungsblog.de/pnr-recognition/

See also Marc Rotenberg, CJEU PNR Decision Unplugs the "Black Box", *European Data Protection Law Review*, Volume 7 (2022), Issue 3 (due September 2022).

[16] Thomas Wischmeyer & Timo Rademacher (eds.), Regulating Artificial Intelligence, Springer, 2020, available at: https://link.springer.com/book/10.1007/978-3-030-32361-5

[17] Reuben Binns & Michael Veale, Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR, in: *International Data Privacy Law*, Volume 11, Issue 4, November 2021, Pages 319–332, available at: https://doi.org/10.1093/idpl/ipab020

Conclusion 1:

It is clear from the PNR judgment of the CJEU that the use of opaque, i.e., unexplainable and hence unchallengeable AI systems is inherently incompatible with the Charter of Fundamental Rights of the EU. In particular, the use of systems with such characteristics violates the very essence of the right to an effective remedy - and current machine-learning based AI systems (ML/AI systems) typically have those characteristics. This has broad and significant implications generally (not just in relation to PNR data screening).

Even in relation to not-ML/AI-based decisions, there must still be **strict rules** to ensure that they are explainable and challengeable and they do not result in discriminatory outputs and outcomes or excessive numbers of false positives. Specifically, in these regards, the Court stresses in its judgment that Member States must ensure that the entity involved in the assessments under the PNR Directive (the so-called Passenger Information Units or PIUs) "*establishes, in a clear and precise manner, **objective review criteria** enabling its agents to"* identify false positives (individuals being wrongly identified by the AI system as possible terrorists or serious criminals) and to verify "*the non-discriminatory nature of automated processing operations under [the PNR Directive]*" (para. 206, emphasis added; cf. also para. 205 of the judgment and para. 228 of the A-G opinion).[18]

Conclusion 2:

The use of all AI systems must still be subject to strict conditions based on their level of risk and, must make it possible to monitor and review the outputs and outcomes[19] of those systems, especially in order to ensure that they do not generate discriminatory outputs or result in discriminatory outcomes, and to assess the numbers and percentages of false positives and false negatives.

[18] On these latter points, see again my earlier opinion (footnote 8, above), section 4.9(f)*, Matching of data in the PNRs against more complex "pre-determined criteria" or profiles* and more specifically sub-section (fe) of the full opinion, on *The limitations of and flaws in the technologies*. There, I make the point that because of what is known as the "base-rate fallacy", algorithmic analyses (even not-ML/AI-based ones) are *inherently unsuited* – and can therefore never be "necessary" or "proportionate" to searches for very small classes (e.g., terrorists) in a very large population (e.g., all 500 million people who travel to or from the EU each year). I return to this in section 4.

[19] On the conceptual difference between outputs and outcomes, see my earlier opinion, section 4.9(f), sub-section (fe), at Ii, *built-in biases*, and more specifically the quote from a University of Delft/EDRi report on pp. 89 – 90. Basically, outputs are the results generated by IT systems, whereas outcomes are the consequences of the application of those outputs (often by humans [over-]relying on the outputs).

Crucially, the Court linked its prohibition of the use of unexplainable and unchallengeable ML/AI systems in the context of the PNR Directive and the strict conditions imposed on AI systems directly to major fundamental rights protected by the EU Charter of Fundamental Rights: the rights to privacy and data protection (Article 7 and 8 CFR) and to freedom from discrimination (Article 21) (judgment, para. 213) and the right to an effective remedy (Article 47 CFR) (judgment, para. 195, quoted above).

Hopefully, in due course, the European Court of Human Rights will take the same approach and hold that the use of unexplainable and unchallengeable AI systems is also fundamentally incompatible with the European Convention on Human Rights. Given that such systems affect exactly the same fundamental rights as were referenced by the EU Court of Justice: privacy and data protection, non-discrimination and effective remedy – enshrined in Articles 8, 13 and 14 of the Convention, respectively – and that the two courts tend to interpret the two instruments of which they are the respective guardians in broadly the same way, this is in my opinion likely to happen (although, as explained in an earlier report by Brown and me, the Strasbourg Court has arguably been somewhat less strict in respect of national security surveillance issues than the Luxembourg Court has been).[20]

That is important particularly in relation to state activities relating to national security: as also explained in that report (and further discussed in section 4, below), there is a "hole" in the EU legal system in relation to national security that is partly "patched" by the fact that all EU Member States are party to the ECHR (with being a party to the Convention indeed being a condition of membership of the EU).[21]

2.3 General implications of the PNR judgment for EU law

It is crucial to draw once again the attention to the following conclusion of the PNR judgment [emphasis added]:

> […] **given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match**. **In those circumstances, use of such technology may deprive the data**

[20] Cf. the discussion of the ECtHR Grand Chamber *Big Brother Watch* judgment in Ian Brown and Douwe Korff, Exchanges of personal data after the Schrems II judgment, study carried out at the request of the European Parliament's Civil Liberties (LIBE) Committee into the future of EU – US flows of personal data, July 2021, section 2.3.13, *Requirements relating to access to personal data by state authorities*, under the sub-heading *"ECtHR and national constitutional requirements relating to direct access to personal data by EU Member States' intelligence agencies"*, p. 47ff. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

[21] Idem, section 2.2.2, The national security exemption in the EU Treaties.

> **subjects also of their right to an effective judicial remedy enshrined in Article 47 of the Charter**, for which the PNR Directive, according to recital 28 thereof, seeks to ensure a high level of protection, in particular in order to challenge the non-discriminatory nature of the results obtained.

It follows from the above that **the use of unexplainable and unchallengeable AI systems – must be prohibited in all areas of EU competence** including the Internal Market, Police Cooperation and Europol and other matters within the Area of Freedom, Security and Justice (AFSJ), the Common Foreign and Security Policy (CFSP) including the Common Security and Defence Policy (CSDP), etc – since it breaches the subjects' right to an effective judicial remedy as protected by Article 47 of the Charter of Fundamental Rights of the EU.

It also follows that **strict regulations must be imposed on the use of all AI systems (in all areas of EU competence)** including all the areas mentioned above.

This is to some extent recognised in the proposal for the AI Act:[22]

> The horizontal nature of the proposal requires full consistency with existing Union legislation applicable to sectors where high-risk AI systems are already used or likely to be used in the near future.

The proposal then claims that such consistency is already achieved because it leaves other regulation intact:[23]

> Consistency is also ensured with the EU Charter of Fundamental Rights and the existing secondary Union legislation on data protection, consumer protection, non-discrimination and gender equality. The proposal is without prejudice and complements the General Data Protection Regulation (Regulation (EU) 2016/679) and the Law Enforcement Directive (Directive (EU) 2016/680) with a set of harmonised rules applicable to the design, development and use of certain high-risk AI systems and restrictions on certain uses of remote biometric identification systems. Furthermore, the proposal complements existing Union law on non-discrimination with specific requirements that aim to minimise the risk of algorithmic discrimination, in particular in relation to the design and the quality of data sets used for the development of AI systems complemented with obligations for testing, risk management, documentation and human oversight throughout the AI systems' lifecycle. The proposal is without prejudice to the application of Union competition law.

[22] Poposal (footnote 2, above), section 1.2, Consistency with existing policy provisions in the policy area.

[23] Idem.

More generally, as I will discuss further,, the consistent, horizontal application of the rules on AI in all areas of EU law that the Commission claims it espouses is actually fundamentally undermined by two exemptions I note there: for research, development and use by **Europol**, and for AI systems developed or used for **military purposes**.

More generally, as I will discuss further,, the consistent, horizontal application of the rules on AI in all areas of EU law that the Commission claims it espouses is actually fundamentally undermined by two exemptions I note there: for research, development and use by **Europol**, and for AI systems developed or used for **military purposes**.

Conclusion 3:

The application of the in-principle prohibition of fully automated decision-making in the General Data Protection Regulation (GDPR) and in the regulation laying down the data protection obligations for the EU institutions, bodies and agencies (Regulation (EU) 2018/1725) – as well as the restrictions on the use of such systems in the Law Enforcement Directive (LED) and the Europol Regulation[24] (and any other rules in the Area of Freedom, Security and Justice) – should be aligned with the AI Act and the PNR judgment.

The application of the in-principle prohibition of fully automated decision-making in the General Data Protection Regulation (GDPR) and in the regulation laying down the data protection obligations for the EU institutions, bodies and agencies (Regulation (EU) 2018/1725) – as well as the restrictions on the use of such systems in the Law Enforcement Directive (LED) and the Europol Regulation[25] (and any other rules in the Area of Freedom, Security and Justice) – should be aligned with the AI Act and the PNR judgment.

The European Data Protection Board and the European Data Protection Supervisor should issue opinions (or preferably a joint opinion) on the use of AI systems in processing of personal data subject to these instruments, in which they clarify 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 thus never allowed under either the GDPR or Regulation 2018/1725 or the LED or the Europol Regulation (or any other rules in the Area of Freedom, Security and Justice).

[24] See footnote 44, below.

[25] See footnote 44, below.

Pending such an opinion, companies and public bodies should already refrain from using unexplainable and unchallengeable AI systems in any processing of personal data that is subject to the GDPR or Regulation 2018/1725 or the LED, and they should only use (and be allowed to use) AI systems if they comply with those strict conditions. Otherwise, they will be in breach of Article 22 GDPR, Article 24 of Regulation 2018/1725 or Article 11 LED (whichever is the applicable instrument).[26] The same should apply mutatis mutandis to Europol, Frontex, and any other EU agency operating in the Area of Freedom, Security and Justice.

[26] *Idem*.

3. The general approach taken in the new AI instruments

Both the AI Act and the AI Convention are based on classifications of "AI systems"[27] according to the risk they, by their very nature, are supposed to pose, and on that basis lay down prohibitions on **"unacceptable" systems** and strict conditions on the use of **"high risk" systems**.

3.1 The approach under the AI Act

The AI Act[28]is based on a four-tiered risk framework.[29] Each tier aims to set proportionate requirements and obligations for providers and users of AI systems, recognising the range of potential risks to health, safety, and fundamental rights by different types of AI systems in various contexts. The categories and the corresponding regulatory approaches are as follows:[30]

[27] The AI Act as proposed by the Commission does not define "artificial intelligence", but rather only "artificial intelligence system". The latter is defined as *"software that is developed with one or more of the techniques and approaches listed in Annex I and [that] can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."* (Article 3(1), emphases added)

The artificial intelligence techniques and approaches referred to in this article are set out in Annex I as follows:

(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods.

Cf. also the definition of "AI system" in section I of the OECD Recommendation (footnote 3, above).

[28] For a good overview of the AI Act, see: Lilian Edwards, The EU AI Act: a summary of its significance and scope (footnote 6, above). This accompanies a more critical analysis by the same author:

Lilian Edwards, Regulating AI in Europe: four problems and four solutions, Ada Lovelace Institute, March 2022, *Introduction*, p. 1, emphasis added, available at:

https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf

[29] This approach has been criticised as "dysfunctional": "This approach of ex ante designating AI systems to different risk categories does not consider that the level of risk also depends on the context in which a system is deployed and cannot be fully determined in advance." European Digital Rights (EDRi), An EU Artificial Intelligence Act for Fundamental Rights – A Civil Society Statement, 30 November 2021, section 1, A cohesive, flexible and future-proof approach to 'risk' of AI systems, available at:

https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf

See also section 2, Prohibitions on all AI systems posing an unacceptable risk to fundamental rights.

Further details on this point are set out in Edwards, Regulating AI in Europe (footnote 25, above), pp. 5 – 8, with reference in particular to "general purpose" AI systems. However, this general approach is unlikely to be changed in the process of adopting the AI Act (or indeed, the AI Convention).

Risk category:	Regulatory approach:	AI systems covered:

Unacceptable risk
(Title II, Article 5)*****
***NB: still under discussion**
	Prohibited	Using subliminal techniques;
		exploiting vulnerabilities;
		social scoring; real-time remote biometric identification (RBI) in public spaces (with exceptions).[31]

High risk (Title III, Article 6 & Annex III)***** ***NB: still under discussion**	*Conformity assessment*	System is a safety component; biometric identification and categorisation of persons; access to education; recruitment & worker management; access to essential public and private services; credit scoring; emergency responses; law enforcement (various); migration, asylum and border control (various); administration of justice.

Limited risk
(Title IV, Article 52)
	Transparency	Emotion recognition;
		biometric classification;
		chat bots; creation of deep fakes;

Minimal risk (Article 69)	*Code of conduct "encouraged"*	E.g.: spam filters; video games

For the present purpose, the most important categories are those of AI systems that pose "**unacceptable risks**", i.e., "*all those AI systems whose use is considered unacceptable as contravening Union values, for instance by violating fundamental rights*"[32] and "**high risks**", in particular to "*the health and safety or fundamental*

[30] This overview draws in part on a useful simple overview provided by the Centre for Data Ethics and Innovation of the UK Department for Digital, Culture, Media & Sport (DCMS), with reference to CDEI's own work on AI assurance, see:

https://cdei.blog.gov.uk/2021/05/11/the-european-commissions-artificial-intelligence-act-highlights-the-need-for-an-effective-ai-assurance-ecosystem/

See also Edwards, The EU AI Act (footnote 6, above), pp. 9 – 15.

[31] Note that online spaces are not treated as publicly accessible spaces: Recital 9. As noted and discussed in section 3.2, below, the exceptions relate in particular to the use of RBI systems in public spaces for law enforcement purposes.

[32] Commission proposal (footnote 2, above), section 5.2.2.

rights of natural persons".[33] Systems posing **unacceptable risks** must be prohibited, while systems posing **high risks** are subject to strict regulation. This includes an *ex ante* conformity assessment, the establishment of a risk management and data governance system, the drawing up and having available for inspection of technical documentation and detailed records, post-market surveillance, etc. – all aimed at ensuring that "*adequate mitigation and control measures*" are put in place and deployed "*by design and default*" (to use GDPR terminology). (I will discuss these measures further in section 4.3, below.)

3.2 The approach under the AI Convention

Reportedly, the "zero proposal" for an AI Convention adopts effectively the same approach as has been chosen by the EU, with an appendix to the convention to set out a (model) methodology for risk and impact assessment of artificial intelligence systems. State parties must then, using this methodology (or rather, their own national methodology based on the model), identify AI systems that present "unacceptable" levels of risk or that present "significant levels" of such risks. No details are as yet available, or reported on, as to the details of this methodology.

In relation to systems that pose an "**unacceptable risk**", it is reported that the Convention will require state parties to impose a moratorium on their use; and in relation to systems that pose a "**significant risk**", that they must impose strict conditions to prevent harm.

[33] *Idem*, section 5.2.3.

3.3 Conclusion

Conclusion 4:

Whatever one may think of the approach adopted for both the AI Act and the proposed AI Convention (and it can be criticised),[34] the drafters of the instruments – and the legislators if the proposals are adopted – clearly feel that some AI systems by their very nature, by the predictable negative effects they will have, are "unacceptable" or pose "high risks" to the fundamental rights and freedoms of individuals – and must therefore be banned (or at least suspended) or made subject to very strict regulatory and oversight requirements.

Moreover, it follows from the PNR judgment, discussed above, that the category of "unacceptable" AI systems must be regarded as including the use of unexplainable and unchallengeable, self-modifying AI systems in any decision that significantly affects individuals.

The proposed (reported) exceptions and exemptions to the instruments, discussed in the next section, must be examined in this light.

[34] See footnote 27, above.

4. Exemptions and exceptions

Both the AI Act and (reportedly) the proposed AI Convention are subject to **exemptions**: areas to which the instruments will not apply at all. This is distinct from the **exception clauses** that they also contain, under which some of the requirements of the relevant instruments can be departed from, under certain conditions. Below, I look at these and at the justifications given for them, and discuss the implications, with reference to applicable universal and European standards and to the PNR judgment.

4.1 Exemption and exception clauses in the AI Act

Exemption clauses:

The AI Act, if adopted as proposed by the Council, will not apply at all in four important and highly human rights-sensitive areas, two of them explicitly excluded, one (Europol) because it is subject to separate regulation, and one (the first one mentioned below) excluded because of a general limitation on EU competence. They are:

1. Activities of EU Member States relating to their national security;
2. Activities of EU agencies and EU Member States in the Area of Freedom, Security and Justice (ADSJ);
3. AI systems developed or used for military purposes; and
4. AI systems used by third countries or international organisations.

Below, under each of these headings, I first set out the relevant exemption and then discuss the implications.

4.1.1 Activities of EU Member States relating to their national security

The EU Treaties – the founding documents of the Union – and in particular the Treaty on European Union (TEU) clarify the competences of the Union, and the limits of those competences. In particular, Article 4(1) TEU stipulates:

> competences not conferred upon the Union in the Treaties remain with the Member States.

Article 4(2) adds more specifically:

> The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. **In**

> **particular, national security remains the sole responsibility of each Member State**. (emphasis added)

In simple terms: the EU, as a legislator, has no competence to issue legal rules that as such apply to national security activities of the EU Member States. Indeed, not even the EU Charter of Fundamental Rights can be invoked in relation to such activities. That is significant because, as described in more detail elsewhere, the EU Member States are increasingly using sophisticated, AI-based technologies, in particular surveillance technologies, in this area.[35]

Analysis and conclusion(s)

The exclusion of EU competence in relation to Member States' national security does not mean that there are no links between the EU – and the EU legal order – and such agencies. On the contrary, as noted by Brown and me as long ago as 2014, Member States' national security agencies are working increasingly closely with their own law enforcement, border control and military agencies[36] – and with the EU entities and missions that are involved in such matters. To mention just two specific issues I noted in the context of the PNR Directive: (i) the "competent authorities" to which PNR data may be sent include not only law enforcement agencies *stricto sensu*, but also, in many Member States, the states' intelligence agencies; (ii) in some Member States the PIUs that assess the PNR data are actually embedded in the national security agencies.[37] The national security agencies can also (indirectly) enter "Article 36" alerts on "persons of interest" into Europol's SIS system.[38]

[35] For a description of the kinds of technologies used, see Ian Brown & Douwe Korff, The inadequacy of UK data protection law in general and in view of UK surveillance laws, Part Two on *UK surveillance law*, 30 November 2020, available at:

https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-Part-Two-DK-IB201130.pdf

Although this describes the UK surveillance technologies, practices and arrangements, the remaining EU Member States are increasingly using the same technologies and practices in this context, and in this context are creating (or have already created) similar networks and data sharing arrangements with other countries including non-EU countries (so-called third countries) including the UK.

[36] See Ian Brown & Douwe Korff, Privacy and Law Enforcement, study for the UK Information Commissioner, released on the Commissioner's website in September 2004 as *"Striking the Right Balance: Respecting the Privacy of Individuals and Protecting the Public from Crime"*, Paper No. 4, *The legal framework: an analysis of the 'constitutional' European approach to issues of data protection and law enforcement*, p. 146 (repeated on p. 164). No longer available from the ICO website but available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3737428

[37] Earlier opinion (footnote 8, above), section 4.2, *The [PNR] system*, on p. 39.

[38] *Idem*, box on p. 17.

In that regard, it is important to note that, as discussed in more detail elsewhere,[39] **the Court of Justice has restrictively interpreted the national security exemption in the Treaties**. First of all, in its Grand Chamber judgment in *La Quadrature du Net* (*LQDN*),[40] the Court for the first time[41] gave a definition of national security:

> That responsibility corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.
>
> (LQDN, para. 135)

This is similar to the derogation clause in the European Convention on Human Rights that refers to" time[s] of war or other public emergency threatening the life of the nation" (Article 15).

Secondly, the Court confirmed its earlier case-law in which it held that:

> although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law.
>
> (*LQDN*, para. 99, with reference to earlier judgments)

The Court therefore held that the rules on personal data processing operations by entities that are, during such processing, subject to EU data protection law (in that case, providers of electronic communication services, who are subject to the e-Privacy Directive), *including processing operations by such entities resulting from obligations imposed on them under Member States' laws for national security purposes* can be assessed by the Court for their compatibility with the relevant EU data protection instrument and the Charter of Fundamental Rights.[42] In that case, the

[39] Ian Brown and Douwe Korff, Exchanges of personal data after the Schrems II judgment, study carried out at the request of the European Parliament's Civil Liberties (LIBE) Committee into the future of EU – US flows of personal data, July 2021, section 2.2.2, *The national security exemption in the EU Treaties*, available at:

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

[40] CJEU, GC judgment in Joined Cases C-511/18, C-512/18, La Quadrature du Net v. France, and C-520-18, Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL and others v. Belgium, 6 October 2020, ECLI:EU:C:2020:791.

[41] Sarah Eskens, *EU power over intelligence gathering for national security purposes*, presented at TILTing 2021: Regulating in Times of Crisis, 19 May 2021.

[42] Para. 101 (see also para. 102).

Court held that laws that required telecom providers "*as a preventive measure, … the general and indiscriminate retention of traffic and location data*", were incompatible with the Charter.[43]

Conclusion 5:

It follows from the PNR judgment of the CJEU that even when Member States hold exclusive competence in some areas (such as, in particular, national security), if the exercise of that competence affects an area where the EU has competence and that is covered by EU law (e.g., data protection, internal market), the exercise of that exclusive Member State competence may not impinge on the EU legal order or undermine the relevant EU legal rules.

Therefore, whenever an EU Member State exercises its exclusive competence in relation to national security to impose obligations on entities that are subject to EU law in their relevant activities, whether these are those telecommunication service providers, airlines, or providers or users of AI – those obligations must be compatible with the relevant EU law such as the GDPR, the LED, or the Europol Regulation (all read in line with the PNR judgment This compatibility also needs to extend to future such as the AI Act (also read in that way), and more generally with the EU Charter of Fundamental Rights- and the Court of Justice is competent to assess that compatibility. Therefore, whenever an EU Member State exercises its exclusive competence in relation to national security to impose obligations on entities that are subject to EU law in their relevant activities, whether these are those telecommunication service providers, airlines, or providers or users of AI – those obligations must be compatible with the relevant EU law such as the GDPR, the LED, or the Europol Regulation (all read in line with the PNR judgment). This compatibility also needs to extend to future regulation such as the AI Act (also read in that way), and more generally with the EU Charter of Fundamental Rights- and the Court of Justice is competent to assess that compatibility.

With specific regard to the deployment of AI systems, **when such systems are operated by national security agencies, their results are often fed into the systems of other entities that are subject to EU law and the Charter of Fundamental Rights (e.g., Frontex, Europol or national law enforcement agencies). This determines or influences the decisions of those entities. Alternatively the national security agencies themselves use data provided by entities that are subject to EU law and the Charter, in order to take decisions in relation to such individuals.**

[43] Para. 228.

As further discussed at 4, the Commission, in its proposal for the AI Act rightly noted that (emphasis added):

> **To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union**, this Regulation should also apply to providers and users of AI systems that are established in a third country, to the extent the output produced by those systems is used in the Union. (Recital 11)

In my opinion, this same reasoning should apply in relation to entities that, while established in the EU, are not subject to EU law or the Charter – i.e., to the EU Member States' national security agencies.

In the present context, this means that:

Conclusion 6:

Any EU rules covering the links 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. In the present case, of the AI Act, this includes the ban on unexplainable and unchallengeable AI systems that in my opinion (because of the PNR judgment).

Specifically, those rules should ensure that the exchanges of personal data between entities governed by EU law (including Europol, Frontex, EU missions, law enforcement agencies of EU Member States) and the national security agencies of the EU Member States do not result in the making decisions that significantly affect the rights of individuals protected by the Charter on the basis of the use of unexplainable and unchallengeable AI systems.

4.1.2 Activities of EU agencies and EU Member States in the Area of Freedom, Security and Justice (AFSJ)

The AI Act is a single market measure, like the EU General Data Protection Regulation.[44] Private-sector entities using AI systems in the context of their

[44] Proposal (footnote 2, above), section 2.1, Legal basis. This explains that *"The legal basis for the proposal is in the first place Article 114 of the Treaty on the Functioning of the European Union (TFEU), which provides for the adoption of measures to ensure the establishment and functioning of the internal market".* Indeed, *"This proposal constitutes a core part of the EU digital single market strategy."* But: *"In addition, considering that this proposal contains certain specific rules on the protection of individuals with regard to the processing of personal data, notably restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement, it is appropriate to base this regulation, in as far as those specific rules are concerned, on Article 16 of the TFEU."*

economic activities will therefore be subject to the Act. The same applies to providers (developers) of AI systems, even if the systems they develop are intended for use by law enforcement agencies (or indeed by national security agencies): developing and placing such systems on the market is an economic activity that is subject to internal market rules (and Article 16 CFR).

Entities such as Europol and Frontex and Member States' law enforcement agencies, when acting under other instruments (the Europol Regulation, Regulation 2018/1725, or the Law Enforcement Directive, etc.) will not be subject to the AI Act (just like they are not subject to the GDPR). However, they are still subject to the Charter as interpreted by the Court of Justice, and specific rules relating to their area of activity must be adopted for them that mirror the AI Act rules including the ban on unexplainable and unchallengeable ML/AI systems that must now be read into the AI Act because of the PNR judgment.

More specifically, in relation to processing of personal data, the Law Enforcement Directive and the Europol Regulation contain extensive rules that are generally close to those set out in the GDPR and in the data protection regulation for the EU institutions, Regulation (EU) 2018/1725. The exception to this is –= that the LED and the Europol Regulation are less strict as concerns the taking of decisions based solely on automated processing, including profiling – which typically involves the use of AI – , leaving this largely to EU or Member State law.[45]

On 29 September 2022, it was reported that the Council Legal Service (CLS) is of the opinion that one of the legal bases used in the proposed Artificial Intelligence Act "is not justified", and the Act can only rely on provisions relating to the internal market and data protection. See:

https://www.statewatch.org/news/2022/september/eu-ai-act-council-legal-service-says-police-cooperation-legal-basis-is-not-justified/

[45] The GDPR and the data protection regulation for the EU institutions, Regulation (EU) 2018/1725, stipulate in identical terms that (subject to exceptions) *"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."* (Article 22(1) GDPR; Article 24(1) Regulation 2018/1725). By contrast, the Law Enforcement Directive stipulates that *"Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller"* (Article 11)(1) LED); and the Europol Regulation stipulates that *"No decision by a competent authority which produces adverse legal effects concerning a data subject shall be based solely on automated processing of [sensitive data], unless the decision is expressly authorised pursuant to national or Union legislation."* (Article 30(4)).

Crucially, as explained in my earlier opinion,[46] Europol in particular has become increasingly involved in algorithm/AI-based data analysis (and in the research underpinning those technologies):[47]

> Europol is [already – DK] described as the EU's 'criminal information hub'[48] and the main 'information broker',[49] as it facilitates information exchange between EU Member States, Europol, other EU bodies, international organisations and third countries, and produces criminal intelligence on the basis of information acquired from various sources, including Member States and its partners. **Amongst its many tasks, Europol** also supports and coordinates cooperation on cross-border police work and **produces** regular assessments that offer comprehensive, **forward-looking analyses of crime and terrorism in the EU**.

This development is reinforced by the recently updated Europol mandate, that also expands data exchanges with private parties and third countries:[50]

The text of the new mandate introduces changes in the following areas:

> **Research and innovation**
>
> Given the challenges that the use of new technologies by criminals poses to the EU's security, law enforcement authorities need to strengthen their technological capabilities. To achieve this, the regulation tasks Europol with supporting member states in the use of emerging technologies. **Europol should also work to explore new approaches and develop common technological solutions, including solutions based on artificial intelligence, which should always be subject to robust security and fundamental rights safeguards**.

[46] Earlier opinion (footnote 8, above), section 2.3, The Schengen Information System (SIS), Europol and European Arrest Warrants (EAWs).

[47] Niovi Vavoula and Valsamis Mitsilegas, Strengthening Europol's mandate: A legal assessment of the Commission's proposal to amend the Europol Regulation, study requested by the European Parliament's Civil Liberties (LIBE) Committee, May 2021, p. 12, emphasis added, available at:

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694200/IPOL_STU(2021)694200_EN.pdf

[48]'Europol Strategy 2020+' (*Europol*, 5 February 2019) < https://www.europol.europa.eu/publications-documents/europolstrategy-2020 > accessed 3 May 2021, 4 [original footnote]

[49] Thomas Wahl, 'The European Union as an Actor in the Fight Against Terrorism' in Marianne Wade and Almir Maljevic (eds), A War on Terror? (Springer 2010) 144. [original footnote]

[50] EU Council press release, "Europol: provisional agreement between the Council presidency and the European Parliament on the agency's new mandate", 1 February 2022, emphases added, available at:

https://www.consilium.europa.eu/en/press/press-releases/2022/02/01/europol-provisional-agreement-between-council-presidency-and-european-parliament/

The new mandate entered into force on 28 June 2022:

https://www.europol.europa.eu/media-press/newsroom/news/europols-amended-regulation-enters-force

> **Processing of large data sets**
>
> Data collected in criminal investigations have been increasing in size and complexity. Member states cannot always detect cross-border links through their own analysis of the data. Under the draft regulation, **Europol will be able to process large and complex data sets to support member states in their fight against serious crime and terrorism**. The regulation also includes strict requirements to ensure that any data **processing by Europol always respects fundamental rights**, including the right to privacy, aligning this regulation with the EU regulation on data protection.
>
> …
>
> **Cooperation with private parties**
>
> As a result of the increased use of online services by criminals, private parties hold an increasing amount of personal data that may be relevant for criminal investigations. Under the draft regulation, Europol will be able to receive personal data directly from private parties, to ensure a point of contact at EU level to lawfully share multijurisdictional data sets. Europol will then be able to **analyse these data** sets in order to identify the relevant member states and forward the information to the national authorities.
>
> **Cooperation with third countries**
>
> The regulation extends the scope for Europol to cooperate with third countries. It introduces the possibility to **exchange personal data with countries where appropriate safeguards have been provided for in a legally binding instrument or exist based on a self-assessment carried out in the framework of Europol**.

Analysis and conclusion(s)

It is worth noting that while the above does mention "aligning [of the Europol Regulation] with the EU regulation on data protection", i.e., with the GDPR and the Law Enforcement Directive (LED), it does not mention alignment with the AI Act. In my opinion, it follows from the PNR judgment that the Europol Regulation, as well as any rules that apply to EU agencies acting in the Area of Freedom, Security and Justice, and the rules that apply to national law enforcement agencies when they operate under EU law, must all be aligned also with the AI Act, as applied in accordance with the PNR judgment.

Conclusion 7:

Unexplainable and unchallengeable AI systems should not be researched, developed or used in any area of EU competence, i.e., not in the internal market (as will be clear if the AI Act and the GDPR are applied in accordance with the PNR judgment), but also not by Europol or any other EU agency or Member State entity active in the Area of Freedom, Security and Justice.

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 the taking of any decision that significantly affects the fundamental rights of individuals is incompatible with the Charter and therefore also with each and every one of those instruments. Consequently:

(i) The application of the Europol Regulation should be expressly aligned with the AI Act (just as it is supposedly already aligned with the GDPR and the LED) and in any processing of personal data that is subject to the Europol Regulation, Europol should not use unexplainable and unchallengeable AI systems;

(ii) All EU legal instruments and policies relating to police cooperation between the EU Member States and between the Member States and the EU (in particular Europol) should be reviewed and revised to reflect and respect the prohibition on the use of unexplainable and unchallengeable AI systems in relation to the taking of decisions that significantly affect the fundamental rights of individuals;

(iii) Member States' law enforcement agencies should, in any processing of personal data that is subject to EU law including the Law Enforcement Directive and the Charter, not use unexplainable and unchallengeable AI systems;

(iv) All EU legal instruments and policies relating to Frontex or other border control or other AFSJ matters should be reviewed and revised to reflect and respect the prohibition on the use of unexplainable and unchallengeable AI systems in relation to the taking of decisions that significantly affect the fundamental rights of individuals; and

(v) All EU Institutions should, in any processing of personal data that is subject to Regulation 2018/1725 (and the Charter), not use unexplainable and unchallengeable AI systems.

(vi) Moreover, none of the above entities should only be allowed to use non-ML-based AI systems unless they comply with the strict conditions set out above.

(vii) Pending the formal revisions of the instruments mentioned at (i) to (v) above, all EU research and development of AI systems – and a fortiori all already-in-place deployments of such systems – should be urgently reviewed in the light of the PNR judgment.

4.1.3 AI systems developed or used for military purposes:

Article 2(3) of the proposed AI Act stipulates bluntly that:

> This Regulation shall not apply to AI systems developed or used exclusively for military purposes.

The relevant recital, recital 12, suggests that, just as in relation to Europol and other matters falling within the Area of Freedom, Security and Justice, this is because military matters "*fall[ ] under the exclusive remit of the Common Foreign and Security Policy regulated under Title V of the Treaty on the European Union (TEU)*", i.e., cannot be regulated in a single market instrument.[51] However, the recital actually qualifies this and stipulates that:

> AI systems exclusively developed or used for military purposes should be excluded from the scope of this Regulation *where that use falls under the exclusive remit of the Common Foreign and Security Policy regulated under Title V of the Treaty on the European Union (TEU)* (italics added)

Analysis and conclusion(s)

The above deserves three areas of comment. First of all, as the recital actually makes clear, **military activities and matters relating to defence are not excluded from EU competences**. Indeed, the **EU Common Security and Defence Policy (CSDP)** (which is part of the EU Common Foreign and Security Policy, CFSP):[52]

> Provides the European Union with an operational capacity to deploy civilian and military missions and operations abroad.
>
> Their tasks range from conflict prevention and peace-keeping, crisis-management, joint disarmament operations, and military advice and assistance tasks to humanitarian and rescue and post-conflict stabilisation tasks. ...
>
> Since 2003 the EU has launched and run 37 operations and missions on three continents. As of today [March 2022], there are 18 ongoing CSDP missions and operations [involving around 4,000 EU military and civilian staff], of which 11 are civilian and 7 military.

[51] Cf. footnote 42, above.

[52] European External Action, *EU Missions and Operations*, March 2022, available at: https://www.eeas.europa.eu/eeas/eu-missions-and-operations_en

In 2016, the EU Council also agreed to deepen defence cooperation among the Member States and adopted a common set of proposals for EU-NATO cooperation, based on the Joint Declaration signed in Warsaw in July 2016, and endorsed by both EU and NATO Councils on 6 December of that year.[53] The Joint Declaration identified seven areas of deeper EU-NATO cooperation including "defence industry and research".[54] The **EU's European Defence Action Plan (EDAP)** also aims to:[55]

1. **Establish a European Defence Fund** to foster cooperation in defence projects and support the whole sequence of defence capability development, from research to prototype and acquisition. It is be composed of two complementary "windows":
   - (i) a "research window" to fund collaborative research in innovative defence technologies such as electronics, metamaterials, encrypted software or robotics but also any technologies needed to developed specific defence capabilities considered a priority. €25 million for defence research have already been approved as part of the 2017 EU budget. This allocation is a first step to test the waters for supporting defence research at EU level. The Commission expects that this budget allocation could grow to a total of €90 million until 2020.[56]
   - (ii) A "capability window" to support Member States in developing defence capabilities through cooperation

2. **Foster investments in SMEs** and other suppliers to the defence industry through supporting efforts to improve their access to funding from the European Investment Bank and the European Structural and Investment Fund.

3. **Strengthen the Single Market for defence.** Developing an open and competitive European defence market will help companies operate across borders and Member States get best value for money in their defence procurement.

[53] See: EEAS, Defence Package: Fact Sheet, available at:

https://www.eeas.europa.eu/sites/default/files/defence_package_factsheet_0.pdf

[54] Idem.

[55] Idem.

[56] That was written in 2016. In 2017, it was reported that the Commission was launching a scoping study to refine the budget estimates for the "capability window" of the European Defence Fund, and that "the funding for the Research Window will come from the EU budget. We [the European Commission] have proposed an overall budget of €90 million for the Preparatory Action and €500 million per year for a research programme under the next multi-annual Financial Framework starting in 2021." European Defence Matters, Issue 12 (undated), Lowri Evans, European Commission Director General for Internal Market, Industry, Entrepreneurship and SMEs: *"EDAP needs to be implemented in a transparent way and in close partnership with Member States"*, available at:

https://eda.europa.eu/webzine/issue12/cover-story/edap-needs-to-be-implemented-in-a-transparent-way-and-in-close-partnership-with-member-states

The research into and development of "innovative" military and defence "capabilities" will undoubtedly include research and development and placing on the market of AI systems. As NATO puts it in relation to its own activities and standards in this field:[57]

> Artificial Intelligence (AI) is changing the global defence and security environment. It offers an unprecedented opportunity to strengthen our technological edge but will also escalate the speed of the threats we face. This foundational technology will likely affect the full spectrum of activities undertaken by the Alliance in support of its three core tasks; collective defence, crisis management, and cooperative security.

The technology will clearly equally affect "the full spectrum of activities" undertaken by the EU in this area, in particular those noted in relation to the ECDP and EDAP.

Secondly, it is correct that since the AI Act is a (digital) single market measure, it cannot apply to activities relating to the CFSP and the CSDP under Title V TEU. However, as the recital itself makes clear, not all "AI systems developed or used for military purposes" – indeed, not even all such systems "exclusively" developed or used for those purposes – are used in the context of the CSFP.

There is no reason why military AI systems (or indeed any military products) brought onto the market in the EU, or used by users in the EU, should not be subject to single market rules including, e.g., competition or product safety rules – and the AI Act – even if the *use* of such products or services in a CFSP context will be covered by separate rules (to which I will come below).

Indeed, trade in military equipment *is* actually subject to EC directives, most notably the Defence_Procurement Directive and the Intra-Community Transfers (ICT) Directive that make up the **EU Defence Package** (even though they do not appear to be very effectively implemented).[58] [59]

It is therefore simply not true that the Commission has no competence in relation to the development or placing on the market or putting into service of military AI goods or services (software including AI systems can take either form, in the latter case if offered as "Software-as-a-Service" or SaaS).

[57] NATO, Summary of the NATO Artificial Intelligence Strategy, 22 October 2021, available at: https://www.nato.int/cps/en/natohq/official_texts_187617.htm

[58] See the study for the European Parliament, Isabelle Ioannides (ed.), EU Defence Package: Defence Procurement and Intra-Community Transfers Directives, October 2020, available at: https://op.europa.eu/en/publication-detail/-/publication/3a977249-3e88-11eb-b27b-01aa75ed71a1/language-en

[59] The EU has also adopted rules on the export of military goods. See, e.g., the "Common Military List" of the EU, covering equipment covered by Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XG0313(07)

Conclusion 8:

There is no justification for the exemption in the AI Act relating to AI systems developed or used for military purposes (or dual purposes: see below) 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. Furthermore, 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.

Third, because CSFP activities – like all EU activities – are subject to the Charter, the separate CFSP rules should also unambiguously stipulate that AI systems posing "unacceptable" risks to fundamental rights should not be used by any EU entity, also not "*where that use falls under the exclusive remit of the Common Foreign and Security Policy regulated under Title V of the Treaty on the European Union (TEU).*" This is all the more important because unexplainable and unchallengeable AI systems pose an especially serious – indeed, potentially lethal – risk in military contexts. For instance, they could be used to try and determine whether a certain person in a conflict zone is a combatant (and thus a legitimate target) or a civilian or otherwise protected person; or whether a certain object is a civilian object or a military objective (the making of such distinctions being fundamental to the application of international humanitarian law, IHL).[60]

In fact, there are warnings that ML/AI-based lethal autonomous drones could soon become a reality (if they are not already).[61] As long ago as 2017, the US Department of Defense opened a call for the development of "automatic target recognition of personnel and vehicles from an unmanned aerial system using

[60] See, e.g., Marco Sassòli, Legitimate Targets Of Attacks Under International Humanitarian Law, Cambridge, 2003, available at:

https://hhi.harvard.edu/files/humanitarianinitiative/files/session1_legitimate_targets_ihl.pdf?m=1615827575

[61] BBVA Open Mind, Drones That Kill on Their Own: Will Artificial Intelligence Reach the Battlefield?, 8 May 2018, available at: https://www.bbvaopenmind.com/en/technology/artificial-intelligence/drones-that-kill-on-their-own-will-artificial-intelligence-reach-the-battlefield/

learning algorithms."[62] The Stop Killing Robots Coalition campaigns against them.[63]

In relation to AI, there is the additional complication that many AI systems are "general purpose" and can be used, or attuned for use, for civil or military (or indeed national security) purposes: in terms of the Wassenaar Agreement, they are "dual use".[64] This is the case, for instance, in relation to surveillance technologies – that increasingly rely on AI.[65]

Conclusion 9:

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 the taking of decisions that significantly affect the fundamental rights of individuals (especially any decisions on the use of force).

Pending the formal revisions of the CFSP and CSDP instruments mentioned above, all research and development of AI systems – and a fortiori all already-in-place deployments of such systems – used in these contexts, too, should be urgently reviewed in the light of the PNR judgment of the CJEU.

4.1.4 AI systems used by third countries or international organisations

When AI systems are operated by third country agencies or international organisations, specific international agreements may allow for their results to be fed into the systems of entities that are subject to EU law and determine or influence the decisions of those entities (e.g., EU institutions including Europol and Frontex, EU missions, law enforcement agencies of EU Member States operating under EU law). Equally, third country agencies or international

[62] Call for tenders for Automatic Target Recognition of Personnel and Vehicles from an Unmanned Aerial System Using Learning Algorithms, 29 November 2017, available at: https://www.sbir.gov/sbirsearch/detail/1413823

[63] https://www.stopkillerrobots.org/

[64] "The Wassenaar Arrangement has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. The aim is also to prevent the acquisition of these items by terrorists." https://www.wassenaar.org/

[65] Cf. The open letter sent by Reporters Without Borders, Amnesty International, Digitale Gesellschaft, the International Federation for Human Rights (FIDH), Human Rights Watch, Open Technology Institute and Privacy International to the Members of the Wassenaar Arrangement on 2 December 2014, available at: https://rsf.org/en/open-letter-members-wassenaar-arrangement

organisations may be allowed by international agreements to use data provided to them by entities that are subject to EU law (and the Charter) in order to take such decisions in relation to such individuals.

Nonetheless, Article 2(4) of the AI Act stipulates that:

> This Regulation shall not apply to public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States.

The reference to paragraph 1 of Article 2 relates to the fact that the AI Act will apply not only to "providers placing on the market or putting into service AI systems in the Union" (even if they are not established in the EU) (Article 2(1)(a)) and to "users of AI systems located within the Union" (Article 2(1)(b)), but also to:

> providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union (Article 2(1)(c)).

The justification is provided in recital 11:

> To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and users of AI systems that are established in a third country, to the extent the output produced by those systems is used in the Union. Nonetheless, **to take into account existing arrangements and special needs for cooperation with foreign partners with whom information and evidence is exchanged, this Regulation should not apply to public authorities of a third country and international organisations when acting in the framework of international agreements concluded at national or European level for law enforcement and judicial cooperation with the Union or with its Member States.** Such agreements have been concluded bilaterally between Member States and third countries or between the European Union, Europol and other EU agencies and third countries and international organisations. (Emphasis added)

The "existing arrangements with foreign partners with whom information and evidence is exchanged" and the "international agreements for law enforcement and judicial cooperation" concluded between third countries and the EU and between third countries and EU Member States bilaterally are not spelled out. But in 2018, the European Data Protection Supervisor issued an opinion on negotiating mandates to conclude international agreements allowing the exchange of data between Europol and eight third countries of the Middle East and North African (MENA) regions, i.e,. Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey.[66] The EDPS wrote that the international agreements that would result from the negotiations "*would provide the required legal basis for the exchange of personal data between Europol and the authorities of these third countries competent to fight serious crimes and terrorism.*"[67] This is somewhat odd, because Europol's own website says that "*[s]ince 1 May 2017, Europol no longer concludes any agreements which allow for the exchange of personal data*" (i.e., "operational agreements").[68] That is in fact contradicted by a later statement, of April 2021, that said that:[69]

> Thanks to the conclusion of the [EU-UK Trade and Partnership Agreement], Europol could initiate the operational cooperation with the UK as third state [and thus exchange personal data with the UK – DK] already at the start of this year.

But whatever that be, two matters must be noted. First of all, while the EDPS is in principle correct in noting that international agreements can provide a legal basis for the exchange of personal data between Europol and authorities of third countries, such agreements are of course nevertheless subject to the Charter: any agreement – or specific elements of an agreement – that would be in breach of the Charter, or would foreseeably lead to breaches of the Charter, must be regarded as invalid, and can, and should be, invalidated by the Court.

Secondly, there is an odd conflict between the first and the second sentence in the long quote from recital 11, provided above. The first sentence notes the need to "*to prevent the circumvention*" of the AI Act. But the second sentence suggest that this need can be ignored in relation to "*existing arrangements and special needs for cooperation with foreign partners*" in the area of law enforcement.

Analysis and conclusion(s)

The above is dubious in general: since the whole point of the AI Act is the adoption of measures to ensure the establishment and functioning of the internal market and to protect individuals and their fundamental rights, its requirements

[66] EDPS, Opinion 2/2018 on eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries, 14 March 2018, available at:

https://edps.europa.eu/sites/default/files/publication/18-03-19_opinion_international_agreements_europol_en.pdf

Executive Summary available at:

https://edps.europa.eu/sites/default/files/publication/18-03-19_opinion_international_agreements_europol_executive_summary_en.pdf

[67] Executive Summary, *Introduction*, second paragraph.

[68] See: https://www.europol.europa.eu/partners-collaboration

[69] Europol, Conditions applicable to the cooperation with the UK since 1 January 2021, 29 April 2021, available at:

https://www.europol.europa.eu/media-press/newsroom/news/conditions-applicable-to-cooperation-uk-1-january-2021 should not be overridden in a law enforcement context (although there can be special, limited and conditional exceptions, as discussed below). But more specifically, if under the AI Act (and the PNR judgment) a particular AI system must classified as "unacceptable" and fundamentally in breach of the Charter – then no exception can be allowed to its use. Also, not – indeed especially also not – in an international law enforcement context.

Conclusion 10:

Rather than exempting whole ranges of "arrangements" and "agreements" with foreign countries and partners from the protections of individuals that must be granted to them under the Charter, no such "arrangements" and "agreements" should ever be entered into or adopted if they do not respect, or lead to violations of, the rights and freedoms of individuals under the Charter. For example: such links and data exchanges should never lead to the torture or unlawful killing of anyone, or to refoulement of refugees.

If there are previously-agreed "arrangements" or previously-adopted "agreements" in place that do not meet the requirements of the Charter – or even expressly allow for actions that violate the Charter – then those "arrangements" and "agreements" must be urgently suspended, reviewed and revised to bring them into line with the Charter.

This applies a fortiori to links with third country national security agencies such as the US National Security Agency (NSA) and the UK agencies MI5 and MI6 – to which, as the Court of Justice has expressly clarified, the Article 4 TFEU exemption does not apply.[70]

This also applies when the Court of Justice clarifies what is and what is not compatible with the Charter – as the Court has done in relation to the use of AI systems in its PNR judgment. Specifically:

The links and data exchanges between EU institutions (including Europol and Frontex), EU missions, law enforcement agencies of EU Member States when operating subject to EU law, on the one hand, and third countries and international organisations on the other hand, should not result in the taking of decisions that significantly affect the rights of individuals protected by the Charter on the basis of unexplainable and unchallengeable AI systems.

[70] CJEU Grand Chamber judgment of 16 July 2020 in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("Schrems II"), ECLI:EU:C:2020:559, para. 81. Note in that regard in particular the "operational cooperation" agreement between Europol and the UK, mentioned above and referenced in the previous footnote.

The EU should also provide input into AI policy and standard-setting debates in international organisations including the UN and UNESCO,[71] the OECD,[72] the Council of Europe[73] and NATO,[74] to push for the adoption by those organisations of prohibitions on unexplainable and unchallengeable AI systems in all contexts.

This is especially important in relation to the use of AI for military purposes, as noted above. The EU should involve itself in the debates on the use of military AI, including the use of AI systems in drone strikes, fully in line with the Charter and IHL (which, like the ECHR and IHL, are effectively congruent)[75] and the case-law of the Court of Justice.

Exception clause:

Remote biometric identification in public places for the purpose of law enforcement

The AI Act contains one, rather complex exception clause, in Article 5(1)(d), read with Article 5(2), that reads as follows (emphases added):

> (1) The following artificial intelligence practices shall be **prohibited**:
>
> …
>
> (d) **the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, *unless* and in as far as such use is strictly necessary** for one of the following objectives:
>
> (i) the targeted search for specific potential victims of crime, including missing children;
>
> (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;
>
> (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in

[71] See footnote 3, above.

[72] *Idem*.

[73] There are already close communications and forms of cooperation between the EU and the Council of Europe in this (as in many other) regards.

[74] Extensive attention is being given to AI in military circles and within NATO. See, e.g.:

https://emerj.com/ai-sector-overviews/artificial-intelligence-in-the-military-an-overview-of-capabilities/

https://www.rand.org/pubs/research_reports/RR3139-1.html

https://stanleycenter.org/publications/military-applications-of-artificial-intelligence/

https://link.springer.com/content/pdf/10.1007/978-3-030-51110-4.pdf (with a useful section on applicable IHL standards)

[75] See footnote 84, below.

Article 2(2) of Council Framework Decision 2002/584/JHA 62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.

(2) The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements:

(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;

(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with **necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations**.

Analysis and conclusion(s)

This exception clause is seriously problematic because remote biometric identification (RBI) systems (as distinct from authentication systems) are inherently unreliable, leading to both excessive false positives – which in law enforcement contexts lead to persons being stopped, searched and detained who in fact are not linked to a relevant threat or crime – and discriminatory outputs and outcomes that disproportionally affect ethnic minority and other disadvantaged groups.[76] Systems with such serious defects fail to "respect the essence" of the rights to privacy, to freedom to move freely in public spaces, to not be discriminated against, and even to liberty. Furthermore, as is clear from the PNR judgment of the CJEU, the inherent opacity of the algorithms on which the systems are based also affects the essence of the right to an effective remedy.

[76] See "Reclaim Your Face" Campaign: Open Letter to the Members of the European Parliament, 10 May 2022: https://reclaimyourface.eu/meps-will-you-stand-up-for-our-rights-and-ban-bms/; and Press Release "European Parliament calls loud and clear for a ban on biometric mass surveillance in the AI Act", 14 September 2022: https://edri.org/our-work/european-parliament-calls-loud-and-clear-for-a-ban-on-biometric-mass-surveillance-in-ai-act/

Conclusion 11:

The exceptions to the prohibition of the use of 'real-time' remote biometric identification systems (as distinct from authentication systems) in publicly accessible spaces for the purpose of law enforcement in the AI Act should be scrapped altogether: all uses of RBI (whether real-time or post) in publicly- accessible spaces should be included in the prohibition, as they do not meet existing EU fundamental rights standards.

4.2 Exemption and exception clauses in the draft CoE AI Convention

Exemption clause:

National defence

Reportedly, the "zero draft" of the AI Convention does not provide for an exemption from the Convention in relation to national security. Rather, national security is to be mentioned in the exception ("restriction") clause, discussed below under the next heading.

On the other hand, it is proposed that the proposed AI Convention should not apply to the design, development or application of AI systems that are (or are to be) used for purposes related to national defence.[77]

The final preparatory document for the convention, containing an "outline of the elements of an appropriate legal instrument" relating to AI says the following in this regard:[78]

> It is important to underline that the planned legal instrument would not regulate all aspects of the design, development and application of artificial intelligence systems, but merely those pertaining to the mandate of the Council of Europe with a specific focus on such artificial intelligence systems that pose a risk from the point of view of safeguarding and protecting human rights, preserving and fostering democracy and observing the rule of law.
>
> It also means that the scope of the planned legal instrument would reflect the limitations imposed by the mandate of the Council of Europe in that military matters such as those relating to national

[77] Reportedly, the "zero draft" of the AI Convention uses the American version of the term, "defense", even though the CofE Statute provision to which it is said to relate (as discussed in the text) uses "defence".

[78] Council of Europe, Committee on Artificial Intelligence (CAI), *Outline of the Elements of an Appropriate Legal Instrument – Proposal from the Secretariat* (CAI(2022)01), 11 March 2022, p. 2.

> defence in accordance with Article 1 (d) of the Statute of the Council of Europe would fall outside of it. At the same time, the latter limitation would not create any prejudice or be detrimental to the already existing level of human rights protection under the existing international legal regime.

Analysis and conclusion(s)

The above argument is disingenuous and dangerous.

It is important to differentiate the limitation in Article 1(d) of the Statute of the Council of Europe from the exclusion from legislative (or other) competence of the European Union under Article 4(1) TEU. As noted in relation to EU law, above, the EU AI Act will be an EU law (more specifically, a regulation) that is part of the legal order of the EU – an order that is separate from and has primacy over the law of the EU Member States.[79] The EU is a *supra*-national governmental organisation with its own legal order and its legal instruments operate, and must operate and be construed, within the EU Treaties.

The situation in relation to the Council of Europe is fundamentally different. The Council of Europe is an *inter*-governmental organisation. The (many) treaties it issues are separate agreements between the states that become party to them – and that can often be states that are not even members of the Council.[80]

Crucially, the most important Council of Europe-written treaty, the European Convention on Human Rights,[81] does not contain any stipulation exempting "matters relating to national defence" from its scope.[82] On the contrary, it has a special clause, Article 15, that permits derogations from most (not all) the

[79] The CJEU developed the fundamental doctrines of direct effect and primacy of EU law in the landmark cases van *Gend en Loos v Nederlandse Administratie der Belastingen* and *Costa v ENEL*. For a brief summary, see: European Parliament Fact Sheet on the European Union, *Sources and scope of European Union law*, June 2022, available at:

https://www.europarl.europa.eu/factsheets/en/sheet/6/sources-and-scope-of-european-union-law

The European Commission reaffirmed the primacy of EU law in the face of threats to it from the Polish Constitutional Court in October 2021, see:

https://ec.europa.eu/commission/presscorner/detail/en/statement_21_5142

[80] The Council of Europe treaty database website (which is searchable by treaty name or number) lists 224 treaties: https://www.coe.int/en/web/conventions/full-list

Treaties that are only open to Council of Europe Member States – such as the European Convention on Human Rights – are called "European Conventions", while treaties that are also open to non-Council of Europe Member States – such as the CoE Data Protection Convention – are called "Council of Europe Conventions". The AI Convention will be one such "Council of Europe Convention" and therefore open for accession by non-Council of Europe states.

[81] CETS No. 005.

[82] It also contains no exemption in relation to national security – and in fact there is extensive case-law under the ECHR in which the Convention provisions are applied to national security matters including surveillance, typically with reference to the exception clauses discussed under the next heading. See: European Court of Human Rights Research Division, National security and European case-law, Strasbourg, 2013, available at: https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf

Convention rights “in time of war or other public emergency threatening the life of the nation”. The second paragraph of that article moreover stipulates, *inter alia*, that no derogation shall be permissible, even in times of war, from the right to life as guaranteed by Article 2 of the Convention, “*except in respect of deaths resulting from lawful acts of war*”.[83]

If the European Convention on Human Rights did not apply at all in relation to “national defence” – i.e., to war, or more specifically, a situation in which the laws of war, International Humanitarian Law apply – there would have been no need for the derogation clause. The *travaux préparatoires* to the Convention, as now available online, contain no suggestion that any of the drafters of the Convention felt that matters relating to defence need not be covered because they fell outside the scope of the Convention.[84]

The authors of the leading textbook on the Convention write in the latest edition that:[85]

[83] As I pointed out in the Council of Europe Human Rights Handbook No. 8: The Right to Life, : A guide to the implementation of Article 2 of the European Convention on Human Rights, Strasbourg, 2006: *“The reference to ‘deaths resulting from lawful acts of war’ is a straightforward reference to the norms of international humanitarian law. This means that acts resulting in loss of lives, committed during times of war, and which contravene international humanitarian law, are ipso facto also violations of Article 2. Conversely, killings in times of war which are in accordance with international law are not in violation of the Convention. The Convention and the standards derived from international humanitarian law are thus, in this respect, fully congruent.”* (p. 55). The Handbook is available at:

https://www.echr.coe.int/LibraryDocs/HR%20handbooks/handbook08_en.pdf

See also the Court’s own, more recent Guide on Article 2 of the European Convention on Human Rights – Right to Life, updated on 30 April 2022, which clarifies that *“The Court has … underlined that Article 2 must be interpreted in so far as possible in light of the general principles of international law, including the rules of international humanitarian law”* (para. 124). The Guide is available at:

https://www.echr.coe.int/Documents/Guide_Art_2_ENG.pdf

[84] European Commission of Human Rights, Preparatory Work on Article 15 of the European Convention on Human Rights (DH(56)4), 22 May 1956, available at:

https://www.echr.coe.int/LibraryDocs/Travaux/ECHRTravaux-ART15-DH(56)4-EN1675477.pdf

The original version in French is also available:

https://www.echr.coe.int/LibraryDocs/Travaux/ECHRTravaux-ART15-DH(56)4-FR1675476.pdf

These documents were previously confidential. However, in 1965, the Parliamentary Assembly of the Council of Europe (PACE), called for the travaux préparatoires to be publishd and made available: PACE Recommendation 417(1965), available at:

https://pace.coe.int/en/files/14454/html

The full travaux préparatoires were commercially published in eight volumes running to several thousand pages by Martinus Nijhoff, publishers. However, the Court has also made travaux préparatoires on specific articles available on its on website and although these contain the advice to not cite those, but rather the full version, I have chosen to ignore that and work with the online pages.

[85] Harris, O’Boyle & Warbrick, Law of the European Convention on Human Rights, 4th ed., Oxford, 2018, p. 806. Regrettably, they do not provide references to any such cases.

> The Strasbourg authorities [i.e., the European Court of Human Rights and the previous European Commission of Human Rights] have rejected the claims of states that questions arising under Article 15 are beyond their competence altogether …

(They add that, rather, "[those authorities] have approached cases before them rather cautiously, some say too cautiously" – but that is beside the present point.)

If the reported assertions of the proponents of the "zero draft" of the AI Convention, that Article 1(d) of the Statute of the Council of Europe imposes on them a duty to exclude AI systems used for national defence purposes from the AI Convention – then that same obligation would rest, and would have rested ab initio, on the drafters of all Council of Europe-issued treaties, including the ECHR. And to the extent that this was not explicitly spelled out in those treaties, that limitation would have had to be read into (all of) them.

But even though it appears that some states at least may have put forward arguments on that line, they have been rejected by the Court of Human Rights – which has applied the Convention including, in particular, Article 2 (the right to life) to many situations of internal and international armed conflict.[86] See, e.g.: the cases of *Kelly* and *Shenaghan* that concerned killings by the UK armed forces in Northern Ireland; the cases of *Baysayeva* concerning unlawful detention of a person by unidentified servicemen, and of *Isayeva* that concerned the killing of a civilian, both in connection with Russian military operations in Chechnya; and the case of *Oruk* about the killing of six children in the context of Turkish military operations in the Kurdish region.

The proponents of the "zero draft" reportedly claim that their proposed full exclusion of military AI (and even its development) from the proposed AI Convention would not create any prejudice to the highly developed human rights protection system of the Council of Europe.

But that is simply untrue: Either those proponents are right – and in that case *no* CoE treaty can apply to defence matters. Or the European Court of Human Rights is right in holding that the ECHR can apply to defence matters – and in that case, *all* CoE treaties can apply to them.

The claim that the Statute of the Council of Europe "imposes" on the drafters of CoE treaties a duty to exempt military matters is also belied by practice. I have checked twenty-five CoE treaties that have some possible relevance in relation to

[86] See the Court's Guide on Article 2 (footnote 83, above), that gives numerous examples.

"military matters" and/or to processing of (personal) data in AI systems.[87] There is an exemption in relation to military contexts in only one: the Council of Europe Convention on the Prevention of Terrorism (CPT, CETS 196). Article 26 of this convention stipulates, in paras. (4) and (5) that:

> 4. Nothing in this Convention shall affect other rights, obligations and responsibilities of a Party and individuals under international law, including international humanitarian law.
>
> 5. The activities of armed forces during an armed conflict, as those terms are understood under international humanitarian law, which are governed by that law, are not governed by this Convention, and the activities undertaken by military forces of a Party in the exercise of their official duties, inasmuch as they are governed by other rules of international law, are not governed by this Convention.

But note that this exemption is to clarify that in the context of armed conflict, international humanitarian law applies, rather than the CPT. It is not argued in the Explanatory Report that this exemption is required because of Article 1(d) of the Statute of the Council of Europe. Rather, the Explanatory Report says that:

> The wording of paragraph 4 is based on similar provisions in recent international texts, including the Inter-American Convention against Terrorism (Article 15, paragraph 2) and United Nations Security Council

[87] I.e.: the ECHR (CETS 005); the European Cultural Convention (CETS 018); the European Convention for the Peaceful Settlement of Disputes (CETS 023); the European Convention on Mutual Assistance in Criminal Matters (CETS 030); the European Social Charter (CETS 035); the Agreement between the Member States of the Council of Europe on the issue to Military and Civilian War-Disabled of an International Book of Vouchers for the repair of Prosthetic and Orthopaedic Appliances (CETS 040); the Convention on the Reduction of Cases of Multiple Nationality and on Military Obligations in Cases of Multiple Nationality (CETS 043); the Protocol to the European Convention on Consular Functions concerning the Protection of Refugees (CETS 061A); the European Convention on the Protection of the Archaeological Heritage (CETS 066); the European Convention on State Immunity (CETS 074); the European Convention on the Non-Applicability of Statutory Limitation to Crimes against Humanity and War Crimes (CETS 082); the European Convention on the Suppression of Terrorism (CETS 090); the European Agreement on Transfer of Responsibility for Refugees (CETS 107); the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Data Protection Convention) (CETS 108); the European Convention on Offences relating to Cultural Property (CETS 119); the European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CETS 126); the Framework Convention for the Protection of National Minorities (CETS 157); the European Convention on the Exercise of Children's Rights (CETS 160); the Convention on the Protection of the Environment through Criminal Law (CETS 172); the Criminal Law Convention on Corruption (CETS 173); the Civil Law Convention on Corruption (CETS 174); the Convention on Cybercrime (Cybercrime Convention, also known as the Budapest Convention) (CETS 185); the Council of Europe Convention on the Prevention of Terrorism (CETS 196); the Council of Europe Convention on preventing and combating violence against women and domestic violence (also known as the Istanbul Convention) (CETS 210); and the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the Modernised Data Protection Convention) (CETS 223).

> Resolution 1566 (2004) which contains similar language (preambular paragraph 6).
>
> (Para. 276).

Of course, torture and inhuman or degrading treatment or punishment is also forbidden under IHL. In other words, the clause merely clarifies that in relation to such treatment in the context of armed conflict, IHL is a *lex specialis*, and applies instead of the CPT.

By contrast, there is no clause on the lines proposed for the CoE AI Convention in any of the other twenty-four treaties. The ECHR and the Social Charter contain derogation clauses for "times of war or other public emergency threatening the life of the nation" (in, respectively, Article 15 and 30), and the European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) (CETS 126) also contains a (very limited) exception/derogation clause (Article 9), but as already noted, if anything those confirm the application of those treaties to such circumstances (subject to the stipulations in those clauses). Other treaties mention "war disabled" and "war cripples" (CETS 040) or "military service" and "military obligations" (CETS 043), but again, if anything, this confirms that they apply to "military matters". One treaty (CETS 074 on State Immunity) contains a "without prejudice" clause (Article 31) that stipulates that:

> Nothing in this Convention shall affect any immunities or privileges enjoyed by a Contracting State in respect of anything done or omitted to be done by, or in relation to, its armed forces when on the territory of another Contracting State

but that, too, does not amount to a full exemption clause.

By contrast, the European Convention on the Non-Applicability of Statutory Limitation to Crimes against Humanity and War Crimes (CETS 082) is specifically aimed at "safeguard[ing] human dignity in time of war" and ensuring war crimes are punished. And most explicitly, the preamble to the relatively recent Istanbul Convention on preventing and combating violence against women and domestic violence (CETS 210) expressly recognises:

> the ongoing human rights violations during armed conflicts that affect the civilian population, especially women in the form of widespread or systematic rape and sexual violence and the potential for increased gender-based violence both during and after conflicts".

Indeed, Article 2(3) expressly stipulates that:

> This Convention shall apply in times of peace and in situations of armed conflict.

Conclusion 12:

"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.

The proposed exemption from the AI Convention for AI systems used for national defence purposes, if accepted as necessary to comply with Article 1(d) of the Statute, 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.

Exception clause:

General exception clause

The "zero draft" of the AI Convention reportedly contains an exception clause on the lines of the limitation clauses in Article 8 – 11 of the ECHR, i.e., limitations that are provided by "law", serve a major legitimate public interest and are necessary and proportionate to the relevant interest. The zero draft also reportedly includes a clause requiring appropriate procedural safeguards and remedies.

Conclusion 13:

As noted earlier, when it is not possible to provide an AI subject with sufficient information to effectively challenge any AI system-based decision affecting that individual's rights or interests, the decision will be incompatible with the right to an effective remedy. This follows from the PNR Judgment of the CJEU and is likely to be followed by the European Court of Human Rights as well. Therefore, the final text of the AI Convention should reflect this conclusion and never allow unexplainable - and hence unchallengeable – AI systems, not even under the exception clauses.

4.3 Practical implications of conditions placed on "high risk" AI systems (and explainable and challengeable AI systems)

At 3.1, I noted that the draft AI Act imposes on "high risk" AI systems a range of strict conditions, 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.;[88] and in the subsequent sections and lists of implications I have stressed that when such systems are used in EU contexts not subject to the AI Act, those same strict conditions must still be imposed (because the Court of Justice derived them directly from the Charter).

The proposed CoE AI Convention will reportedly point to the need for similar restrictions and safeguards, *ex ante*, during deployment and *ex post*, and for transparency, explainability and challengeability.

These requirements of the new instruments have **significant practical implications** in relation to the use of explainable and challengeable AI systems that are nonetheless still categorised as "high risk" AI systems.

Conclusion 14:

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 "commercial confidentiality" or "national security".

The above applies a fortiori to any claim by any developer that they offer any AI system that need not be considered "unacceptable" (and thus banned) because, different from other (currently typical) AI systems, their system is transparent, and its outputs are explainable and can be effectively challenged. For now, such systems appear to be elusive.

Douwe Korff, Cambridge (UK), October 2022

[88] For details, see Edwards, The EU AI Act (footnote 6, above), pp. 16 – 23.

ANNEX. List of Conclusions

Conclusion 1:

It is clear from the PNR judgment of the CJEU that the use of opaque, i.e., unexplainable and hence unchallengeable AI systems is inherently incompatible with the Charter. In particular, the use of systems with such characteristics violates the very essence of the right to an effective remedy - and current machine-learning based AI systems (ML/AI systems) typically have those characteristics. This has broad and significant implications generally (not just in relation to PNR data screening).

Conclusion 2:

The use of all AI systems must still be subject to strict conditions based on their level of risk and, must make it possible to monitor and review the outputs and outcomes[89] of those systems, especially in order to ensure that they do not generate discriminatory outputs or result in discriminatory outcomes, and to assess the numbers and percentages of false positives and false negatives.

Conclusion 3:

The application of the in-principle prohibition of fully automated decision-making in the General Data Protection Regulation (GDPR) and in the regulation laying down the data protection obligations for the EU institutions, bodies and agencies (Regulation (EU) 2018/1725) – as well as the restrictions on the use of such systems in the Law Enforcement Directive (LED) and the Europol Regulation (and any other rules in the Area of Freedom, Security and Justice) – should be aligned with the AI Act and the PNR judgment of the CJEU.

The European Data Protection Board and the European Data Protection Supervisor should issue opinions (or preferably a joint opinion) on the use of AI systems in processing of personal data subject to these instruments, in which they clarify 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 thus never allowed under either the GDPR or Regulation 2018/1725 or the LED or the Europol Regulation (or any other rules in the Area of Freedom, Security and Justice).

[89] On the conceptual difference between outputs and outcomes, see my earlier opinion, section 4.9(f), sub-section (fe), at Ii, *built-in biases*, and more specifically the quote from a University of Delft/EDRi report on pp. 89 – 90. Basically, outputs are the results generated by IT systems, whereas outcomes are the consequences of the application of those outputs (often by humans [over-]relying on the outputs).

Pending such an opinion, companies and public bodies should already refrain from using unexplainable and unchallengeable AI systems in any processing of personal data that is subject to the GDPR or Regulation 2018/1725 or the LED, and they should only use (and be allowed to use) AI systems if they comply with those strict conditions. Otherwise, they will be in breach of Article 22 GDPR, Article 24 of Regulation 2018/1725 or Article 11 LED (whichever is the applicable instrument). The same should apply *mutatis mutandis* to Europol, Frontex, and any other EU agency operating in the Area of Freedom, Security and Justice.

Conclusion 4:

Whatever one may think of the approach adopted for both the AI Act and the proposed AI Convention (and it can be criticised),[90] the drafters of the instruments – and the legislators if the proposals are adopted – clearly feel that some AI systems by their very nature, by the predictable negative effects they will have, are "unacceptable" or pose "high risks" to the fundamental rights and freedoms of individuals – and must therefore be banned (or at least suspended) or made subject to very strict regulatory and oversight requirements.

Moreover, it follows from the PNR judgment of the CJEU, discussed above, that the category of "unacceptable" AI systems must be regarded as including the use of unexplainable and unchallengeable, self-modifying AI systems in any decision that significantly affects individuals.

Conclusion 5:

It follows from the PNR judgment of the CJEU that even when Member States hold exclusive competence in some areas (such as, in particular, national security), if the exercise of that competence affects an area where the EU has competence and that is covered by EU law (e.g., data protection, internal market), the exercise of that exclusive Member State competence may not impinge on the EU legal order or undermine the relevant EU legal rules.

Therefore, whenever an EU Member State exercises its exclusive competence in relation to national security to impose obligations on entities that are subject to EU law in their relevant activities, whether these are those telecommunication service providers, airlines, or providers or users of AI – those obligations must be compatible with the relevant EU law such as the GDPR, the LED, or the Europol Regulation (all read in line with the PNR judgment). This compatibility also needs to extend to future regulation such as the AI Act (also read in that way), and more generally with the EU Charter of Fundamental Rights– and the Court of Justice is competent to assess that compatibility.

[90] See footnote 27, above.

Conclusion 6:

Any EU rules covering the links 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. In the present case, of the AI Act, this includes the ban on unexplainable and unchallengeable AI systems (because of the PNR judgment).

Specifically, those rules should ensure that the exchanges of personal data between entities governed by EU law (including Europol, Frontex, EU missions, law enforcement agencies of EU Member States) and the national security agencies of the EU Member States do not result in making decisions that significantly affect the rights of individuals protected by the Charter on the basis of the use of unexplainable and unchallengeable AI systems.

Conclusion 7:

Unexplainable and unchallengeable AI systems should not be researched, developed or used in any area of EU competence, i.e., not in the internal market (as will be clear if the AI Act and the GDPR are applied in accordance with the PNR judgment), but also not by Europol or any other EU agency or Member State entity active in the Area of Freedom, Security and Justice.

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 the taking of any decision that significantly affects the fundamental rights of individuals is incompatible with the Charter and therefore also with each and every one of those instruments. *Consequently*:

(i) The application of the Europol Regulation should be expressly aligned with the AI Act (just as it is supposedly already aligned with the GDPR and the LED) and in any processing of personal data that is subject to the Europol Regulation, Europol should not use unexplainable and unchallengeable AI systems;

(ii) All EU legal instruments and policies relating to police cooperation between the EU Member States and between the Member States and the EU (in particular Europol) should be reviewed and revised to reflect and respect the prohibition on the use of unexplainable and unchallengeable AI systems in relation to the taking of decisions that significantly affect the fundamental rights of individuals;

(iii) Member States' law enforcement agencies should, in any processing of personal data that is subject to EU law including the Law Enforcement Directive and the Charter, not use unexplainable and unchallengeable AI systems;

(iv) All EU legal instruments and policies relating to Frontex or other border control or other AFSJ matters should be reviewed and revised to reflect and respect the prohibition on the use of unexplainable and unchallengeable AI systems in relation to the taking of decisions that significantly affect the fundamental rights of individuals; and

(v) All EU Institutions should, in any processing of personal data that is subject to Regulation 2018/1725 (and the Charter), not use unexplainable and unchallengeable AI systems.

(vi) Moreover, none of the above entities should only be allowed to use non-ML-based AI systems unless they comply with the strict conditions set out above.

(vii) Pending the formal revisions of the instruments mentioned at (i) to (v) above, all EU research and development of AI systems – and *a fortiori* all already-in-place deployments of such systems – should be urgently reviewed in the light of the PNR judgment.

Conclusion 8:

There is no justification for the exemption in the AI Act relating to AI systems developed or used for military purposes (or dual purposes: see below) 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. Furthermore, 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.

Conclusion 9:

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 the taking of decisions that significantly affect the fundamental rights of individuals (especially any decisions on the use of force).

Pending the formal revisions of the CFSP and CSDP instruments mentioned above, all research and development of AI systems – and *a fortiori* all already-in-place deployments of such systems – used in these contexts, too, should be urgently reviewed in the light of the PNR judgment of the CJEU.

Conclusion 10:

Rather than exempting whole ranges of “arrangements” and “agreements” with foreign countries and partners from the protections of individuals that must be granted to them under the Charter, no such “arrangements” and “agreements” should ever be entered into or adopted if they do not respect, or lead to violations of, the rights and freedoms of individuals under the Charter. For example: such links and data exchanges should never lead to the torture or unlawful killing of anyone, or to *refoulement* of refugees.

If there are previously-agreed “arrangements” or previously-adopted “agreements” in place that do not meet the requirements of the Charter – or even expressly allow for actions that violate the Charter – then those “arrangements” and “agreements” must be urgently suspended, reviewed and revised to bring them into line with the Charter.

This applies *a fortiori* to links with third country national security agencies such as the US National Security Agency (NSA) and the UK agencies MI5 and MI6 – to which, as the Court of Justice has expressly clarified, the Article 4 TFEU exemption does not apply.

This also applies when the Court of Justice clarifies what is and what is not compatible with the Charter – as the Court has done in relation to the use of AI systems in its PNR judgment. Specifically:

The links and data exchanges between EU institutions (including Europol and Frontex), EU missions, law enforcement agencies of EU Member States when operating subject to EU law, on the one hand, and third countries and international organisations on the other hand, should not result in the taking of decisions that significantly affect the rights of individuals protected by the Charter on the basis of unexplainable and unchallengeable AI systems.

The EU should also provide input into AI policy and standard-setting debates in international organisations including the UN and UNESCO, the OECD, the Council of Europe and NATO, to push for the adoption by those organisations of prohibitions on unexplainable and unchallengeable AI systems in all contexts.

This is especially important in relation to the use of AI for military purposes, as noted above. The EU should involve itself in the debates on the use of military AI, including the use of AI systems in drone strikes, fully in line with the Charter and IHL (which, like the ECHR and IHL, are effectively congruent) and the case-law of the Court of Justice.

Conclusion 11:

The exceptions to the prohibition of the use of ‘real-time’ remote biometric identification systems (as distinct from authentication systems) in publicly accessible spaces for the purpose of law enforcement in the AI Act should be scrapped altogether: all uses of RBI (whether real-time or post) in publicly- accessible spaces should be included in the prohibition, as they do not meet existing EU fundamental rights standards.

Conclusion 12:

“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.

The proposed exemption from the AI Convention for AI systems used for national defence purposes, if accepted as necessary to comply with Article 1(d) of the Statute, 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.

Conclusion 13:

As noted earlier, when it is not possible to provide an AI subject with sufficient information to effectively challenge any AI system based decision affecting that individual’s rights or interests, the decision will be incompatible with the right to an effective remedy. This follows from the PNR Judgment of the CJEU and is likely to be followed by the European Court of Human Rights as well. Therefore, the final text of the AI Convention should reflect this conclusion and never allow unexplainable - and hence unchallengeable – AI systems, not even under the exception clauses.

Conclusion 14:

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 “commercial confidentiality” or “national security”.

The above applies *a fortiori* to any claim by any developer that they offer any AI system that need not be considered “unacceptable” (and thus banned) because, different from other (currently typical) AI systems, their system is transparent, and its outputs are explainable and can be effectively challenged. For now, such systems appear to be elusive.

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