European Center for
Not-for-Profit Law

info@ecnl.org
0031 639029805
www.ecnl.org
@enablingNGOLaw

Artificial Intelligence Act Amendments

Scope of the EU Artificial Intelligence Act (AIA): Military Purposes and National Security

This document introduces a proposed amendment to Article 2 of the draft AIA (Scope) in order to clarify the actual scope of the regulation and ensure it adequately covers the placing on the market, putting into service and use of AI systems in the Union according to Union values, fundamental rights and principles.[1]

What does the scope of the AIA proposal currently not cover?

The EU Commission proposal (Article 2) delimits the scope of application of the AIA and establishes, *inter alia*, that,

"This Regulation shall not apply to AI systems developed or used exclusively for military purposes." (Article 2, para 3).

The compromise text adopted by the Slovenian Presidency of the Council of the EU further narrows down the scope of application of the AIA, namely to exclude from its coverage:

- *3. AI systems developed or used exclusively for military* ***or national security*** *purposes;*
- ***6. AI systems, including their output, specifically developed and put into service for the sole purpose of scientific research and development;***
- ***7. Any research and development activity regarding AI systems in so far as such activity does not lead to or entail placing an AI system on the market or putting it into service.***

[1] Highlights are our own for emphasis.

What does the definition "military purposes" actually mean in the context of AI regulation?

In the context and for the purposes of the AIA, it is unclear what "military purposes" consist of exactly: in Recital (12) of the proposal, the Commission explains 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)." However, there is no such mention or definition of "*military purposes*" in the Common Foreign and Security Policy (CFSP) provisions of the TEU, which only refer to competence related to:

- *decisions having military or defence implications* (Article 31, para 4,TEU));
- *operations having military or defence implications* (Article 41, para 2, TEU;)
- *military assets* (Article 42, para 1, 3, 6, TEU);
- *military means* (Article 43, para 1, TEU);
- *military advice* (Article 43, para 1, TEU);
- *military aspects of [...] tasks* (Article 43, para 2,TEU);
- *military capability objectives* (Article 45, par 1(a),TEU);
- *military capabilities* (Articles 45, para 1 (c); 46, para 1,TEU);
- *military expenditures* (Article 45, para 1(e),TEU);
- *military implications or those in the area of defence* (Article 48, para 7,TEU).

The use of "or" between "military" and "defence" implications seems to infer that military implications can be different from those of (national or international) defence.

The compromise text of the Slovenian Presidency of the EU Council offers a rationale for the exclusion of "military purposes" where it states that, "***Such exclusion is justified by the specificities of the Member States' and the common Union defence policy subject to public international law, which is therefore the more appropriate legal framework for the regulation of AI systems in the context of the use of lethal force and other AI systems in the context of military activities.*** *Nonetheless,* ***if an AI system developed exclusively for military purposes is used outside those purposes, such system would fall within the scope of this Regulation.***"

Therefore, the compromise text appears to define "military purposes" alternatively as:

- military activities carried out under the Member States' defence policy;
- military activities carried out under the common Union defence policy; or

- activities entailing the use of lethal force under the above-mentioned defence policies.

However, the justification offered by the Slovenian Presidency's compromise text does not provide accurate guidance for the application of the exemption in the AI Act: for example, it remains unclear:

- whether AI systems developed by private actors under their own initiative (that is, without prior public procurement) in order to be marketed to Member States exclusively for "military purposes" would be covered by the AI Act provisions or not;
- if the military activities undertaken for national or international defence purposes – and therefore excluded by the AI Act – would also extend to other actions not requiring the use of lethal force, such as peace-keeping, conflict prevention, strengthening international security, combat forces in crisis management, post-conflict stabilisation, or supporting third countries in combating terrorism in their territories.

Indeed, Section 2 of Title V of the TEU (Articles 42-46) – which focuses specifically on the EU Common Security and Defence Policy (CSDP) as "*an integral part of the common foreign and security policy*" – establishes that (Article 42, para 1):

- The CSDP "*shall provide the Union with an operational capacity drawing on civilian and military assets*";
- The EU may use such assets (i.e., either civilian or military assets) for "*missions outside the Union for peace-keeping, conflict prevention and strengthening international security in accordance with the principles of the United Nations Charter*" (Article 42, para 1, TEU)

Article 43, para 1, TEU, clarifies that:

1. *The tasks referred to in Article 42, para 1*, [i.e., missions outside the Union for peace-keeping, conflict prevention and strengthening international security] *in the course of which the Union may use civilian and military means, shall include joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, tasks of combat forces in crisis management, including peace-making and post-conflict stabilisation. All these tasks may contribute to the fight against terrorism, including by supporting third countries in combating terrorism in their territories.*
2. *"The Council shall adopt decisions relating to the tasks referred to in paragraph 1, defining their objectives and scope and the general conditions for their implementation. The High Representative of the Union for Foreign Affairs and Security Policy, acting under the authority of the Council and in close and*

constant contact with the Political and Security Committee, shall ensure coordination of the civilian and military aspects of such tasks."

Question/Example 1: if a military force uses a Remote Biometric Identification (RBI) system (including with emotion recognition functionality) in the context of a peace-keeping operation, a conflict prevention mission or a humanitarian mission, is that a "military purpose" and therefore falling outside the remit of the AI Act and under the exclusive competence of the Council?

Question/Example 2: if an AI-driven RBI system (with emotion recognition functionality) is used by a "civilian asset" but still in the context of a CSFP/CSDP operation, does this fall within the scope of the AIA because the AIA only excludes AI systems used or developed exclusively for "military purposes"? Or is it also excluded from the AIA application – even if not explicitly mentioned - because it falls under the exclusive remit of the Common Foreign and Security Policy (Article 43, para 1, TEU)?

What is the rationale for exempting "national security purposes" from the AIA?

The rationale given by the above-mentioned compromise text of the Council of the EU for excluding AI systems developed or used exclusively for national security purposes from the scope of the AIA is that "*national security remains the sole responsibility of Member States in accordance with Article 4(2) TEU.*"

However, it is worth reminding that the Court of Justice of the European Union (CJEU), in its Grand Chamber Judgment in La Quadrature du Net (LQDN) and Others has significantly limited that exemption, clarifying 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.*" (para 99).[2]

[2] Also see: Douwe Korff & Ian Brown, Exchanges of personal data after the Schrems II judgment, study carried at the request of the European Parliament's Civil Liberties (LIBE) Committee into the future of EU – US flows of personal data, July 2021, available at:https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

In the same Judgment, the CJEU also for the first time gives a definition of "national security", clarifying that, "*That responsibility [...] 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.*" (para 135). However, as stated by the Commission itself, the AIA proposal is structured around four different overarching objectives:

1. ensuring that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;
2. ensuring legal certainty to facilitate investment and innovation in AI;
3. enhancing governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
4. facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

In other words: the purpose of the AIA is *not* to regulate national security policies – whose sole responsibility remains with EU Member States and who can shape such policies as they please – but to ensure a harmonised horizontal legal framework with minimum common rules and safeguards for the placing on the market, putting into service and use of AI systems. The requirements in the AIA are very basic and mostly ensure that the systems are accurate, robust, secure, and function according to their specification. A fragmented market excluding some sectors from such framework regulation would not only cause legal uncertainty but also undermine trustworthiness, discourage innovation and risk deploying unreliable and un-secure AI systems in extremely sensitive, high-stakes contexts.

It is also worth reminding that the 2014 Opinion on surveillance of electronic communications for intelligence and national security purposes of Article 29 Data Protection Working Party states, "*Another part of the question that needs to be answered is to what extent an exemption focused on national security continues to reflect reality, now it appears the work of the intelligence services is more than ever before intertwined with the work of law enforcement authorities and pursues several different purposes.*" This is a line of reasoning that easily applies to the research, deployment and use of AI systems too, especially since "law enforcement" is indisputably acknowledged in the AIA as one of the areas where "high-risk" AI systems are listed (Annex III) . In the context of developing technology, there is no clear line between law enforcement and national security. [3] Arguably, the line is not very clear

[3] With the regard to the lack of a clear line between law enforcement and national security and the argument that intelligence service agencies could also be seen as a public authority competent for "the safeguarding against threats to public security – which is the definition of law enforcement authority" proposed by Article 3(40) of the AIA, also see Smuha, Nathalie A. and Ahmed-Rengers, Emma and Harkens, Adam and Li, Wenlong and MacLaren, James and Piselli, Riccardo and Yeung, Karen, How the EU

legally either.[4] AI developers will not distinguish between an AI-based system to be used in an investigation related to an organised drug crime or a bomb threat.

Example:

NSO Group's Pegasus spyware is a perfect example of technology nominally referred to as "*developed or used exclusively for national security purposes*". However, the practice has demonstrated how this technology was also used allegedly for "law enforcement" purposes and abused even in those circumstances, resulting in human rights violations around the world on a massive scale.[5]

Therefore, it is practically and legally impossible to define *ex ante* any technology "*developed or used exclusively for national security purposes*". As noted above, the AI Act aims to ensure a harmonised horizontal legal framework with minimum common rules and safeguards. These rules and safeguards should be applicable to AI systems that can potentially be used for national security purposes.

Furthermore, the exclusive competence of Member States on national security has to be read in context with their shared competence with the EU on the areas of "*freedom, security and justice*", which allows the EU to regulate issues pertaining to security within the EU territory. We recall, in this sense:

- the European Council's The Hague Programme (2005 – 2009), which called on Member States "*not to confine their activities to maintaining their own security, but to focus also on the security of the Union as a whole*";
- the European Council's Stockholm Programme (2010 – 2014), which called for the establishment of an Internal Security Strategy based, inter alia, on a "*horizontal and cross-cutting approach" since "the enhancement of actions at European level, combined with better coordination with actions at regional and national level, are essential to protection from trans-national threats.*"

Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act – p. 19 (August 5, 2021).

[4] See, e.g., overlaps in EU Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. In addition, the European Data Protection Supervisor in his Preliminary Remarks on Modern Spyware summarises the overlaps and applicability of EU law (as well as the European Convention on Human Rights) in the context of technology tools that are supposed to be used for the detection, prevention and prosecution of terrorism and serious crimes.

[5] See EDRi/EIJI, The Rise and Rise of Biometrics Mass Surveillance in the EU, Chapter 4 – Pegasus Spyware.

What would be the consequences of excluding AI for "national security purposes" from the AIA?

Intrusive AI-based technologies – including with mass surveillance outcomes – could be used in the public sector with no special limitations or safeguards whenever "national security" grounds are invoked by a Member State. Even those AI systems presenting "unacceptable" levels of risks and therefore prohibited by the AIA could be easily "resuscitated" or "recycled" for the exclusive purpose of national security (e.g., 'real-time' RBI systems in publicly accessible spaces used for the prevention of a specific, substantial and imminent threat of a terrorist attack, Article 5, para 1(d) (ii) or other exception which, as the European Data Protection Supervisor (EDPS) and Board (EDPB) warn, constitutes such a wide set of exceptions that "*even with the foreseen limitations, the potential number of suspects or perpetrators of crimes will almost always be "high enough" to justify the continuous use of AI systems for suspect detection, despite the further conditions in Article 5(2) to (4) of the Proposal.*").

Proposed Amendment

We propose to replace the definition "military purposes" in Article 2 with a reference to the actual language in the TEU ("o*perations having military or defence implications*") and add a recital clarifying their scope. The recital already included by the Slovenian Presidency of the EU Council is a good starting point, which we propose to amend as follows:

Recital proposed by Slovenian Presidency of the EU Council	Our proposed amendment to the Recital (added words highlighted)
Such exclusion *[of AI systems used for military purposes]* ***is justified by the specificities of the Member States' and the common Union defence policy subject to public international law, which is therefore the more appropriate legal framework for the regulation of AI systems in the context of the use of lethal force and other AI systems in the context of military activities****. Nonetheless,* ***if an AI system developed exclusively for military purposes is used outside those purposes,***	***Such exclusion*** *[of AI systems used for military purposes]* ***is justified by the specificities of the Member States' and the common Union defence policy, which is subject to public international law, international humanitarian law and international human rights law (as reflected, for instance, in the NATO Principles of Responsible Use of Artificial Intelligence in Defence)[6], which is are therefore the more appropriate legal framework for the regulation of AI systems***

[6]NATO - Summary of the NATO Artificial Intelligence Strategy, 22-Oct.-2021

such system would fall within the scope of this Regulation.	***in the context of the use of lethal force and other AI systems in the context of military activities. Any action of Member States and/or the EU in the area of the EU Common Security and Defence Policy (CSDP) must fully comply with such principles of international law.*** *Nonetheless, if an AI system developed exclusively for military purposes is used outside those purposes, such system would fall within the scope of this Regulation.*

We also propose not to include "national security purposes" as a blanket exemption to the scope of the AI Act: the exemption of AI systems developed or deployed for national security reasons – including surveillance – should always be assessed on the basis of their strict necessity and proportionality and without prejudice to the application of Union law, including the EU Charter of Fundamental Rights:

Commission proposal	Council compromise text	Our proposed amendment
Article 2(3) This Regulation shall not apply to AI systems developed or used exclusively for military purposes.	Article 2(3) *This Regulation shall not apply to AI systems developed or used exclusively for military* ***or national security*** *purposes.*	Article 2(3) *This Regulation shall not apply to AI systems developed or used exclusively for* ***operations having military or defence implications carried out by military capabilities under the exclusive remit of the Common Foreign and Security Policy regulated under Title V of the Treaty on the European Union*** **(TEU).** ***Any exemptions from the application of this Act to AI systems used exclusively by***

		Member States for national security purposes will be without prejudice to the application of Union law to any activity carried out by the Union or by a Member State that is subject to Union law.

This paper was drafted by the European Center For Not-For-Profit Law (ECNL) and is also signed/endorsed by:

European Digital Rights (EDRi)

Access Now

AlgorithmWatch

ARTICLE 19

Electronic Frontier Finland (EFFI)

Electronic Privacy Information Center (EPIC)

Panoptykon Foundation