Chapter 9

Legal Aspects of Military and Defence Applications of Artificial Intelligence Within the European Union

Marko Jurić

Abstract

This chapter aims to map the primary legal instruments relevant to governing the use of artificial intelligence (AI) for military and defence purposes in Europe. The analysis indicates that, while there is no lack of regulation, the legal framework itself should not pose insurmountable obstacles for the industry and entities operating within the military and defence sectors. This issue is particularly evident in the regulation of lethal autonomous weapons systems (LAWS). There are no binding EU rules on this matter in the European Union (EU); however, some European institutions are advocating for reasonable safeguards to enhance human control and accountability.

The drafters of the EU AI Act have made concerted efforts to exempt the military, defence, and national security sectors from its scope. However, this does not mean that all AI-related activities in these domains will escape scrutiny by the Court of Justice of the European Union (CJEU). As existing case law demonstrates, the Court has in various areas under the primary competence of Member States, including matters of national defence. Therefore, it is possible that a similar approach may be applied in AI-related cases.

Finally, the most significant challenges in developing and using AI in the military and defence domains may arise from rules governing data usage. This chapter demonstrates that the current EU laws apply within the military and defence sectors. The possibilities for excluding their application appear narrower than in AI Act, particularly given the CJEU's established case law. Combined with the broad concept

Marko Jurić (2024) 'Legal Aspects of Military and Defence Applications of Artificial Intelligence Within the European Union'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 395–433. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_9

of personal data, it is easy conceivable that personal data protection rules could substantially impact the capacity of national defence and military entities to process certain data.

Keywords: Artificial intelligence, AI, military AI, defence AI, personal data, AI Act

1. Introduction

Artificial intelligence (AI) has been one of the most discussed issues in recent years. Everyone talks about it, and many want to use it for different purposes. As Rickli and Mantellassi write, it is 'the defining technology of this generation'.[1] The term AI appears everywhere, from office software to social networks. However, while one might be a bit sceptical about whether everything which passes for it nowadays is "true" AI, there seems to be little doubt that it will have a substantial impact on society.

Like in other spheres of human activity, the potential uses of AI in the military and defence sectors seem almost unlimited. But as in other sectors, there is also considerable debate on the use of AI for military and defence purposes. While autonomous drones and other lethal weapons systems that act without or with limited human control rightly occupy the top of the list of our concerns, there are many more areas where AI can make a meaningful impact. For instance, the U.S. Department of Defence considers that AI 'is expected to impact every corner of the Department, spanning operations, training, sustainment, force protection, recruiting, healthcare, and many others'.[2]

However, the expected impact of AI use might also involve many security, safety, ethical, and legal concerns associated with its use.[3] These issues are currently addressed mostly through various principles and codes of conduct, which provide guidelines for the responsible development of AI. However, this was true only in the initial phases. As noted by Anand and Deng, 'only a handful of states and intergovernmental organisations have publicly adopted principles, standards or ethical frameworks tailored to AI applications in the defence sector'.[4]

When we turn from the principles and codes of conduct, which at best can be seen as "soft law", towards binding legal norms, the situation is even more uncertain because AI legislation is yet to be developed. For instance, the EU's Artificial Intelligence Act, supposed to be the world's first comprehensive regulation of AI, was

[1] Rickli and Mantellassi, 2023, p. 12.

[2] U.S. Department of Defense, 2019, p. 5.

[3] Anand and Deng, 2023, p. 6.

[4] Ibid.

enacted during the writing of this chapter. In other jurisdictions, AI regulation is even less developed.

The purpose of this chapter is to analyse how the EU legal framework addresses the use of AI for military and defence purposes. As noted above, many parts of the legislation are currently still in development; therefore, in many aspects, this is a forward-looking and speculative analysis. There are several reasons for this observation.

First, there seems to be ambiguity regarding the possible uses of AI in the military. While it is almost universally acknowledged that the possibilities are immense, when we look at how militaries are planning to use AI, the situation is less clear. For instance, most NATO Member States do not currently have a dedicated military AI strategy. Only a few states (see below) have formalised their strategic thinking regarding military and defence AI. As noted in NATO's 2021 AI Strategy, military AI is still in early development.[5] Therefore, as AI technologies and their uses develop over time, regulatory issues will become increasingly emphasised.

Second, legal regulations for AI are also being developed daily. To illustrate this point, multiple versions of EU regulations regarding AI have been made public during the preparation of this contribution. In addition, with the growing understanding that AI can affect different sectors and activities, it is clear that some aspects of its use can be covered by existing rules. In the European context, this is most prevalent in the rules regulating the use of data.

2. AI in military and defence: what are the regulatory issues?

In this chapter, we seek to broadly map areas in which AI is already, or could be, used for military and defence purposes. This will be the basis for the analysis of the applicable legal framework in section 3. However, at the outset, we are already faced with problems of definition. To identify what might be the uses of AI in these sectors, we first have to define AI. The problem here is that there are many definitions of AI, and depending on the definition, the same system can be seen as either AI or not.[6]

For instance, the 2018 U.S. Department of Defense AI strategy broadly defines AI as 'the ability of machines to perform tasks that normally require human intelligence'.[7] Specific examples include 'recognising patterns, learning from experience,

[5] Gray and Ertan, 2021, p. 6.

[6] This problem is also emphasized when discussing lethal autonomous weapons system. For instance, Tadeo and Blanchard (2021) analysed existing definitions of autonomous weapons systems and concluded that different countries and organisations focus on different elements, leading to different approaches in addressing legal and ethical problems posed by these systems, p. 12.

[7] U.S. Department of Defense, 2019, p. 5.

drawing conclusions, making predictions, or taking action – whether digitally or as the smart software behind autonomous physical systems'. Similarly, the United Kingdom (UK) 2022AI strategy sees AI as 'a family of general-purpose technologies, any of which may enable machines to perform tasks normally requiring human or biological intelligence, especially when the machines learn from data how to do those tasks'.[8] The 2019 French Ministry of Defence, AI strategy (see below) suggests AI processes are 'mechanisms of cognition and thought and use a combination of hardware and software to imitate them in order to assist or replace human activities'.[9]

The potential military and defence applications of these technologies seem almost unlimited, and many authors and organisations have attempted to provide some structure and classify the possible uses of AI for military and defence purposes according to certain criteria. At the most basic level, some policy documents differentiate between warfighting and other uses of AI in the military.[10] Rickli and Mantellassi consider that AI can serve as an analytical enabler (such as using AI for important data analysis), as a disruptor (using technologies such as deepfakes to produce and spread disinformation and otherwise disrupt institutions and processes), and as a force multiplier (using AI in weapon systems).[11] Gray and Ertan focus on technologies, categorising AI and autonomous systems into autonomous vehicles, autonomous air and missile systems, autonomous missiles, AI-enabled aircraft, data analytics, and logistics and personnel management.[12] Taddeo et al. differentiate between the uses of AI for sustainment and support,[13] non-kinetic adversarial uses (defensive and offensive cyber operations), and kinetic adversarial uses (decision-making leading to the use of force, LAWS, and supporting tactical decisions and personnel in combat).[14]

The aim of this chapter is to examine how the European legal framework might address the use of AI for military and defence purposes. Therefore, it is necessary to define the issues of using AI, which are important from a regulatory perspective. To do so, we briefly analyse the existing strategies covering AI in the military and defence sectors of NATO Member States.

The *NATO Artificial Intelligence Strategy* (NATO AI Strategy) was published in 2021.[15] There are plans to update this strategy to include issues such as generative AI.[16] The strategy calls for AI to be mainstreamed, ensuring that its development and use are undertaken responsibly, while at the same time safeguarding against threats

[8] UK Ministry of Defence, 2022.

[9] French Ministry of Defence, 2019, p. 3.

[10] Devitt et al., 2020, p. 4.

[11] Rickli and Mantellassi, 2023, p. 22.

[12] Gray and Ertan, 2021, pp. 19–21.

[13] Encompassing AI for system's robustness and resilience; to support back-office operations; to support logistics and operational planning; for situational awareness; for peacekeeping; for national contingency operations. Taddeo et al., 2023, p. 163.

[14] Taddeo et al., 2023, p. 163.

[15] NATO, 2021a.

[16] Gosselin-Malo, 2023.

from the malicious use of AI by state and non-state actors.[17] The first goal is defined based on the Principle of Responsible Use, which includes lawfulness, responsibility and accountability, explainability and traceability, reliability, governability, and bias mitigation.[18] Second, it is recognised that adversaries and non-state actors might interfere with allied AI programmes using manipulation or sabotage; hence, it is necessary to protect against such events. It is further recognised that AI can also impact critical infrastructure and civil capabilities and preparedness, creating potential vulnerabilities.[19] Finally, the threat of disinformation campaigns using AI has also been recognised.[20]

The 2019 *Artificial Intelligence in Support of Defence* (French AI strategy) references compliance with the laws of war, armed conflicts, and other indirectly relevant rules.[21] Notably, France considers that contrary to certain popular misconceptions, AI has a potential which, properly managed and controlled, will help the French armed forces to take better account of the fundamental principles of the law of armed conflict because it can help mitigate discrimination between combatants and non-combatants, apply the principle of proportionality, and guarantee that action is determined strictly by need.[22] Finally, an important part of the French strategy is data governance. France recognises that the development and use of AI systems is dependent on access to vast, reliable, and up-to-date datasets. In this context, the French strategy recognises the difference between personal and non-personal data, and specifically mentions compliance with the General Data Protection Regulation (GDPR).[23]

The UK published its *Defence Artificial Intelligence Strategy* in 2022.[24] The UK generally considers that ‘progress in AI must be achieved responsibly and safely according to democratic norms and the rule of law’.[25] It also emphasises the rule of international law, considering that it:

> provides a robust, principle-based framework for the regulation of weapons development and use, focusing on effects rather than the nature of any particular technology. It imposes positive obligations that take account of core principles – distinction, necessity, humanity and proportionality – and is the most appropriate way of regulating new means and methods of warfare.[26]

[17] NATO, 2021a, para 3.
[18] Ibid., para. 9.
[19] Ibid., para. 16.
[20] Ibid., para. 17.
[21] French Ministry of Defence, 2019, pp. 5–6.
[22] Ibid., p. 6.
[23] Ibid., pp. 12–13.
[24] UK Ministry of Defence, 2022.
[25] Ibid., p. 11.
[26] Ibid., p. 53.

Like France, the UK has expressed its commitment to work under the UN *Convention on Certain Conventional Weapons*.[27]

The European Union (EU) does not have a unified strategy for AI in its defence and military domains.[28] This is not surprising, considering the complex division of competences and interests between the EU and its Member States and various EU institutions. Consequently, it is hardly surprising that the EU's strategic thinking on the use of AI in the defence and military domains is not as coherent as NATO's and the national strategies mentioned above. However, this is not to say that it is impossible to discern some general positions of the EU in relation to the AI issues analysed in this report. However, as the overview below shows, it seems more appropriate to speak about the positions and policies of specific institutions in relation to specific AI issues than to say that there is a coherent and over-reaching strategy in this domain.

In 2018, the European Commission published a strategy, *Artificial Intelligence for Europe*, broadly outlining the state of development and policy aims in this area. This document called for many specific measures to boost the European EU's capacity for AI. An important aspect of this strategy is that the measures were designed to boost access to data, which is crucial for developing AI. From a legal perspective, AI is seen as being at least partially regulated by the existing rules at that time, primarily those covering personal data protection and the regulation of the flow of non-personal data. This calls for the development of appropriate ethical standards and criteria to ensure safety and liability. However, when it comes to the issue of AI in the defence and military domains, the 2018 strategy remains silent. The only mention of these issues is in relation to the work of international organisations, and it is mentioned that the use of AI in military domains is being discussed in these forums.[29]

In 2019, a team of AI experts established by the European Commission prepared a report on *Ethics Guidelines for Trustworthy AI*. In this report, the use of lethal autonomous weapon systems (LAWS) was highlighted as a critical concern. In this context, the Commission endorsed the position of the European Parliament and called for:

> the urgent development of a common, legally binding position addressing ethical and legal questions of human control, oversight, accountability and implementation

[27] Ibid., p. 53.

[28] Soare summarizes the current EU position as follows: 'Europeans lack a common AI integration strategy in defence which links technological power to strategic autonomy in terms of operational advantage against and competitiveness with other rival great powers. The EU does not have, nor does it currently plan to develop a common European military strategy to integrate AI in cyber and cross- domain military operations for operational and strategic advantage and it does not possess a common, regular threat and opportunity assessment based on European intelligence about its rivals' AI military innovation efforts and other international actors' geopolitical needs. The EU is not politically ready – or interested – to develop the kind of military capabilities, enablers, and legal powers to conduct algorithmic warfare'. Soare, 2023a, p. 78.

[29] European Commission, 2018.

> of international human rights law, international humanitarian law and military strategies.[30]

In 2020, the European Commission published a white paper, *On Artificial Intelligence – A European Approach to Excellence and Trust*.[31] This paper identified the key legal challenges to the deployment of AI, including compliance with fundamental rights and freedoms, risks to safety, and the functioning of the liability regime. Finally, it calls for establishment of a clear legal framework for the development and use of AI in the EU. However paper clearly states that 'it does not address the development and use of AI for military purposes'.[32]

The position of the European Parliament appears to differ. The parliament has addressed the issue of AI use in the defence and military sectors multiple times. Most of these interventions focus on the use of LAWS; however, some broader concerns and policy positions have also been articulated. In 2020, the parliament developed a framework to tackle the ethical aspects of AI, robotics, and related technologies.[33] This resolution elaborates on the positions of parliaments regarding the use of AI in the security and defence domains. In essence, the parliament maintained its earlier position regarding the use of LAWS without meaningful human control. Broader than that, it insists on respect for all applicable laws, including international humanitarian law, international human rights law, and EU law, in all situations where AI is used for defence purposes. However, the parliament also recognises the benefits of AI in the defence and military sectors, such as "higher quality collected data, greater situational awareness, increased speed for decision-making, reduced risk of collateral damage thanks to better cabling, protection of forces on the ground, as well as greater reliability of military equipment and hence reduced risk for humans and of human casualties".[34]

Interestingly, the use of AI in the defence and military sectors has attracted the attention of some EU Member States. For instance, during the Finnish presidency in 2019 Finland, Estonia, France, Germany, and the Netherlands published a food for thought paper on digitalization and artificial intelligence in defence.[35] In addition to seeking to open general discussions on disruption and transformation in defence and the impact of AI on military capabilities, this paper also addressed some regulatory issues. Generally, the paper seems to oppose a categorical ban on AI or autonomous systems and instead proposes that autonomous weapon systems be discussed and agreed upon internationally, specifically in the UN CCW forum.[36]

[30] European Commission, 2019.
[31] European Commission, 2020.
[32] European Commission, 2020, p. 1.
[33] European Parliament, 2020.
[34] European Parliament, 2020, para. 93.
[35] *Digitalization and Artificial Intelligence in Defence*, 2019.
[36] Ibid., p. 2.

In 2022, the EU adopted *A Strategic Compass for Security and Defence*, which outlines the EU's future security and defence agenda.[37] It calls for the development of capabilities in the land, maritime, air, space, and cyber domains. AI is viewed as a part of the cyber domain, and it is proposed that the EU will 'develop and make intensive use of new technologies, notably quantum computing, AI and Big Data, to achieve comparative advantages, including in terms of cyber responsive operations and information superiority'.[38] Moreover, it calls for stepping up efforts at the national and EU levels to better prepare for the future battlefield and next-generation technology.[39]

Finally, the issue of regulating AI in military, defence, and national security contexts became the subject of discussion in the drafting process of the EU AI Act.

3. The legal and regulatory landscape for the use of AI in European military and defence sectors

Some key global issues and challenges posed by AI in the defence and military sectors have been outlined above (and in other chapters of this book). We now consider the regulatory and legal landscape within which those issues and challenges must be addressed in the EU. Initially we can note that the EU appears to be recognised for its strict regulatory requirements. For instance, the French AI strategy describes the EU as:

> an aspiring intermediate power … whose hardline approach to legal and ethical issues may be a strength or a weakness depending on its impact (standard-setting power underpinned by many public- and private-sector actors vs risk of having a research or entrepreneurial development policy that is too timid or hampered by excessive regulation).[40]

Soare is even more direct when she argues that 'European states exhibit self-imposed ethical and legal restraints, bordering on cultural-technological conservatism, which inhibits an ambitious European agenda on adopting military AI'.[41]

In this section, we discuss legal issues, which might impact the use of AI in the military and defence.

[37] European Union External Action, 2022.

[38] Ibid., p. 45.

[39] Ibid., p. 48.

[40] French Ministry of Defence, 2019, p. 7.

[41] Soare, 2023b, p. 81.

3.1. Lethal autonomous weapons systems

One theme which features prominently in strategic documents and discussions on the use of AI in the military is the use of LAWS. There appears to be a consensus that these systems represent a particularly significant risk. However, there are different positions in terms of deployment and use. For instance, it is explicitly stated in the French strategy that France 'has no plans to develop fully autonomous systems where human operators have no control over the definition and performance of their missions', but at the same time it is against a preventive ban because it considers that such a ban "would hinder responses to legal and ethical challenges raised by them".[42] Other countries do not exclude the possibility of developing and using autonomous weapons systems with varying degrees of involvement.

Moreover, it appears that the most important part of the debate is the definition of LAWS. For instance, when Taddeo and Blanchard (2021) analysed the policies and documents of countries participating in discussions on LAWS in the UN Convention on Certain Weapons, they identified 12 definitions of LAWS.[43] Therefore, even if an international consensus on banning some fully autonomous systems emerges (which thus far seems unlikely), the issue of what constitutes such systems should first be resolved.

The EU law is understandably silent on the issue of LAWS. There is no EU law on the use of arms, and therefore no EU legal framework on the use of LAWS. However, some policy considerations have been expressed, most importantly by the European Parliament.

In 2014, the European Parliament passed a resolution on the use of armed drones, in which it, *inter alia*, called for a ban on the 'development, production, and use of fully autonomous weapons which enable strikes to be carried out without human intervention'.[44] This issue was addressed more comprehensively in 2018 in the resolution on autonomous weapon systems, in which the parliament called for 'a common position on LAWS that ensures meaningful human control over the critical functions of weapon systems, including during deployment, and to speak in relevant forums with one voice and act accordingly'.[45]

In 2019, the expert team on Artificial Intelligence established by the European Commission, stated in its *Ethics Guidelines for Trustworthy AI* that the development of LAWS 'could lead to an uncontrollable arms race on a historically unprecedented level and create military contexts in which human control is almost entirely relinquished, and the risks of malfunction are not addressed'.[46]

[42] French Ministry of Defence, 2019, pp. 8, 10.

[43] Taddeo and Blanchard, 2021, p. 7.

[44] European Parliament, 2014.

[45] European Parliament, 2018.

[46] European Commission, 2019, p. 34.

Finally, in 2020, the European Parliament passed a resolution on the issue of a framework for the ethical aspects of AI, robotics, and related technologies.[47] This resolution elaborates on the position of the parliament regarding the use of AI in the security and defence domains. In essence, the parliament maintains its earlier position regarding the use of LAWS without meaningful human control and calls for international regulation of the development and use of fully autonomous, semi-autonomous, and remotely operated LAWS. The position of the parliament is that development, production and use of LAWS enabling strikes to be carried out without meaningful human control and that systems without respect for the human-in-the-loop principle' should be prohibited. The crucial elements in the position of parliament are human control and accountability.

Regarding human control, the parliament states that human control must be present in all phases of the design, development, deployment, and use of AI systems.[48] In particular, it is necessary that '…humans retain the agency to detect and disengage or deactivate deployed systems should they move beyond the mission framework defined and assigned by a human commander, or should they engage in any escalatory or unintended action'.[49] Generally, the position of the parliament is that 'human control should remain effective for the command and control of AI-enabled systems, following the human-in-the-loop, human-on-the-loop and human-in-command principles at the military leadership level'.[50]

This is further extended by the need for accountability. In this context the parliament 'stresses the need to establish clear and traceable authorisation and accountability frameworks for the deployment of smart weapons and other AI-enabled systems'.[51] More specifically, it 'considers that AI-enabled systems, products and technology intended for military use should be equipped with a "black box" to record every data transaction carried out by the machine'.[52]

However, while the policy considerations of the European Parliament seem to be well developed and reasonable, the fact remains that they are not binding in any formal way. As explicitly confirmed in the EU's AI Act, the use of AI in the military context is determined by the specificities of the Member States' and the EU defence policies, which are subject to public international law.[53] Therefore, it recognises that international law is the appropriate legal framework for the regulation of AI systems in the context of the use of lethal force.[54]

[47] European Parliament, 2020.

[48] European Parliament, 2020, para. 102.

[49] European Parliament, 2020, para. 101.

[50] European Parliament, 2020, para. 102.

[51] Ibid.

[52] European Parliament, 2020, para. 101.

[53] AI Act, Recital 24.

[54] AI Act, Recital 24.

3.2. General regulation of AI

The EU is sometimes considered a global regulatory champion, and not without reason. Very high regulatory standards have been set in sectors such as personal data protection and the use of data in general, online content, and online platforms. The same applies to regulation of AI.

Following its 2020 White Paper on AI and many other policy papers and proposals issued by multiple EU institutions over the past several years, the European Commission prepared a draft for a comprehensive regulatory framework for AI. Hence, a proposal for a regulation laying down harmonised rules on AI, better known as the Artificial Intelligence Act, was published in April 2021 (2021 AI Act draft).[55] This document has been extensively debated and amended. For the purposes of the analysis in this chapter, it is important to consider the proposal which was prepared during the Slovenian presidency, in November 2021 (2021 AI Act compromise).[56] The latest publicly available official version was adopted by the European Parliament on 13 March 2024 (hereinafter, the AI Act).[57] While this version is yet to undergo a final legal and linguistic analysis and a formal endorsement by the Council of the EU, it can be expected that it will not undergo further significant changes. Therefore, we refer to the March 2024 version of the AI Act in this chapter.

The key question is, what might be the impact of the AI Act on the development and use of AI systems in the military and defence sectors? To address this question, it is necessary to consider the scope of the AI Act, which excludes most AI systems used in the military and defence, and the possible impact of the Act on the development of dual-use AI systems.

3.2.1. Situations where the AI Act does not apply

Based on the first draft of the AI Act in 2021 excluded certain systems used for military purposes from its scope. However, two subsequent publicly available texts show that the thinking behind this provision evolved and that the provision itself became both broader and more precise.

The 2021 draft provided in Article 2(3) that '[t]his Regulation shall not apply to AI systems developed or used exclusively for military purposes', which seems relatively clear but is, in effect, very limited. First, it should be noted that the 2021

[55] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence *(Artificial Intelligence Act)*, 2021. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf (Accessed: 5 February 2024).

[56] Ibid.

[57] *European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts*, 2021. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7536_2024_INIT (Accessed: 5 February 2024).

draft did not contain a provision regarding which legislative acts of the EU do not apply to an activity which falls outside the scope of EU law, which is otherwise ordinarily used in EU legislation. Secondly, it was declared that the AI Act would not apply to 'systems developed or used exclusively for military purposes', but there was no mention of defence purposes. Since one might argue that there are substantial differences between military and defence purposes, with the latter being broader, this exception could have indeed been limited. Finally, the scope of Article 2(3) was further elaborated on in Recital 12, where it was explained as follows:

> 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).

It would, therefore, follow that if Article 2(3) was interpreted in line with Recital 12, AI systems developed for military purposes would be excluded from the scope of the AI Act only under the condition that they were used for activities falling under the remit of the Common Foreign and Security Policy as regulated by the Treaty on the European Union (TEU). This would once again significantly limit the scope of exceptions because it would not cover national military activities which are not part of the CFSP.

In November 2021, during the Slovenian presidency, a compromise text was drafted that included substantial amendments to the scope of the AI Act. Most importantly, Article 2(3) was broadened to include national security, so that it read '[t]his Regulation shall not apply to AI systems developed or used exclusively for military or national security purposes'. Moreover, the relevant Recital was also amended to explain the following:

AI systems exclusively developed or used for military purposes should be excluded from the scope of this Regulation. Such exclusion is justified by the specifities 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. … When AI systems are exclusively developed or used for national security purposes, they should also be excluded from the scope of the Regulation, taking into account the fact that national security remains the sole responsibility of Member States in accordance with Article 4(2) TEU.

Finally, in the version of the AI Act adopted in March 2024, Article 2(3) regarding exclusions from the scope was also amended, and now reads as follows:

> This Regulation does not apply to areas outside the scope of Union law, and shall not, in any event, affect the competences of the Member States concerning national

security, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences.
This Regulation does not apply to 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.
This Regulation does not apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.

Moreover, Recital (24) was also changed and now reads as follows:

If and insofar AI systems are placed on the market, put into service, or used with or without modification of such systems for military, defence or national security purposes, those should be excluded from the scope of this Regulation regardless of which type of entity is carrying out those activities, such as whether it is a public or private entity. As regards military and defence purposes, such exclusion is justified both by Article 4(2) TEU and by the specificities of the Member States' and the common Union defence policy covered by Chapter 2 of Title V TEU that are 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 and defence activities. As regards national security purposes, the exclusion is justified both by the fact that national security remains the sole responsibility of Member States in accordance with Article 4(2) TEU and by the specific nature and operational needs of national security activities and specific national rules applicable to those activities. Nonetheless, if an AI system developed, placed on the market, put into service or used for military, defence or national security purposes is used outside those temporarily or permanently for other purposes, for example, civilian or humanitarian purposes, law enforcement or public security purposes, such a system would fall within the scope of this Regulation. In that case, the entity using the system for other than military, defence or national security purposes should ensure compliance of the system with this Regulation, unless the system is already compliant with this Regulation. AI systems placed on the market or put into service for an excluded purpose, namely military, defence or national security, and one or more non-excluded purposes, such as civilian purposes or law enforcement, fall within the scope of this Regulation and providers of those systems should ensure compliance with this Regulation. In those cases, the fact that an AI system may fall within the scope of this Regulation should not affect the possibility of entities carrying out national security, defence and military activities, regardless of the type of entity carrying out those activities, to use AI systems for national security, military and defence purposes, the use of which is excluded from the scope of this Regulation. An AI system placed on the market for civilian or law enforcement

> purposes which is used with or without modification for military, defence or national security purposes should not fall within the scope of this Regulation, regardless of the type of entity carrying out those activities.

Compared to the 2021 version, the 2024 Draft AI Act defines exemptions from the scope more broadly and precisely. Several important points should be noted. First, Article 2(3) now explicitly excludes AI-related activities in areas outside the scope of EU law from the scope of the Act. This is in line with other EU legal instruments in the fields of electronic communications, personal data, non-personal data analysed in this chapter. To further clarify, it is explicitly stipulated that AI systems which are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes are excluded from the scope of the AI Act. The same goes for AI systems which are not placed on the market or put into service in the EU, provided that the output is used exclusively for military, defence or national security purposes in the EU.

Second, the AI Act makes it explicit in Article 2(3) that exclusions from its scope apply regardless of the type of entity entrusted by the Member States to carry out the tasks in relation to those competences. This seems especially important for at least two reasons. First, developers of AI systems are usually private entities, so it is useful to clarify that when those entities are acting in national security, defence or military domains for the benefit of Member States, the exceptions still apply. Second, this solution also addresses the issues the CJEU had in some personal data protection cases (see a more extensive discussion below), when it concluded *inter alia* that the exception of national security does not apply when data processing is conducted by private entities (service providers) and not by the Member States themselves (or more precisely, by state bodies).

Considering the legislative history, explanations provided in the Recitals, and generally the efforts which went into drafting what is now Article 2(3), it seems clear that the drafters intended to ensure broad exemption for the use of AI systems in the national security, defence and military sectors. The main consequence of this approach is that the use of AI in those domains remains within the competence of Member States presumably outside the control of the CJEU. The first point seems uncontroversial since it is obvious that in those areas where the EU does not have competence and which are excluded from the scope of secondary EU laws, Member States can legislate freely. Therefore, starting from the premise that any limitations in the development and use of AI capabilities for defence and military sectors can be seen as a self-imposed restraint, it seems that EU law addresses this properly and essentially empowers Member States to decide for themselves.

However, the second and much more complicated question is: are the actions of Member States still under the control of the CJEU? Based on the approach previously pursued by the CJEU, it appears that the answer might be affirmative, at least in part. The CJEU has been explicit many times in cases regarding national security. For example:

> 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.[58]

Similarly, and specifically in the context of the armed forces, the CJEU concluded in *Sirdar v. The Army Board and Secretary of State for Defence* that:

> "decisions taken by Member States in regard to access to employment, vocational training and working conditions in the armed forces for the purpose of ensuring combat effectiveness do not fall altogether outside the scope of Community law".[59]

Moreover, in *Kreil v. Bundesrepublik Deutschland,* the CJEU used the same approach as in *Sirdar* ***v.*** *The Army Board and Secretary of State for Defence* concluded that while it is for Member States to make decisions on the organisation of their armed forces, this does not mean that such decisions fall entirely outside the scope of EU law *per se*.[60] Consequently, CJEU considered that it is competent to verify 'whether the measures taken by the national authorities in the exercise of their recognised discretion did, in fact, have the purpose of guaranteeing public security and whether they were appropriate and necessary to achieve that aim'.[61] Following its analysis, the CJEU concluded that EU law precluded national measures providing for the general exclusion of women from military posts involving the use of arms.

The same principles were also confirmed in the *Dory v. Bundesrepublik Deutschland*[62] case, where the CJEU repeated that it is competent to supervise the decisions of national authorities in the area of guaranteeing public security, but at the same time, confirmed that community law does not preclude compulsory military service being reserved for men. It appears that one of the reasons for such a conclusion (and different from the *Kreil v. Bundesrepublik Deutschland* case) was that there are no provisions governing 'the Member States' choices of military organisation for the defence of their territory or of their essential interests' in EU law, while (as in *Kreil v. Bundesrepublik Deutschland*) 'the principle of equal treatment of men and women in connection with employment, including access to military posts', is subject to EU law.

Finally, in the recent case of *B. K. v. Republika Slovenija* (2021), the CJEU was asked to answer several questions regarding the application of Directive 2003/88/EC concerning certain aspects of the working hours for an officer in the Slovenian army.

[58] C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and others v. Premier minister and Others*), para. 99, and cases cited there.

[59] C-273/97 (*Sirdar v. The Army Board and Secretary of State for Defence*), para. 21.

[60] C-285/98 (*Kreil v. Bundesrepublik Deutschland*)*,* para. 15.

[61] C-186/01 (*Dory v. Bundesrepublik Deutschland*), para. 34.

[62] Ibid.

Once again, it was argued that EU law does not apply to the military on the basis of Article 4(2) of the TEU, and once again, the CJEU concluded otherwise, stating that the provision in question does not exclude the working hours of military personnel from the scope of EU law.[63] According to the court, Article 4(2) of the TEU requires:

> application to military personnel of the rules of EU law relating to the organisation of working time is not such as to hinder the proper performance of those essential functions. Therefore, those rules cannot be interpreted in such a way as to prevent the armed forces from fulfilling their tasks and, consequently, so as adversely to affect the essential functions of the State, namely the preservation of its territorial integrity and the safeguarding of national security.

Thus, the CJEU set specific criteria for determining when the directive governing working hours for military personnel would be applied or excluded.

While the cases mentioned above are not directly related to the use of AI in the military or defence arenas, applying the same logic about competencies suggests that the CJEU might not accept that any use of AI in national security, defence or military sectors is excluded from its scope of its review. Hence, the real question is probably how active the court will be in setting the boundaries of the permissible use of AI in these sectors.

For instance, it seems reasonable to think that the use of LAWS should not be subject to any scrutiny by the court. However, what about other AI systems that might be used in the military or defence, such as personnel management, logistics, training optimisation, situational awareness, and threat analysis? Recital 24 specifically mentions AI systems in the context of the use of lethal force and other AI systems in the context of military and defence activities. Therefore, it appears that the legislative intent here was to create broad exceptions to the application of AI in the national security, defence, and military domains.

While fully accepting the principle that exceptions must be interpreted narrowly, it seems correct to also consider positions of the institutions involved in drafting the AI Act, which obviously intended for Member States to retain significant, if not full, discretion over the use of AI in defence and military sectors. The drafting process highlighted the difficulty of legislating in a rapidly changing technological environment like AI. A parallel can be drawn with the CJEU's handling of causes related to the surveillance of electronic communications metadata, where the Court initially set conditions for lawful retention but then had to clarify and refine its approach over numerous cases. For these reasons, it would be preferable to see the CJEU exercising its powers very cautiously when addressing the inevitable questions about the use of AI in military and defence domains.

[63] C-742/19 (*B.K. v. Republika Slovenija*), para. 46.

3.2.2. Situations where the AI Act applies

The AI Act is ambitious and seeks to promote elements of market regulation of AI while at the same time promoting 'human-centric and trustworthy artificial intelligence'[64] and protecting health, safety, fundamental rights, democracy, and the rule of law. Most importantly, the Act seeks to protect against the harmful effects of AI systems.[65] To what extent will all of this be achievable is yet to be seen, but there is no denying that the legislative aims are set high. In this chapter, we only briefly outline the main elements and approaches of the AI Act. The Act regulates the use of AI systems and subjects them to strict regulatory requirements.

3.2.2.1. AI systems

The definition of an AI system has changed significantly through legislative procedures. In the final version adopted by the Act, an AI system is defined as follows:

> A machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[66]

From the above definition, we see that the main characteristics of an AI system are that it is (1) machine-based, (2) has ability to infer, (3) autonomy, and possibly, but not necessarily, exhibits adaptiveness.

First, the AI system is machine-based, which pursuant to Recital 12, simply denotes the fact that AI systems run on machines. It will obviously include software, which was the term used in the 2021 AI Draft Act, provided that the requirements regarding autonomy and the ability to infer are satisfied. It appears that one of the reasons for removing the word "software" was to make it explicit that AI systems do not include 'simpler traditional software systems or programming approaches' or 'systems that are based on the rules defined solely by natural persons to automatically execute operations'.[67]

Secondly, and connected to the above, a key defining element of an AI system is its ability to infer, which is defined as 'the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments', as well as the 'capability of AI systems to derive models

[64] AI Act, Recital 1.
[65] AI Act, Article 1(1).
[66] AI Act, Article 3(1).
[67] AI Act, Recital 12.

or algorithms from inputs or data'.[68] Moreover, it is explained that the capacity of an AI system to infer:

> transcends basic data processing' and 'enables learning, reasoning or modelling'.[69] This can be achieved by techniques which 'include 'machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved.[70]

Third, AI systems operate with varying levels of autonomy. They have 'some degree of independence of actions from human involvement and of capabilities to operate without human intervention'.[71] Finally, AI systems may (but do not have to) exhibit adaptiveness, which refers to 'self-learning capabilities, allowing the system to change while in use'.[72]

The AI Act regulates three categories of AI systems: (1) those which encompass prohibited AI practices, (2) high-risk AI systems, and (3) other AI systems.

3.2.2.2. Prohibited AI systems

Prohibited AI systems are those which support manipulative, exploitative and social control practices.[73] They include (under certain conditions) AI systems which:

- Are manipulative, in the sense that they (a) seek to influence behaviour of a person or a group of persons, inducing them to take decisions they would not otherwise taken, and thereby causing them significant harm, or creating a likelihood of such harm, or (b) exploit any of the vulnerabilities due to age, disability of specific social or economic situation, leading to a distortion of behaviour causing them significant harm, or creating a likelihood of such harm.[74]
- Provide for social scoring of natural persons.[75]
- Are used for assessing or predicting the likelihood of a natural person committing a criminal offence.[76]
- Create of expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.[77]

[68] AI Act, Recital 12.
[69] Ibid.
[70] Ibid.
[71] Ibid.
[72] Ibid.
[73] Ibid., Recital 28.
[74] Ibid., Article 5(1)(a,b).
[75] Ibid., Article 5(1)(c).
[76] Ibid., Article 5(1)(d).
[77] Ibid., Article 5(1)(e).

- Infer emotions of natural persons in workplace and in education institutions.[78]
- Enable biometric categorisation of persons on the basis of specific criteria.[79]
- Provide for real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes.[80]

The systems mentioned above are considered particularly harmful, abusive, and contrary to the EU's fundamental values, democracy, and individual human rights and freedoms. Consequently, it is prohibited to place them on the market, put them into service, or use them. Placing on the market is defined as making available on the market for distribution or use 'in the course of a commercial activity, whether in return for payment or free of charge'. Therefore, it appears that the prohibition becomes operative only when an AI system has already been developed and becomes available for use. For instance, the AI Act does not seem to preclude the development of a system which can infer the emotions of military personnel in certain high-stress situations. Further, because placing AI systems exclusively for military, defence, and national security purposes in the market is excluded from the scope of the AI Act, we can see that the development and use of generally prohibited AI systems might be possible in these domains. This is an example of a situation where legal challenges could occur. For instance, courts might think about the usage of AI emotion recognition systems for selecting military personnel for certain functions and whether that would be considered a matter falling fully within Article 4(2) of the TEU, or a matter where the court could exercise its competence and possibly provide some guidance.

3.2.2.3. High-risk AI systems

Following prohibited AI practices, the next category is high-risk AI systems. These are products, or safety components of products,[81] specifically listed in the AI Act and regulated under EU law.[82] They include such items as machinery, toys, lifts, some medical devices, products in the field of aviation security, and some vehicles. High-risk AI can also be specific systems[83] in biometrics; critical infrastructure; education and vocational training; employment; workers management; access to and enjoyment of essential private services and essential public services and benefits; law enforcement; migration, asylum and border control management; administration of justice and democratic processes.[84]

[78] Ibid., Article 5(1)(f).
[79] Ibid., Article 5(1)(g).
[80] AI Act, Article 5(1)(h).
[81] Ibid., Article 6(1).
[82] Ibid., Annex II.
[83] Ibid., Article 6(2a).
[84] Ibid., Annex III.

High-risk AI systems are subject to strict regulatory requirements, which form a significant part of the regulations. These include having appropriate risk management systems, rules on using data for training AI models, documentation and record-keeping, transparency and providing information to deployers, accuracy, robustness and cybersecurity. These obligations generally seek to ensure that high-risk AI systems are trustworthy.

3.2.2.4. Other AI systems

The AI Act also contains obligations for AI systems which are neither specifically prohibited nor high-risk but still require additional regulations. First, where an AI system (for instance, a chatbot or virtual assistant) is intended to interact directly with natural persons, there is, with some exceptions, a duty to inform the person that they are interacting with an AI system.[85]

Secondly, providers of AI systems which generate synthetic audio, image, video or text content, have an obligation to ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated.[86] Similarly, deployers of AI systems that generate or manipulate image, audio, or video content constituting “deep fake”, or those which generate or manipulate text published for the purpose of informing the public, must disclose that the content has been artificially generated or manipulated.[87]

Third, deployers of an emotion recognition system or biometric categorisation system must inform natural persons exposed to the operation of the system and process their data in accordance with personal data protection rules.[88]

3.2.2.5. General-purpose AI models

General purpose AI models are regulated by a separate set of provisions under the AI Act. Pursuant to a definition in Article 3(66) of the AI Act, the general-purpose AI model is:

> an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are released on the market.

[85] Ibid., Article 50(1).

[86] Ibid., Article 50(2).

[87] Ibid., Article 50(4).

[88] Ibid., Article 50(3).

The key characteristics of general-purpose AI models are that they are capable of significant generality and able to competently perform a wide range of distinct tasks.[89] Furthermore, they can, but do not have to be, trained with large amounts of data using different methods. And while generality and the ability to perform a wide range of tasks can be determined by various factors, 'models with at least a billion of parameters and trained with a large amount of data using self-supervision at scale' are considered to satisfy those conditions.[90] Typical examples of general-purpose AI models are those which allow for 'flexible generation of content, such as in the form of text, audio, images or video, that can readily accommodate a wide range of distinctive tasks'.[91]

As explained in Recital 97, although AI models are essential components of AI systems, they do not constitute AI systems on their own. AI models require the addition of further components, such as for example a user interface, to become AI systems. AI models are typically integrated into and form part of AI systems. Hence, if an AI model which allows image processing is integrated as a safety component in an autonomous car, it becomes part of an AI system. Providers of general-purpose AI models are subject to multiple obligations, including ensuring transparency of their models. Hence, with some exceptions, they are required to publish up-to-date documentation about their models, address copyright issues, and explain how their models are trained.[92]

3.2.2.6. General-purpose AI models with systematic risks

Some general-purpose AI models are considered to pose systematic risks and are, therefore, subject to stricter regulatory regimes. General-purpose AI models pose a systematic risk if they possess certain technical capabilities or are capable of producing certain effects.[93] The specific determining criteria are provided in Annex XIII of the AI Act. In addition to obligations applicable to providers of all general-purpose AI models, providers of models with systemic risk must undertake additional duties regarding evaluation, risk assessment and mitigation, incident management, and cybersecurity.[94]

3.2.2.7. Impact on defence and military sectors

As previously discussed, the development and use of AI systems and general-purpose AI models are subject to strict regulatory requirements. Generally, there are no rules which would exclude the possibility of using an AI system or model in

[89] See also Recital 97 of the AI Act.
[90] AI Act, Recital 98.
[91] AI Act, Recital 99.
[92] AI Act, Article 53.
[93] AI Act, Article 51.
[94] AI Act, Article 55.

defence and military domains. In contrast, as elaborated above, Article 2(3) of the AI Act generally seeks to exclude the use of AI in these sectors from the scope of regulation. The main issue here might be that many AI systems have dual uses. For instance, an AI system used as a component in a civilian vehicle can at the same time be used for military vehicles. An AI model used to produce synthetic videos in the form of deep fakes can be used for civilian purposes or to lead a campaign aimed at achieving certain military aims. However, the AI Act generally contains sufficient rules to address these issues when it creates broad exclusions for the national security, military, and defence sectors.

It must be acknowledged that the AI Act will impose significant requirements on the AI industry, when it comes into force. And of course, if we compare Europe to jurisdictions with fewer or no regulations, then the legal framework for development and use of AI in Europe may appear more restrictive. However, whether these rules will seriously limit innovation and creativity and the use of AI products remains to be seen. Furthermore, AI technology is itself just one part of the equation. Another one is the data processed by AI which might be an area with potentially an even bigger need for legal regulation.

3.3. AI as an analytical enabler: processing of data

One of the most promising uses of AI in the military is in the intelligence, surveillance, and reconnaissance domains. In this context, AI acts as an analytical enabler, making it possible to analyse substantial quantities of data, including live data, which would otherwise require disproportionate amounts of work by human analysts.[95] Similarly, Nurkin stated that:

> near ubiquitous and networked sensors embedded in equipment and in human operators will collect massive amounts of data that could overwhelm the capacity of humans to process – be it video, images, biometric data, signals intelligence, geospatial intelligence, or other types of information.[96]

According to the French AI strategy, AI is used in applications which aim to detect and recognise data, predict future outcomes, seek correlations in order to deduce a generic form of behaviour or flag up abnormal behaviour, and optimise solutions to problems such as logistical flows or flight paths.[97]

All these factors are highly dependent on the availability of reliable data. This is explicitly recognised by NATO, which is addressing this issue through its Data Exploitation Framework Policy. The purpose of this policy is to 'ensure that NATO is able to leverage data as a strategic resource' and to improve the data exploitation

[95] Rickli and Mantellassi, 2023, p. 19.

[96] Nurkin, 2023, p. 37.

[97] French Ministry of Defence, 2019, p. 3.

capabilities across all levels in the military, civilian, and political domains'.[98] By doing so, the alliance aims to achieve multiple goals, including information superiority and data-driven decision-making at all levels.[99] This Policy makes explicit reference to NATO's AI Strategy; therefore, it is obvious that one of the purposes of the data exploitation policy is to support the alliance's AI efforts.

The use of AI for data analytics purposes also features prominently in national strategic documents, and it is clear that data analytics can support both combat and noncombat operations. Regarding combat operations, AI is primarily expected to improve situational awareness and decision-making.[100] As explained in the U.S. 2018 strategy, 'AI can generate and help commanders explore new options so that they can select courses of action that best achieve mission outcomes'.[101] It is also recognised that the use of AI for analytics can contribute to compliance with the law of armed conflicts, because advanced analytics can improve the accuracy of military assessments and enhance mission precision, thereby reducing the risk of civilian casualties and other collateral damage.[102]

With regard to noncombat operations, the benefits of AI are manifold, including reducing inefficiencies in manual, laborious, and data-centric tasks, simplifying workflows, and improving the speed and accuracy of repetitive tasks.[103] It can increase the safety and supply of operating equipment, and streamline business processes.[104]

However, data can be a scarce resource for at least two reasons. First, some states might not have access to the same quantities of data because they do not have strong local data-centric industries. In this context, the French AI strategy states that:

> major digital players, especially American and Chinese, … have access to what really fuels AI: the vast mass of data that their customers provide to them free of charge at each interaction. Having initially sought to know their customers better in order to enhance their products and services, these actors are now using their very deep pockets to pursue greater ambitions, such as driverless cars, smart cities and personalised healthcare. Their products set the standard, and the sheer extent of their use cases makes them attractive to the military, especially in the many dual-use applications. As in the digital sphere as a whole, the defence sector does not necessarily blaze a trail but takes advantage of advances in civilian uses, adapting them to its own particular needs where necessary.[105]

[98] NATO, 2021b, para. 1.1.
[99] Ibid., para 2.1.
[100] U.S. Department of Defense, 2019, p. 11.
[101] Ibid., p. 11.
[102] U.S. Department of Defense, 2019, p. 6.
[103] Ibid., p. 6.
[104] Ibid., p. 11.
[105] French Ministry of Defence, 2019, p. 4.

Second, states operate under different legal requirements where the use of data is concerned. In some countries, there are no strong privacy or personal data protection laws, which consequently creates a more permissive environment for data processing. Others may be operating in different circumstances. As also noted in the French AI strategy, 'the collection and exploitation of data on a massive scale cannot be envisaged without strict compliance with prevailing personal data legislation, especially the GDPR'.[106] Likewise, the NATO Data Exploitation Framework Policy calls for 'data exploitation efforts aligned with core Alliance values, including the protection of personally identifiable information and privacy'.[107]

Globally, it is difficult to find a legal system which imposes stricter requirements for data processing than that of the EU. From the perspective of EU law, any piece of data is either personal or non-personal. Both categories are subject to legal regulations, with that governing the use of personal data being much more stringent. Moreover, specific rules are applicable to electronic communications data. Therefore, in the following sections, we consider whether and how the EU rules regulating the use of data can indirectly impact the use of AI systems.

3.3.1. Electronic communications data

Electronic communications are a rich source of data that can be used for law enforcement, national security, and defence purposes. For instance, surveillance of electronic communications is a method routinely used by investigative agencies all around the world when dealing with serious crime, and the same methods are also frequently used for national security purposes. Electronic communications data can be especially useful in the context of military operations. For instance, it was recently reported that the use of cell phones by a group of Russian soldiers enabled Ukrainian military to determine their location, leading to a deadly strike on the premises where they were located.[108] This is an obvious example of a military action taken on the basis of analysed electronic communications data, but such data can also be used outside of military conflicts, for various intelligence gathering, counter-intelligence and surveillance purposes in the context of national defence. And while in times of war accessing electronic data for defence purposes may not trigger legal concerns, the situation is different in peacetime when access to data still might be necessary.

When dealing with communications surveillance, it is useful to differentiate between content data and metadata. Content data is 'the meaning or purport of the communication, or the message or information being conveyed by the communication'.[109] Metadata can include various categories of technical data generated in the

[106] Ibid., 2019, p. 13.

[107] NATO, 2021b, para. 3.1.

[108] *Unauthorized use of cellphones by Russian soldiers led to Ukrainian strike that killed 89 troops, military says*, 2023.

[109] Council of Europe, 2001, para. 209.

course of the conveyance of communications. It includes what is sometimes designated as “traffic data” and “location data”. For instance, in the Council of Europe’s Convention on Cybercrime traffic data is defined as any data ‘indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service’.[110] EU Directive 2002/58 defines it more generally as ‘any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof’.[111] The now invalidated EU Data Retention Directive had a detailed list of categories of data falling within this definition, including data indicating the source and destination of communication; the date, time duration, and type of communication, and the location and type of mobile communication equipment used.[112]

Tapping these data provides a rich source of information for state authorities in the domains of law enforcement, national security, and national defence. The interception of content data and the real-time monitoring of traffic data for criminal investigations and proceedings is explicitly envisaged at the European level by the Council of Europe’s Convention on Cybercrime.[113] Almost all countries use similar powers based on domestic legislation for national security purposes.

In the EU, the Directive on Privacy and Electronic Communications (ePrivacy Directive) regulates the processing of personal data and the protection of privacy in the electronic communications sector. It applies to all publicly available electronic communications services in public communications networks in the EU,[114] but pursuant to Article 1(3), it does not apply to:

> activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Member States are required to ensure the confidentiality of communications and the related traffic data, and in particular prohibit ‘listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data’.[115] Generally, traffic data must be erased or anonymised when they are no longer needed for communication transmission.[116] Location data can generally be processed anonymously or with the user’s consent.[117] An exception, is prescribed in

[110] *Convention on Cybercrime*, 2001, Article 1(d).
[111] Directive 2002/58/EC, Article 2(b).
[112] Directive 2006/24/EC, Article 5.
[113] *Convention on Cybercrime*, 2001, Article 20.
[114] Directive 2002/58/EC, Article 3.
[115] Directive 2002/58/EC, Article 5(1).
[116] Directive 2002/58/EC, Article 6(1).
[117] Directive 2002/58/EC, Article 9(1).

Article 15(1) of this directive that Member States of the EU may legislate to restrict the scope of the above rules when such a restriction:

> constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.[118]

It is further explained that 'to this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph'.[119]

Articles 1(3) and 15(1) of the ePrivacy Directive appear to clearly exempt activities concerning core state functions, such as national security, national defence, and activities of the state in areas of criminal law, namely the prosecution of criminal offences, from safeguards defined in the directive. However, the situation is much more complicated. Member States are, among other exceptions to privacy and personal data protection in the context of electronic communications, permitted (per Article 15(1) of the ePrivacy Directive) to enact legislation requiring service providers to retain (proactively store) traffic data, for a limited period, on grounds which includes *inter alia* national security and defence. Several years after the ePrivacy Directive was enacted, the permission for Member States to provide for retention of data became their obligation, when the Data Retention Directive came into force in 2006. That directive now required Member States to adopt measures to ensure that traffic data (as defined in its Article 5) be retained for a period of not less than six months and not more than two years from the date of the communication.[120] The Data Retention Directive had a transposition period until 15 September 2007 which could have been extended by individual Member States to 2009 for internet access, internet telephony, and internet e-mail.

Although the Data Retention Directive envisaged the use of retained data primarily for law enforcement purposes, it did not limit access to retained data solely to state authorities acting in the criminal law domain. Instead, it was prescribed that the retained data be accessible to competent national authorities in specific cases and in accordance with national law.[121] Therefore, many Member States provided that in addition to law enforcement, authorities in the national security and defence sectors could also access and use the retained data.

For the next approximately seven years, the Member States were obligated to ensure that communication service providers retained traffic data for all their users and made it accessible to competent national authorities, as defined in national law.

[118] Directive 2002/58/EC, Article 15(1).

[119] Directive 2002/58/EC, Article 15(1).

[120] Directive 2006/24/EC, Articles 3, 5 and 6.

[121] Directive 2006/24/EC, Article 4.

Then in 2014, the Court of Justice of the EU (CJEU) invalidated the Data Retention Directive in *Digital Rights Ireland* case, on the account that it disproportionately interferes with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. The court applied a strict necessity test and found the directive lacking, for multiple reasons.

After the Data Retention Directive was invalidated, the situation effectively reverted to that established by the ePrivacy Directive: Member States were permitted, but no longer obliged, to require service providers to retain data. However, this was only the beginning of the EU data retention saga. Two years after *Digital Rights Ireland*, the CJEU ruled in *Tele2 and Watson*[122] that national legislation which provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication is contrary to Article 15(1) of the ePrivacy Directive, interpreted in light of CFEU.[123]

Although the issue of the scope of restrictions mentioned in Articles 1(3) and 15(1) was occasionally raised before, in *La Quadrature du Net and Others v. Premier minister and Others* the CJEU was explicitly asked to rule, *inter alia*, whether general and indiscriminate retention of traffic and location data for, among other purposes of national security, territorial integrity, and national defence, is in violation of relevant EU law.[124] In these joined cases, several Member States advanced the argument that national legislation pursuing those aims falls outside the scope of the ePrivacy Directive on the basis of Article 1(3),[125] also considering the division of competences between the Union and its Member States, as defined in Article 4(2) of the Treaty on European Union (TEU). It was argued that activities of intelligence services 'in so far as they relate to the maintenance of public order and to the safeguarding of internal security and territorial integrity, are part of the essential functions of the Member States and, consequently, are within their exclusive competence'.[126]

However, the CJEU was not persuaded. In fairness, many of the problems stem from the fact that the ePrivacy Directive stipulates in Article 1(3) that activities concerning public security, defence, state security, etc., are exempt from its scope of application, and then in Article 15(1) allows Member States to, under certain conditions, restrict the scope of rights and obligations provided for in the directive for essentially the same purposes. Therefore, it seems logical to conclude that if all activities related to the security purposes of the state were exempted from the scope of the directive based on Article 1(3), there would be no need to regulate restrictions for those same purposes in Article 15(1). Therefore, the CJEU concluded that:

[122] C-203/15 and C-698/15 (*Tele 2 and Watson*).

[123] C-203/15 and C-698/15 (*Tele 2 and Watson*), para. 134.

[124] C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and others v. Premier minister and Others*), para. 84.

[125] Ibid., para. 86.

[126] Ibid., para. 89.

> Article 15(1) of Directive 2002/58 necessarily presupposes that the national legislative measures referred to therein fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.[127]

However, the opposite is also true: if all activities in the security domain must satisfy the conditions under Article 15(1) of the Directive, then what would be the purpose of exempting those activities based on Article 1(3)?

The CJEU solves this conundrum by differentiating between data processing operations carried out by providers of electronic communications services, including operations resulting from obligations imposed on those providers by public authorities and operations directly implemented by Member States, without imposing processing obligations on service providers.[128] The first category is within the scope of the ePrivacy Directive and can be lawful under EU law, provided that conditions under Article 15 are satisfied. The second category is exempt from the ePrivacy Directive pursuant to Article 1(3).

What is important in this context is that the CJEU is explicit in explaining that the considerations of Article 4(2) of the TEU do not change the outcome. This is because the court maintains the position 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.[129]

It might be claimed that the issues surrounding the use of electronic communications metadata are only marginally relevant to the discussion of the use of AI in the military and defence sectors. However, that is so only on first sight. The core argument here is that the application of personal data protection rules, including those in electronic communications, has the potential to significantly impact data processing in those domains. In short, outcomes of the discussions on data retention in the EU are that Member States are precluded from ordering service providers to store electronic communication's metadata generally and indiscriminately, even when they are acting for national security purposes, which is fully in the domain of competences of the Member States. Furthermore, the CJEU set the standards for permissible data retention itself, by explaining in *Tele2 and Watson* that while general and indiscriminate data retention is prohibited, "targeted retention" (which

[127] Ibid., para. 95.

[128] Ibid., paras. 101, 103.

[129] C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and others v. Premier minister and Others*), para. 99.

is nowhere defined in EU law) might be permitted under certain conditions. It would take too much space in this chapter to define targeted retention, and discuss the legal problems caused by the approach mandated by the CJEU. In our view, the main message here is that the courts should not assume the role of legislators and should exercise their discretion moderately.

3.3.2. Personal data

The analysis above was limited to discussing the use of data from electronic communications, for the purposes of national security and defence. While this includes vast amounts of data which could be useful in the miliary and defence sectors, there are many more data being generated and processed outside of electronic communications. In legal terms, those other data might be considered "personal data" under applicable EU law. This category of data is currently regulated by the GDPR, which replaced the previously applicable Directive 95/46 in 2018.[130] If data is considered personal and is otherwise within the scope of the GDPR, then very strict regulatory regimes will apply to it.

Pursuant to Article 4(a) of the GDPR, personal data is defined as:

> any information relating to an identified or identifiable natural person („data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This might seem to be a straightforward concept, but once again the devil seems to be in the details. Personal data encompasses (1) any information which is (2) related to (3) an identified or identifiable (4) natural person.[131]

The notion of "any information" is very broad. Importantly, the rights to personal data protection and privacy are not synonymous.[132] Therefore, as was made explicit by the CJEU in *Client Earth,* 'the concepts of "personal data"… and of "data relating to private life" are not to be confused. Consequently, the claim … that the information at issue does not fall within the scope of the private life … is ineffective'.[133] Even if information is provided as part of a professional activity, it can be characterised as personal data.[134] It does not matter whether access to the information is limited

[130] Regulation EU 2016/679.

[131] *Opinion 4/2007 on the concept of personal data*, 2007.

[132] See more extensively in Kokott and Sobotta, 2013.

[133] C-615/13 P (*ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission*), para. 32.

[134] C-615/13 P (*ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission*), para. 30.

or not. Therefore, in *Lindqvist* the CJEU considered that information published on a freely accessible webpage enjoys full protection under data protection law.[135] Regarding the concept of personal data, it does not matter whether the information is ordinary or sensitive, objective or subjective, true or false.[136] It can be stored in any medium or form. In its case law, the CJEU has interpreted the notion of personal data so broadly that it has thus far excluded only abstract legal analyses.[137]

The notion of "natural person" is straightforward since it always covers living natural persons.[138] Therefore, every time information relates to a living person, it is potentially that person's personal data. Crucial for determining whether something is personal data, especially in the context of the issues discussed in this chapter, is the notion of the relationship between the information and the person and the identifiability of that person. As mentioned, information is personal data if, among other conditions, it relates to a natural person. The criteria of "relationship" has so far been most developed by the Article 29 Working Party, which was established under Directive 95/46 as a body composed of a representative of the supervisory authority or authorities designated by each Member State. According to one opinion of this working party, the criterion of relationship requires that information be linked to a person based on its content, purpose, or results. The element of content is deemed to be satisfied if the information is very broadly "about a person". If this condition is not satisfied, it becomes relevant whether the information is processed with a purpose to 'evaluate, treat in a certain way or influence the status or behaviour of an individual'. Finally, if this is also not the case, then information can still be personal data if its processing 'is likely to have an impact on a certain person's rights and interests'. An impact does not have to be a major one, as it is sufficient that the individual may be treated differently from other persons as a result of the processing of the data.[139] The requirement that information relates to a person has not so far generated more extensive analysis by the CJEU, although the court did seem to endorse the criteria of the Article 29 Working Party when it concluded in *Nowak v. Data Protection Commissioner* that 'as regards the latter condition [relates to], it is satisfied where the information, by reason of its content, purpose or effect, is linked to a particular person'.[140]

Finally, information related to a natural person is personal data if the person is identified or identifiable. This issue is subject to extensive debate,[141] as it has the potential to significantly impact the scope of the application of EU personal data

[135] C-101/01 (*Lindqvist*), para. 27.

[136] *Opinion 4/2007 on the concept of personal data*, 2007, pp. 6–9.

[137] C-141/12 (*YS*), para. 39.

[138] It is explained in Recital 27 of the GDPR that it does not apply to the personal data of deceased persons, but Member States may provide for rules regarding the processing of personal data of deceased persons.

[139] *Opinion 4/2007 on the concept of personal data*, 2007, pp. 10–11.

[140] C-434/16 (*Nowak v. Data Protection Commissioner*), para. 35.

[141] Purtova, 2022.

protection rules. Many issues surround the notion of identifiability, but the key issue is what is actually meant by a person being "identified". To simplify a complicated issue to some degree, it might mean that a person's civil identity is determined, or, as was argued by Article 29 of the working party, that a person is somehow "distinguished" from all other members of the group.[142] But it appears that the CJEU did not follow the second approach in *Breyer v. Bundesrepublik Deutschland*, where it reasoned that an IP address 'does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer'.[143] Therefore, according to the CJEU, the question of whether a dynamic IP address is personal data depends on whether the owner of the address 'has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person'.[144] Based on this judgement, it appears that the court pursued the first approach mentioned above, which effectively requires establishing the data subject's civil identity. However, this approach is convincingly criticised in the legal literature, and there is also some guidance from national courts and data protection authorities which pursue different and broader interpretations of the element of identification.[145] Finally, on 7 March 2024 the CJEU published a decision in the *IAB Europe v. Gegevensbeschermingsautoriteit* case,[146] concluding that:

> a string composed of a combination of letters and characters … containing the preferences of a user of the internet or of an application relating to that user's consent to the processing of personal data concerning him or her by website or application providers as well as by brokers of such data and by advertising platforms constitutes personal data within the meaning of that provision in so far as, where those data may, by reasonable means, be associated with an identifier, such as, *inter alia*, the IP address of that user's device, they allow the data subject to be identified. In such circumstances, the fact that, without an external contribution, a sectoral organisation holding that string can neither access the data that are processed by its members under the rules which that organisation has established nor combine that string with other factors does not preclude that string from constituting personal data within the meaning of that provision.

While the CJEU still maintains that identifiability of the data requires the subject of the data to be "identified" (as opposed to singled out), the court did send a strong message that in the context of a particular case the string should be treated as personal data, since identification can happen on the basis of additional data, which

[142] *Opinion 4/2007 on the concept of personal data*, 2007, p. 12.
[143] C-582/14 (*Breyer v. Bundesrepublik Deutschland*), para. 38.
[144] C-582/14 (*Breyer v. Bundesrepublik Deutschland*), para. 49.
[145] See: Purtova, 2022.
[146] C-604/22 (*IAB Europe v. Gegevensbeschermingsautoriteit*), para. 78.

do not necessarily have to be in the possession of the data controller. Finally, it is important to note that the court did not specifically mention its earlier position from *Breyer v. Bundesrepublik Deutschland*, pursuant to which it is relevant whether the data controller has the legal means to obtain the additional data necessary for identification (although this was one of the questions asked).

Looking from the perspective of the use of AI in the military and defence sectors to process data, the key initial challenge will be assessing whether certain data is "personal" in the sense of the GDPR. The problem here lies in the fact that the assessment of whether something is personal data involves complex case-by-case analyses in which multiple legal and technological issues need to be considered. The general issue, in our opinion, is that personal data is a much broader concept than one might think before making an appropriate analysis. Therefore, it might come as a surprise to many entities, including those in the military and defence sectors, to realise that the data they process are actually personal. For instance, when the NATO Data Exploitation Framework Policy mentions the 'protection of personally identifiable information and privacy', it is referring to concepts which are narrower than the personal data. As we have seen from the electronic communications cases, the CJEU is not shy about enforcing personal data protection rules to the fullest extent, even in cases which are ordinarily matters of national regulation.

Even if it is concluded that data is non-personal, it does not mean that it is outside the scope of EU law *per se*, since this matter is regulated by *Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union*.[147]

is the regulation on non-personal data contains a generic provision on its scope, pursuant to which it does not apply to an activity which falls outside the scope of Union law,[148] which, as explained in Recital 12, includes national security.

Compared to the GDPR, the aims of the Regulation on non-personal data are much more limited. Essentially this regulation aims to ensure the free flow of non-personal data within the Union by prohibiting data localisation requirements, thus ensuring the availability of data to competent authorities and facilitating the porting of data for professional users. The Regulation on non-personal data seeks to remove obstacles to the development of data economy in the Union, namely 'data localisation requirements put in place by Member States' authorities and vendor lock-in practices in the private sector'.[149] But the Regulation on non-personal data does not go further than that, and therefore, it will probably not have a significant impact on the use of data in the context of AI activities in military and defence sectors.

Next, we turn to the scope of application of the GDPR. According to Article 2(1), the GDPR applies to the processing of personal data wholly or partly by automated

[147] Regulation (EU) 2018/1807.

[148] Regulation (EU) 2018/1807, Article 2(3).

[149] Regulation (EU) 2018/1807, Recital 2.

means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

As in the case of the ePrivacy Directive mentioned above, the GDPR also exempts some activities from its scope of application.[150] The issues discussed in this chapter include the processing of personal data in the course of an activity which falls outside the scope of EU law[151] and the processing of personal data by Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU.[152] As with other exceptions, the CJEU firmly holds that it must be interpreted narrowly.[153]

Recital 16 of the GDPR elaborates that the exemption for data processing activities outside the scope of EU law includes activities concerning national security. Notably, the earlier Directive 95/46 had the same exemption, specifying that it included 'processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) …'. Although the GDPR now refers only to national security purposes, there should be no doubt that activities outside the scope of EU law also includes data processing for national defence purposes. The CJEU considers the national security exemption a 'continuation of the first indent of Article 3(2) of Directive 95/46'. Therefore, the CJEU speaks about 'activity which is intended to safeguard national security or of an activity which can be classified in the same category'.[154] Moreover, the CJEU explicitly states that 'the activities having the aim of safeguarding national security … encompass… those that are intended to protect essential State functions and the fundamental interests of society'.[155]

Pursuant to the CJEU case law, there are two conditions which need to be satisfied cumulatively for an exception under Article 2(2)(a) to apply. These revolve around the identity of the data controller and the method of the data processing activity.

First, data processing activities should be carried out by competent authorities.[156] This seems, at least to some extent, supported by the reasoning of the CJEU in *La Quadrature du Net and Others v. Premier minister and Others,* where the court referred to Article 23 of the GDPR to differentiate between data processing activities carried out 'by competent authorities' as opposed to those carried out by individuals.

Secondly, it is not sufficient that data processing activity is 'characteristic of the State or of a public authority'.[157] Instead, it should be an activity genuinely intended

[150] GDPR, Article 2(2).
[151] GDPR, Article 2(2)(a).
[152] GDPR, Article 2(2)(b).
[153] C-439/19 (*B v. Latvijas Republikas Saeima*), para. 62; C-272/19 (*VQ v. Land Hessen*), C-311/18 (*Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*), para. 84.
[154] C-439/19 (*B v. Latvijas Republikas Saeima*), para. 64.
[155] C-439/19 (*B v. Latvijas Republikas Saeima*), para. 67.
[156] C-439/19 (*B v. Latvijas Republikas Saeima*), para. 66.
[157] C-439/19 (*B v. Latvijas Republikas Saeima*), para. 66.

to safeguard national security (or an activity which can be classified into the same category, e.g. national defence). As the CJEU explains, 'the activities having the aim of safeguarding national security that are envisaged in Article 2(2)(a) of the GDPR encompass, in particular, those that are intended to protect essential State functions and the fundamental interests of society'. Applying this standard, the CJEU concluded in 2022 that 'activities relating to the organisation of elections in a Member State do not pursue such an objective'.[158]

Overall, it does not seem likely that the use of personal data for purposes of AI in military and defence will be fully exempted from the scope of EU law. As a result, data protection rules, particularly the GDPR, will impact many aspects of data processing in these sectors. It will be necessary to comply with all personal data protection principles, including data minimisation, purpose limitation, and storage limitation. Specifically for purpose limitation, using data collected and processed by some private entities will be considered processing, and will require appropriate legal basis under national law. Finally, even when certain data processing activities fall outside the scope of EU law, they may still be subject to national constitutional law and the requirements of the ECHR.

4. Conclusions

The potential uses of AI in the military and defence sectors appear to be almost unlimited. As explained in this and other chapters, there is almost no area of military and defence activity in which AI could not make a meaningful impact. But to what extent is the development and use of AI in military and defence currently regulated in the EU? Our analysis shows that although there is no lack of regulation, the legal framework itself should not pose insurmountable obstacles for the industries and entities acting for the military and defence sectors. It seems likely that ethical considerations are the real factor preventing European countries from advancing more aggressively with AI solutions in the defence and military arenas.

This is visible for instance in the regulation of LAWS. While there are no binding EU rules on the matter, European institutions have strongly emphasised the responsible development and use of such systems. However, after careful consideration of the European Parliament's stance, it is evident that it is advocating for reasonable safeguards aimed at ensuring human control and accountability.

While autonomous drones and other lethal weapons systems acting without, or with limited human control, rightly occupy the top of the list of concerns, there are many more areas where AI can make a meaningful impact. Therefore, in this

[158] C-306/21 (*Komisia za zashtita na lichnite danni and Tsentralna izbiratelna komisia v. Koalitsia Demokratichna Bulgaria – Obedinenie*), para. 41.

chapter, we examined the legal regulations for AI in general. We identified the forthcoming AI Act as the directly applicable EU regulation, but we also considered rules on access to data processed by AI systems.

The drafters of the AI Act made serious efforts to exclude the military, defence and national security sectors from the scope of application. However, this does not mean that all AI-related activities in these domains will avoid CJEU scrutiny. As the existing case law shows, the court has intervened in many cases in areas which are primary competencies of Member States, including matters of national defence. Therefore, it is possible that the same approach may also be followed in AI-related cases. In our view, considering the division of competences between Member States and the EU, the legislative history of the AI Act, and the challenges of regulating technologically advanced systems such as AI, it would be preferable to see the CJEU exercise its powers very cautiously when it inevitably faces questions about the use of AI in the military and defence domains.

Finally, we believe that the biggest challenges in the development and use of AI in the military and defence domains may stem from regulations governing data use. As data are what really fuels AI, access to data is of fundamental importance. Our analysis shows that current EU rules can be applied to the military and defence sectors, with fewer possibilities of exemption than in the AI Act, especially in light of existing CJEU case law. When we combine this with a broad concept of personal data, it is clear how personal data protection rules could seriously limit the ability of national defence and military entities to process certain types of data.

References

Anand, A., Deng, H. (2023) *Towards Responsible AI in Defence: A Mapping and Comparative Analysis of AI Principles Adopted by States*. Geneva: UNIDR.

Gosselin-Malo, E. (2023) 'NATO to update artificial intelligence strategy amid new threats', *Yahoo News*, 30 November 2023. [Online]. Available at: https://news.yahoo.com/nato-artificial-intelligence-strategy-amid-143228193.html (Accessed: 2 February 2024).

Gray, M., Ertan, A. (2021) *Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment*. Tallinn: NATO CCDCOE.

Kokott, J., Sobotta, C. (2013) 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law*, 3(4), pp. 222–228; https://doi.org/10.1093/idpl/ipt017.

Nurkin, T. (2023) 'AI and Technological Convergence: Catalysts for Abounding National Security Risks in the Post-COVID-19 World' in Raska, M., Bitzinger, R.A. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*. London: Routledge, pp. 37–58; https://doi.org/10.4324/9781003218326-3.

Purtova, N. (2022) 'From knowing by name to targeting: the meaning of identification under the GDPR', *International Data Privacy Law,* 12(3), pp. 163–183; https://doi.org/10.1093/idpl/ipac013.

Rickli, J.-M., Mantellassi, F. (2023) 'Artificial Intelligence in Warfare: Military Uses of AI and Their International Security Implications' in Raska, M., Bitzinger, R.A. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*. London: Routledge, pp. 12–36; https://doi.org/10.4324/9781003218326-2.

Soare, S. (2023a) 'Algorithmic power? The role of artificial intelligence in European strategic autonomy' in Cristiano, F., Broeders, D., Delerue, F., Douzet, F., Géry, A. (eds.) *Artificial Intelligence and International Conflict in Cyberspace*. 1st edn. London: Routledge, pp. 77–108; https://doi.org/10.4324/9781003284093-6.

Soare, S. (2023b) 'European Military AI: Why Regional Approaches Are Lagging Behind' in Raska, M., Richard, B. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*. London and New York: Routledge, pp. 80–111; https://doi.org/10.4324/9781003218326-5.

Taddeo, M., Blanchard, A. (2021) *A Comparative Analysis of the Definitions of Autonomous Weapons Systems*. UNODA. [Online]. Available at: https://documents.unoda.org/wp-content/uploads/2021/10/20210721-Autonomous-Weapon-Systems-Definitions-TO-SHARE.pdf (Accessed: 30 October 2024).

Taddeo, M., McNeish, D., Blanchard, A., Edgar, E. (2023) 'Ethical principles for artificial intelligence in the defence domain' in Cristiano, F., Broeders, D., Delerue, F., Douzet, F., Géry, A. (eds.) *Artificial Intelligence and International Conflict in Cyberspace*. 1st edn. London: Routledge, pp. 159–185; https://doi.org/10.4324/9781003284093-10.

Géry, A. (ed.) *Artificial Intelligence and International Conflict in Cyberspace*. 1st edn. London: Routledge, pp. 160–185; https://doi.org/10.4324/9781003284093-10.

Unauthorized use of cellphones by Russian soldiers led to Ukrainian strike that killed 89 troops, military says (2023) *CBS news*, 4 January 2023. [Online]. Available at: https://www.cbsnews.com/news/ukraine-news-russia-military-blames-cell-phones-strike-soldier-deaths/ (Accessed: 30 October 2024).

Policy documents

Devitt, K., Gan, M., Scholz, J, Bolia, R. (2020) *A Method for Ethical AI in Defence*. Canberra: Australian Department of Defence. [Online]. Available at: https://www.dst.defence.gov.au/sites/default/files/publications/documents/A%20Method%20for%20Ethical%20AI%20in%20Defence.pdf (Accessed: 30 October 2024).

Digitalization and Artificial Intelligence in Defence (2019) *Food for Thought Paper by Finland, Estonia, France, Germany, and the Netherlands,* 15 May. [Online]. Available at: https://valtioneuvosto.fi/documents/11707387/12748699/Digitalization+and+AI+in+Defence.pdf/151e10fd-c004-c0ca-d86b-07c35b55b9cc/Digitalization+and+AI+in+Defence.pdf (Accessed: 30 October 2024).

European Commission (2018) 'Artificial Intelligence for Europe', COM/2018/237 final, *EU Monitor,* Brussels, 25 April.

European Commission (2019) 'Ethics Guidelines for Trustworthy AI', *High-Level Expert Group*, 8 April. [Online]. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 (Accessed: 30 October 2024).

European Commission (2020) 'White Paper On Artificial Intelligence – A European approach to excellence and trust', COM(2020) 65 final, Brussels, 19 February.

European Parliament (2014) *Resolution of 27 February 2014 on the use of armed drones*. OJ C 285, 29 August 2017, pp. 110–111.

European Parliament (2018) *Resolution of 12 September 2018 on autonomous weapon systems,* OJ C 433, 23 December 2019, pp. 86–88.

European Parliament (2020) *Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies*, OJ C 404, 6 October 2021, pp. 63–106.

European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (2021) COM(2021)0206 – C9-0146/2021 – 2021/0106(COD), Brussels, 21 April 2021. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7536_2024_INIT (Accessed: 30 October 2024).

European Union External Action (2022) *A Strategic Compass for Security and Defence*. [Online]. Available at: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf (Accessed: 30 October 2024).

French Ministry of Defence (2019) 'Artificial Intelligence is Support of Defence', September 2019. [Online]. Available at: https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI%20Task%20Force%20September%202019.pdf (Accessed: 30 October 2024).

NATO (2021a) 'Summary of the NATO Artificial Intelligence Strategy', 22 October 2021. [Online]. Available at: https://www.nato.int/cps/en/natohq/official_texts_187617.htm (Accessed: 30 October 2024).

NATO (2021b) 'Summary of NATO's Data Exploitation Framework Policy', 22 October 2021. [Online]. Available at: https://www.nato.int/cps/en/natohq/official_texts_210002.htm (Accessed: 30 October 2024).

UK Ministry of Defence (2022) 'Defence Artificial Intelligence Strategy', June 2022. [Online]. https://assets.publishing.service.gov.uk/media/62a7543ee90e070396c9f7d2/Defence_Artificial_Intelligence_Strategy.pdf (Accessed: 30 October 2024).

US Department of Defense (2019) *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity.* [Online]. Available at: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF (Accessed: 18 January 2024).

Legislation, international treaties and guidelines

Convention on Cybercrime (2001) ETS 185, Budapest, 23 November 2001.

Council of Europe (2001) 'Explanatory Report to the Convention on Cybercrime', ETS 185, Budapest, 23 November.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2002) OJ L 201, Brussels, 31 July 2002, pp. 37–47.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (2006) OJ L 105, 13 April 2006, pp. 54–63.

Opinion 4/2007 on the concept of personal data (2007) Article 29 Working Party Archives 1997 – 2016. [Online]. Available at: https://ec.europa.eu/justice/article-29/documentation (Accessed: 30 October 2024).

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (2021) COM(2021) 206 final, Brussels, 21 April 2021. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A0206%3AFIN (Accessed: 30 October 2024).

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (2021) 2021/0106(COD), Brussels, 29 November 2021. [Online]. Available at: https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf (Accessed: 30 October 2024).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L 119, 4 May 2016, pp. 1–88.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (2018) OJ L 303, 28 November 2018, pp. 59–68.

Case-law

Court of Justice of the European Union, C-101/01 (*Lindqvist*).

Court of Justice of the European Union, C-141/12 (*YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*).

Court of Justice of the European Union, C-186/01 (*Dory v. Bundesrepublik Deutschland*).

Court of Justice of the European Union, C-273/97 (*Sirdar v. The Army Board and Secretary of State for Defence*).

Court of Justice of the European Union, C-285/98 (*Kreil v. Bundesrepublik Deutschland*).

Court of Justice of the European Union, C-306/21 (*Komisia za zashtita na lichnite danni and Tsentralna izbiratelna komisia v. Koalitsia „Demokratichna Bulgaria – Obedinenie"*).

Court of Justice of the European Union, C-203/15 and C-698/15 (*Tele 2and Watson v. Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*).

Court of Justice of the European Union, C-272/19 (*VQ v. Land Hessen*).

Court of Justice of the European Union, C-311/18 (*Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*).

Court of Justice of the European Union, C-434/16 (*Nowak v. Data Protection Commissioner*). Court of Justice of the European Union, C-439/19 (*B v. Latvijas Republikas Saeima*).

Court of Justice of the European Union, C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and others v. Premier minister and Others*).

Court of Justice of the European Union, C-582/14 (*Breyer v. Bundesrepublik Deutschland*).

Court of Justice of the European Union, C-604/22 (*IAB Europe v. Gegevensbeschermingsautoriteit*).

Court of Justice of the European Union, C-615/13 P (*ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission*).

Court of Justice of the European Union, C-742/19 (*B.K. v. Republika Slovenija*).