



## UvA-DARE (Digital Academic Repository)

### The AI Act National Security Exception

*room for manoeuvres?*

Vogiatzoglou, P.

**DOI**

[10.59704/292082becc7cc8e6](https://doi.org/10.59704/292082becc7cc8e6)

**Publication date**

2024

**Document Version**

Final published version

**License**

CC BY-SA

[Link to publication](#)

**Citation for published version (APA):**

Vogiatzoglou, P. (2024). The AI Act National Security Exception: room for manoeuvres?. Web publication or website, Verfassungsblog. <https://doi.org/10.59704/292082becc7cc8e6>

**General rights**

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

**Disclaimer/Complaints regulations**

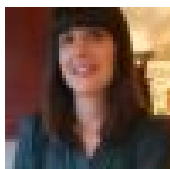
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

# The AI Act National Security Exception

---

**VB** [verfassungsblog.de/the-ai-act-national-security-exception/](https://verfassungsblog.de/the-ai-act-national-security-exception/)

9 December 2024



[Plixavra Vogiatzoglou](#)

This article belongs to the debate » [The EU AI Act's Impact on Security Law](#)

09 December 2024

## room for manoeuvres?

---

In 2024, the EU legislators adopted a detailed national security exception to the AI Act, contravening prior EU case law. Beyond the possibility of a future ruling that would realign the AI Act's scope with said case law, the impact of this exception might be limited by other applicable laws and the interpretative and practical difficulty of distinguishing between national and public security. The AI Act's failure to sufficiently account for these intricacies risks further legal uncertainty within the already complex security landscape. Therefore, this blog post explores the challenges of implementing the exception of national security to the AI Act's scope of application.

## The political background

---

In the final stages of the triilogue negotiations, [Article 2\(3\) of the AI Act](#) was established to exclude from its scope "AI systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities." The provision further clarifies that it shall not affect national competences in that field, as also stipulated in [Article 4\(2\) of the Treaty on European Union](#).

This provision is the latest chapter in the long history of Member States demarcating their hands-off zone and the Court of Justice of the EU (CJEU) responding with numerous conditions to national security invocations. The CJEU has long held that any derogation from EU law on the basis of security must be strictly interpreted (see, e.g. [Commission v Poland](#), paras 143-147). In the famous [La Quadrature du Net \(LQdN\)](#) ruling of 2020, the Court further clarified that the national security exception applies solely to purely governmental practices, that is, without engaging any private actor (paras 102-104). Where national measures impose obligations upon the private sector in a field touching upon EU law, then the EU rules are applicable, and the national measures pursuing the safeguarding of national security through private sector involvement are subject to CJEU scrutiny.

In response, Member States first sought to introduce this broad national security exception, encompassing both public *and* private actors, in 2021, in the proposed ePrivacy Regulation ([Council of Europe, art 2\(a\)](#)), whose fate remains uncertain. Instead, the almost verbatim and controversial provision is now adopted in the AI Act. By disregarding the distinction made by the Court in LQdN between purely governmental action and activities involving private parties, this provision – arguably – goes against the CJEU jurisprudence, which is part of [EU primary law](#), thus overriding the AI Act. Civil society organisations, such as the [European Center for Not-for-Profit Law \(2024\)](#), the [European Disability Forum \(2024\)](#), and the [Center for Technology and Democracy \(2024\)](#), have heavily criticised the AI Act exception for national security activities. It is feared that governments and security authorities might abuse this exception and invoke it to deploy AI systems that interfere with human rights even beyond the strict confines of national security situations, for example, in the field of border management. The lack of a common definition of national security across Member states amplifies this concern. Furthermore, distinguishing it from the wider domain of public security has proven a gargantuan task.

## Defining and distinguishing national security

---

The aforementioned [LQdN ruling](#) also provided for an EU-wide definition of national security. According to this definition, it relates “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*” (para 135, emphasis added).

However, public security has been similarly defined within EU case law and secondary law. For example, as explained in Recital 19 of the [Regulation on the free flow of non-personal data](#), public security “presupposes the existence of a genuine and sufficiently serious threat affecting one of the *fundamental interests of society*, such as a threat to the functioning of institutions and *essential public services and the survival of the population*, as well as the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests” (see also [Tsakouridis, para 44](#), emphasis added). Besides, threats such as terrorism and cyberattacks are subject to and regulated under EU law, although they might touch upon both national and public security.

In the CJEU’s view, a threat to national security is nevertheless distinguishable “by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious offences being committed” ([LQdN, paras 136-137](#)). In other words, whereas the nature of national and public security may be similarly defined by reference to the same interests and types of threats, a threat to national security is severe and present or foreseeable, whereas a threat to public security is general and permanent. This temporal distinction is certainly not as straightforward, nor can it be easily translated into specific timeframes,

after which a threat becomes a matter of public security. Such a transition from foreseeable to general threats can certainly not be implemented ex-ante when producing and placing an AI system in the market. Additionally, it has long been acknowledged how national security authorities increasingly collaborate with law enforcement and other public and private bodies, blurring the lines between national and public security not only in terms of the rhetoric and definitions but also at the institutional level (see [Vogiatzoglou, 2024](#), chapters 2, 3 and 6).

## EU and international law as a safety net?

---

The AI Act does not apply in a vacuum but complements existing EU law, including EU data protection law, which provides the general framework for personal data processing activities ([CNIL 2024](#)). Therefore, only AI systems that do *not* process personal data or that process personal data of data subjects *outside of the EU* escape the EU data protection legislation (see also [Data Guidance 2023](#)). While both the [General Data Protection Regulation](#) and the [Law Enforcement Directive](#) similarly exclude national security activities from their scope, this exclusion is limited by the aforementioned CJEU jurisprudence, which remains pertinent to data processing activities even under the AI Act (see [European Data Protection Board, 2021](#), in relation to the proposed ePrivacy Regulation). In other words, personal data processing activities for the purpose of national security are exempted only insofar as they relate to purely governmental authorities. If the processing operations implicate entities subject to EU law, for example, because the personal data were initially collected by private sector actors, like internet service providers, or other public bodies such as law enforcement authorities, then EU data protection legislation applies. It follows that those AI systems must still abide by not only EU data protection laws but also the [Charter of Fundamental Rights of the EU](#).

The national political will to carve out a wider free-range for states acting in pursuit of safeguarding their national security also found its way to the Council of Europe [Framework Convention on AI](#) (art 3(1)). This expansion is particularly challenging to justify, as the European Convention on Human Rights (ECHR) does not exclude national security from its scope. To counterbalance this exception, the Convention reminds contracting parties of their international obligations to protect human rights, democracy, and the rule of law. The [explanatory report](#) contextualises this provision by referring to numerous such international obligations, including the ECHR and the United Nations International Covenant on Civil and Political Rights (para 32). Since all EU Member States are subject to these obligations, they will remain liable if they make use of AI systems that violate human rights, the rule of law, or other democratic processes.

## In practice

---

AI systems are not subject to the AI Act when put in the EU market or service *exclusively* for military, defence, or national security purposes. However, if the same AI system is also used for law enforcement and public security purposes, then it must abide by the AI provisions (see also Recital 24 AI Act). National security agencies may lack the funds and

capacity to develop such systems without the industry's help (see Powell, 2024, [here](#) and [here](#)). Similarly, [Greene \(2024\)](#) explains how the development of useful AI typically starts with commercial providers and then makes its way into military systems.

In essence, this means that developers of AI systems external to military, defence and national security agencies who supply AI systems for both public and national security uses will have to develop at least two different types of systems: one compliant with the AI Act and one that is not. Additionally, as discussed above, if the system relies upon personal data implicating private sector actors subject to EU law, it must still abide by data protection and human rights laws, regardless of the AI Act exception. Moreover, several EU research schemes foresee the investment of large funds towards security-oriented research. Among others, EU-funded security research comprises civil security, which includes, for example, terrorism and cybersecurity, and the Common Security and Defence Policy. AI systems developed through these security research funding schemes must equally abide by EU law (see European Commission [Innovation and Security research](#) and [European Defense Fund](#)). Excluding the applicability of the AI Act fragments the market and creates practical difficulties for security AI system developers.

## Conclusion

---

The tag war between Member States and national security authorities, on one side, and the judiciary, civil society, and human rights bodies, on the other, might not be over just yet. Until a case is brought before the Court, the European Commission and national authorities are responsible for overseeing the strict application of the AI Act's national security exception. In that regard, approaches at the domestic level might differ significantly. The [Pegasus spyware scandal](#), amongst others, has set a bad precedent of a broadly encroaching national security invocation to circumvent EU oversight and (arguably) democratic processes and human rights obligations.

As with any law, the interpretation of the AI Act's national security exception will depend on the political will of those responsible for interpreting it. Some Member States might be eager to expand the protective veil of national security upon other situations of public security or even border management. Yet, without own-developed and completely standalone deployment of AI systems not involving other public or private actors, it will come down to the industry's decisions to develop separate AI systems purely for national security purposes for the EU market. In other words, as with the AI Act compliance at large, effectively, it is up to the providers, and it is them we will need to keep our eyes on. Ultimately, the AI Act's national security exception might serve more as a power play rather than be implemented in practice.

In this way, investing in AI systems solely for national security purposes to circumvent compliance with the AI Act might simply not prove profitable. Besides, the AI Act provides for very basic accuracy, robustness, transparency, and security requirements, with numerous exceptions for law enforcement (i.a. arts 27(3), 46(1), 49(4)). By excluding

national security from these regulations, the market becomes further fragmented, increasing legal uncertainty and undermining the trustworthiness and innovation of AI technologies at large (see also [European Center for Not-for-Profit Law, n.d.](#)).

---

# MAX PLANCK INSTITUTE

## FOR THE STUDY OF CRIME, SECURITY AND LAW



This article is part of VB Security and Crime: A Cooperation Project of Verfassungsblog and MPI-CSL

---

SUGGESTED CITATION Vogiatzoglou, Plixavra: *The AI Act National Security Exception: room for manoeuvres?*, *VerfBlog*, 2024/12/09, <https://verfassungsblog.de/the-ai-act-national-security-exception/>, DOI: [10.59704/292082becc7cc8e6](https://doi.org/10.59704/292082becc7cc8e6).

### One Comment

---

#### WRITE A COMMENT

1. We welcome your comments but you do so as our guest. Please note that we will exercise our property rights to make sure that Verfassungsblog remains a safe and attractive place for everyone. Your comment will not appear immediately but will be moderated by us. Just as with posts, we make a choice. That means not all submitted comments will be published.
  2. We expect comments to be matter-of-fact, on-topic and free of sarcasm, innuendo and ad personam arguments.
  3. Racist, sexist and otherwise discriminatory comments will not be published.
  4. Comments under pseudonym are allowed but a valid email address is obligatory. The use of more than one pseudonym is not allowed.
- 

Explore posts related to this:

---