European Integration Studies, Volume 20, Number 2 (2024), pp. 107-136.
https://doi.org/10.46941/2024.2.5

MARKO JURIĆ*

Legal regulation on the use of artificial intelligence for national security purposes in Europe**

ABSTRACT: This paper analyses the regulation of the use of AI for national security purposes in Europe. After a brief mapping of most relevant uses of AI for national security purposes, applicable legal framework is analysed. Both the EU AI Act and the Council of Europe's AI Convention provide for broad exceptions regarding the use of AI for national security purposes. This covers activities of both public and private entities acting in the national security domain. In such circumstances, personal data protection law is seen as possessing the most direct impact on the use of AI for national security purposes. In this context, the notion of personal data is explained, emphasizing that any information relating to an identified or identifiable person qualifies as personal data under both the GDPR and Convention 108. The processing of this data, which is broadly defined, can be subject to data protection laws even in national security contexts, provided it meets certain criteria.

The research shows that while there is a lot of uncertainty when it comes to the application of personal data rules to national security situations, existing case-law indicates that application of those rules is not fully excluded. On the contrary, it is to be expected that at least when private entities are involved in data processing operations, personal data protection law might prove to be very effective. Also, it is to be anticipated that the ECHR will play a major role in ensuring that uses of AI for national security purposes remain in line with requirements of democratic society.

KEYWORDS: AI, national security, AI Act, AI Convention, personal data protection.

* Associate professor, Faculty of Law. University of Zagreb, Croatia. https://orcid.org/0000-0001-8499-4193, marko.juric@pravo.unizg.hr.

** The research and preparation of this study was supported by the Central European Academy.

1. Introduction

Artificial intelligence (AI) promises to revolutionise governance in many aspects of private and public affairs. One area that seems particularly ready for such changes is national security.[1] As expressed by the United Kingdom's Government Communications Headquarters (GCHQ), 'an increasing use of AI will be fundamental to GCHQ's mission of keeping the nation safe'.[2] However, at the same time, it is well understood that the use of AI for national security presents many ethical and legal challenges. This study focusses on the latter. In doing so, we attempt to analyse how the use of AI for national security purposes is regulated from the perspective of European law. This is a rather complicated task, for various reasons.

First, as others have noted, the notion of national security is vague and ambiguous,[3] and it ultimately depends on the specific national legal and institutional framework. To simplify things for the purpose of this study, we draw the line between military and non-military actions. Therefore, we consider national security to be a broader concept concerned with protection from non-military threats. Consequently, in this study, we do not analyse specific issues related to the use of AI in the context of military (e.g. most prominently, the use of lethal autonomous weapons systems) and defence activities. Likewise, we also exclude ordinary law-enforcement activities conducted during investigations and prosecution of criminal offences.

Second, when it comes to the regulation of AI, we see a very complicated system of national and supranational legal rules in Europe that impact AI either directly or indirectly. Attached to this is also a complex system of shared competences between organisations such as the European Union (EU) and Council of Europe and their member states, with the Court of Justice of the EU (CJEU) and European Court of Human Rights (ECtHR) playing very prominent roles.

When it comes to regulation of AI, the year 2024 has been very productive for European legislators. First, after several years of

[1] See extensively in Montasari, 2022.

[22] GCHQ, (no date) Pioneering a New National Security: The Ethics of Artificial Intelligence, [Online]. Available at: https://www.gchq.gov.uk/files/GCHQAIPaper.pdf (Accessed: 10 September 2024) p. 4.

[3] Dieu and Montasari, 2022, p. 20; CCBE, 2019, note the lack of a common European concept of "national security" and various national interpretations.

negotiations, the EU AI Act was finally enacted in June 2024.[4] Second, at almost the same time, the Council of Europe's *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CoE AI Convention) was also prepared.[5] With these legal instruments in place, it is possible to argue that Europe is becoming a global leader in the regulation of AI.[6] However, it is open for debate to what extent and how the use of AI specifically for national security purposes will be impacted by these new rules.

To provide a broader overview of the legal rules applicable to the use of AI in the national security domain, this study first seeks to elaborate the possible uses of AI in that domain and the corresponding legal considerations. Second, we analyse which legal sources of the EU and Council of Europe law might prove relevant for regulating AI for national security purposes. In doing so, in addition to the abovementioned AI Act and CoE AI Convention, we consider conditions and safeguards arising under human rights law and the impact of personal data-protection rules. We finish by outlining the most important findings regarding crucial moments of applying legal rules to the use of AI in the context of national security.

2. Possible uses of AI in the national security domain and corresponding legal considerations

The potential of AI in the national security domain seems almost unlimited, but at the same time, even a cursory overview of the relevant literature clearly indicates that it is accompanied by many legal, ethical, and policy considerations.[7] As indicated in section 1, the focus of this study is on legal challenges, specifically those that might arise from the perspective of European law.

However, to identify the legal challenges, it is necessary to first determine the actual uses of AI in national security, and that is not

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act, hereinafter: the AI Act), OJ L, 2024/1689, 12.7.2024.

[5] Council of Europe, 2024.

[6] For a historical overview of AI regulation in Europe, see Jurić, 2024.

[7] See, for instance, Dieu and Montasari, 2022.

necessarily an easy task. There are multiple challenges here. First, problems arise because the notion of national security itself is relatively broad and vague. Therefore, whether some AI is used for national security purposes depends on how we define those purposes. Second, and more importantly, activities of national security authorities are done, almost by default, in closed and relatively secret environments. Although there are typically at least some elements of transparency, they usually do not go as far as to provide very precise elaborations of the technologies used, and there are solid reasons for such an approach. For instance, it was successfully argued during negotiations for the AI Act that registering certain AI systems used by law enforcement in public databases would pose a security risk, affect the capabilities of the authorities, and expose the capabilities of law enforcement to criminals and hostile states.[8] These reasons are emphasised even more in the national security domain. Therefore, while it is known that AI can be very useful in combining and correlating various data sources to create actionable intelligence, it will not be known to the public which data sources are analysed and using which technologies, or this will be described in only very general terms. Therefore, in this study, we describe possible uses of AI in the national security domain in only relatively broad terms based on the findings of other academic works.[9]

The use of AI in national security is sometimes classified into (1) automation of administrative and organisational processes, (2) cybersecurity purposes, and (3) intelligence analysis.[10] Although the benefits of AI in the national security context are usually described in defensive terms, it is necessary to emphasise that the sword cuts both ways. That is, 'state's security can both be strengthened and threatened by the recourse to AI'.[11] For instance, AI can be used to not only facilitate attacks on critical information infrastructure but also prevent such attacks. Looking from an adversarial perspective, AI can very be used well for purposes that compromise national security. The Royal United Services Institute categorises threats in this category into those against (1) digital, (2) political, and (3) physical security.[12]

[8] Palmiotto, 2025.
[9] Babuta, Oswald, and Janjeva, 2020; Benzie and Montasari, 2022; Dieu and Montasari, 2022.
[10] Babuta, Oswald, Janjeva, 2020, pp. 8–16.
[11] Dieu and Montasari, 2022, p. 24.
[12] Babuta, Oswald, and Janjeva, 2020, pp. 16–19.

2.1. Intelligence analysis

Advancements in intelligence analysis seem to be at the top of the expected benefits when it comes to possible uses of AI in the context of national security.[13] The reason for this lies in the fact that national security agencies increasingly face the problem of "information overload."[14] Namely, with improvements in their ability to tap into richer and deeper data sources, they now have the possibility of collecting data on a previously unimaginable scale. However, collecting data on a massive scale is much easier than processing it and turning it into actionable information. Moreover, not only the quantity but also the complexity of data are increasing. This is because data are very frequently found in unstructured and disparate datasets.[15] All information—be it from public registers, communication networks, webpages and other open sources, or various sensor systems—can prove very valuable to national security agencies, especially if it is possible to correlate it. Therefore, what is really at stake is the ability 'to make sense of the data lives of thousands of people in … real time'.[16]

In our opinion, intelligence analysis using AI for national security purposes might trigger personal data considerations and generally raise issues of interference with fundamental rights, particularly privacy. Whether this will be the case depends on whether personal data are being processed (see section 3.4) or whether the data or the manner of their processing fall within the notion of private life (see section 3.3).

2.2. Behavioural analytics

Behavioural analysis might be seen as a subset of intelligence analysis. However, the focus here is on the application of AI to data regarding individuals, with the aim of generating forecasts about human behaviour.[17] Such predictions might include 'threat detection, predicting threats to individuals in public life, identifying potential intelligence sources who may be susceptible to persuasion and predicting potential terrorist activity before it occurs'.[18]

---

[13] See also extensively in Jensen, Whyte, and Cuomo, 2019.
[14] Babuta, Oswald, and Janjeva, 2020, p. 2.
[15] Ibid, p. 11.
[16] Ibid, p. 3.
[17] See extensively in Ferdin et al., 2024.
[18] Babuta, Oswald, and Janjeva, 2020, p. 13.

Such practices can be seen as interfering with many human rights. For instance, they could, under certain conditions, be characterised as profiling in the context of personal data-protection law, and they also give rise to other considerations under that branch of law. Similarly, application of such technologies could be seen as a (particularly serious) interference with fundamental rights to privacy and, in certain scenarios, freedom of expression. Finally, it is particularly due to risks inherent in such practices that they are considered as the ones posing "unacceptable risk" in the context of the AI Act and are therefore prohibited. However, as shall be seen below, that limitation is not applicable to the use of such technologies in the national security context.

2.3. Content moderation

When it comes to threats against political security, one main concern seems to be the use of deepfakes in the form of images or videos, including the ones produced using generative AI.[19] When employed in the context of political campaigns or public debates, such content 'can be used to fuel disinformation, erode trust and compromise democracy'.[20] Generally, although there is a lot of debate about the exact impact of misinformation and disinformation, it is recognised that they can lead to harmful consequences.[21] The same goes for various types of racist or xenophobic content,[22] genocide denial, incitement to extremism or terrorism, etc.

In terms of legal issues, using AI for content moderation purposes will very likely give rise to freedom of expression considerations. Moreover, when moderation is done by analysing the content of electronic communications, it is equally likely that privacy and personal data considerations will arise.

[19] Benzie and Montasari, 2022, pp. 6–11.
[20] Babuta, Oswald, and Janjeva, 2020, p. 18.
[21] Benzie and Montasari, 2022, p. 11.
[22] Around which there is strong international consensus that it should be prohibited. See Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189).

3. How is the use of AI for national security purposes regulated at the level of European law?

Some typical use scenarios for AI in the national security domain have been outlined above. We now turn to the issue of legal regulation of those activities. In doing so, we focus on the regulation at the European level, through legal instruments of the EU and the Council of Europe, and we begin by outlining the scope of application and possible impact of the most relevant and recent EU and Council of Europe sources of AI regulation.

3.1. AI Act

After several years of negotiations, the EU AI Act was finally enacted and entered into force in July 2024. Even though it will take until 2 August 2026[23] for it to become fully operational, it is already starting to impact European AI producers and deployers, as they have approximately two years to bring their activities in compliance with the new law. The AI Act is a complex piece of regulation, seeking to provide for a comprehensive risk-based regulatory framework for AI in the EU. In a nutshell, it does so by categorising AI systems into systems of unacceptable, high, limited, and minimal risk and subjecting them to a specific regulatory regime. Systems posing unacceptable risk are prohibited from use, and most of the regulation covers high-risk systems and general-purpose AI models.

From the perspective of the topic discussed in this study, the key question is to what extent and how the AI Act can impact the use of AI for national security purposes. At first sight, it appears that the answer to this question is rather simple, as activities pertaining to national security are excluded from its scope.[24] Namely, Article 2(3) of the Act prescribes as follows:

> 3. 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

[23] AI Act, Art.113.
[24] For an overview of the legislative process leading to this outcome, see Palmiotto, 2025.

> 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.

While there is some interesting legislative history to this provision in terms of competing proposals,[25] the fact is that the AI Act contains a broad exception for national security, prescribing that it applies 'regardless of the type of entity carrying out those activities'. Such phrasing seems different from the one in other sources of secondary EU law, which usually only stipulate that an act shall not apply to activities falling outside the scope of EU law. According to explanations provided in Recital 24, the purpose of this clarification is to make it explicit that it is irrelevant whether the entity putting into service or using the AI system for national security purposes is a public or private entity. While the reasons for this clarification are not fully elaborated in the AI Act, they might have some connection with the fact that in certain cases related to surveillance of electronic communications, the CJEU has drawn a distinction between activities undertaken for national security purposes based on the type of entity conducting those activities (see section 3.4).

In any case, the intention to provide for a broad exception for using AI in the context of national security was successful. However, this has profound consequences, as it places certain categories of AI completely out of scope of the regulation. This includes AI systems posing what is described as "unacceptable risk," which might play an important role in the context of national security. These include AI systems that[26]

- are used for the evaluation or classification of natural persons or groups of persons based on their social behaviour or known, inferred, or predicted personal or personality characteristics, with the social score leading to certain negative outcomes;
- are used for making risk assessments of natural persons to assess or predict the risk of a natural person committing a criminal offence;

[25] Palmiotto, 2025.
[26] AI Act, Art. 5.

- create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;
- categorise natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation; and
- represent "real-time" remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement.

In such circumstances, we can only conclude that the AI Act provides for no limitation when it comes to the use of AI for national security purposes. This of course comes with an important caveat—supervision of the CJEU. Being the ultimate interpreter of EU law, it is likely that the CJEU will eventually be asked to interpret the scope of exceptions from the AI Act's Article 2(3). If the CJEU's approach in other areas is any indication, it is not impossible that it will seek to interpret that exception narrowly. On the other hand, the AI Act and its drafting process clearly indicate that there was strong consensus about the idea that national security remains the sole responsibility of member states, and therefore the Act should not impact those activities, notwithstanding whether they are done with the assistance of private entities.

3.2. CoE AI Convention

While a comparative analysis of the AI Act and CoE AI Convention is outside the scope of this study, it is important to note that the latter has the potential of a much wider geographical impact for at least two reasons. First and obviously, many European countries that are not member states of the EU will rely on the CoE treaty as their main source of international law for AI regulation. Second, as is the case with many other CoE treaties, the AI Convention is, in line with its Article 31, open for accession to countries that are not parties to the CoE. While it remains to be seen whether the AI Convention will be able to gain traction among non-CoE parties,[27] such a development should in any case be seen as welcome.

As it is an international treaty, the CoE AI Convention creates obligations for its parties and requires them to give effect to its provisions through national law. Majority of its provisions are concerned with principles applicable to AI,[28] including respect of human dignity and

[27] As is, for instance, the case with the Convention on Cybercrime, which with time became truly a global legal instrument for the fight against cybercrime.
[28] CoE AI Convention, Art. 6.

individual autonomy, transparency and oversight, accountability and responsibility, equality and non-discrimination, privacy and personal-data protection, reliability and safe innovation, and remedies.[29] Moreover, the CoE AI Convention calls for its parties to ensure effective procedural guarantees, safeguards, and rights to persons whose fundamental rights and freedoms have been impacted by the use of AI systems.[30] In terms of risk management, which is the main policy in the AI Act, the CoE AI Convention provides for several general rules that need to be developed further in national law.[31]

When it comes to the issue of using AI in the context of national security and corresponding human rights considerations, it is necessary to start from the fact that the CoE AI Convention is intended to be a framework that, as explained in its preamble, means that it 'may be supplemented by further instruments to address specific issues relating to the activities within the lifecycle of artificial intelligence systems'. However, while it is possible that additional instruments impacting the use of AI in national security domain might be agreed upon in the future, that does not seem particularly likely at the moment. This is because it is clear from the approach of the EU and, to a significant extent, of the CoE (see below) that there is generally strong support for the idea of excluding the use of AI for national security purposes from the scope of regulatory instruments.

Regarding the issue of human rights, the CoE AI Convention recognises the challenges of AI very clearly. Therefore, it specifically mentions in its Preamble that activities based on AI may 'undermine human dignity and individual autonomy, human rights, democracy and the rule of law', with particular emphasis on issues of discrimination and creation or aggravation of inequalities, including those against women and persons in vulnerable situations. Maybe even more relevant for the topic discussed in this study is the threat of using AI for repressive purposes in violation of human rights law, including through 'arbitrary or unlawful surveillance and censorship practices that erode privacy and individual autonomy'.

However, when it comes to the applicability of the CoE AI Convention in the domain of national security, Article 3(2) clearly prescribes that

[29] Ibid, Arts. 7–14.
[30] Ibid, Art. 15.
[31] Ibid, Art. 16.

> A Party shall not be required to apply this Convention to activities within the lifecycle of artificial intelligence systems related to the protection of its national security interests, with the understanding that such activities are conducted in a manner consistent with applicable international law, including international human rights law obligations, and with respect for its democratic institutions and processes.

Therefore, parties to the CoE AI Convention are not required, but also not precluded, to apply the convention to their national security activities. While the phrase stating that they should not be precluded from doing so opens the door for application if a particular state so desires, it is not very realistic that countries would follow such an approach. Moreover, pursuant to elaborations in the Explanatory Report, this exception applies 'regardless of the type of entities carrying out the corresponding activities'. It therefore follows that the CoE AI Convention generally pursues the same approach as the one taken in the AI Act when it comes to the regulation of private entities acting in the domain of national security.

Article 3(2) might seem puzzling in part where, in the context of the exception for national security purposes, reference is made to the 'understanding that such activities are conducted in a manner consistent with applicable international law'. However, in our opinion, this signifies nothing more than what is stated in the Explanatory Report—that national security activities, while excluded from the CoE AI Convention, are nevertheless subject to the European Convention on Human Rights (ECHR; and other applicable international treaties, including other regional human rights treaties for parties that are not member states of the Council of Europe).

Moreover, the Explanatory Report makes it clear that dual-use AI systems are generally within the scope of the CoE AI Convention when they are 'intended to be used for other purposes not related to the protection of the Parties' national security interests and are within the Party's obligations under Article 3'. Likewise, it is made explicit that

> … all regular law enforcement activities for the prevention, detection, investigation, and prosecution of crimes, including threats to public security, also remain within the scope of the

> Framework Convention if and insofar as the national security interests of the Parties are not at stake.

To sum up, although there are many differences between the EU approach in the AI Act and the CoE's AI Convention, both pursue the approach of non-applicability to national security situations. This brings us to a question: Which legal standards then remain relevant in such circumstances? In our opinion, it is necessary to first consider the general sources of European human rights law. Among these, the ECHR[32] has the most important role.

3.3. ECHR

The proposal that human rights considerations are relevant in the context of national security is not controversial. To begin with, there can be no dispute that protection provided under the ECHR extends to the area of national security. In the ECHR, this follows clearly from its Articles 8, 10, and 11, all of which provide in their respective paragraphs 2 that the respective rights can be restricted in the pursuance of, *inter alia*, national security aims. Moreover, applicability of the ECHR to national security situations was confirmed by the ECtHR in numerous cases where that court considered national security needs as a legitimate aim for restricting fundamental human rights.[33] Therefore, we do not see any reason for concluding that the use of an AI system for national security purposes would somehow be outside the scope of the ECHR. On the contrary, applicability of the ECHR to such situations is reinforced by the CoE AI Convention, which in Article 3(2) refers to the understanding that when using AI for national security purposes, states must act 'in a manner consistent with applicable international law, including international human rights law obligations, and with respect for its democratic institutions and processes'.

Currently, there are no cases in which the ECtHR would discuss the use of AI in the context of national security. However, when that becomes the case, it is bound to happen in a legal context different from the one established by the AI Act or CoE AI Convention. Namely, while the AI Act (and national legislation that will implement the CoE AI Convention) are regulatory legal instruments, the ECHR is a human rights tool. Looking from the perspective of the ECHR, AI is nothing more than another

[32] Council of Europe, 1950.
[33] For an overview of ECtHR's cases in the domain of national security, see ECtHR, 2013.

technology: It gives rise to human rights considerations only if and when it impacts one of the fundamental human rights recognised in the ECHR.

When analysing possible violations of the rights protected under Articles 8 and 10 of the ECHR, the ECtHR pursues the approach in which the following is analysed:

1) Whether there has been interference with a fundamental right protected under the relevant article of the ECHR
2) Whether the interference is prescribed by law
3) Whether the interference pursues a legitimate aim
4) Whether the interference is necessary in a democratic society

The catalogue of fundamental human rights and freedoms that can be impacted using AI is very broad. For instance, it is not unimaginable that the rights to life, fair trial, freedom of religion or association, free elections, and equality and non-discrimination might be, in certain cases, interfered with through the use of AI systems.[34] However, in the context of national security, we consider that the most likely challenges will be in relation to the protection of private and family life, home and correspondence (Article 8 of the ECHR), and freedom of expression (Article 10 of the ECHR). Although, depending on the specifics of the case, only one or both of these rights can be interfered with, the approach in either situation is generally the same and in line with the criteria mentioned above.

Recognising that national security is an accepted legitimate aim under the ECHR, the key debate will, in our opinion, be about clarity and foreseeability of the legislation governing the use of AI for national security purposes and the necessity of doing so.

In our opinion, the approach pursued by the ECtHR is sufficiently flexible to provide an adequate framework for interferences caused using AI as well. Although AI is a technology and therefore not in question, its specific characteristics are likely to be considered by the court, which has previously emphasised issues raised by new or intrusive technologies. For instance, in *S. and Marper v. United Kingdom*, the court concluded, in relation to the use of modern scientific techniques in the law enforcement sector, that

> … the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any

[34] Dieu and Montasari, 2022, pp. 21–29.

> cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.[35]

Moreover, any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.[36]

In addition, we can generally observe that the ECtHR does not struggle with applying the ECHR to new technologies, as it was able to address challenges posed by various new technologies in cases concerning the use of gross domestic product trackers (*Uzun v. Germany*[37] and *Ben Faiza v. France*),[38] authorities using the "surveillance database" that collects information about persons' movements by train or air (*Shimovolos v. Russia*),[39] use of facial-recognition technologies (*Glukhin v. Russia*),[40] secret surveillance (*Szabó and Vissy v. Hungary*),[41] etc.

In addition to the abovementioned general standards, there are several specific ones in the case law of the ECtHR that might prove valuable for addressing AI-related cases in the context of national security.

First, the ECtHR has a very permissive approach in cases regarding secret surveillance when it comes to establishing the applicant's victim status and the existence of interference with a fundamental right. Namely, the challenge here is that, due to secrecy of measures at the national level, applicants sometimes have difficulties in proving that they have been subject to some form of surveillance. To address these challenges, the ECtHR has developed a specific test that, if satisfied, can enable applicants to have their case heard without demonstrating with certainty that they have been victims of illegality.[42] Since activities in the domain of national

---

[35] *Case of S. and Marper v. United Kingdom* App. Nos. 30562/04 and 30566/04, 04 December 2008, para 112.
[36] Ibid.
[37] *Case of Uzun v. Germany* App. No. 35623/05, 2 September 2010.
[38] *Case of Ben Faiza v. France* App. No. 31446/12, 08 February 2018.
[39] *Case of Shimovolos v. Russia* App. No. 30194/09, 21 June 2011.
[40] *Case of Glukhin v. Russia* App. No. 11519/20, 04 October 2023.
[41] *Case of Szabó and Vissy v. Hungary* App. No. 37138/14, 06 June 2016.
[42] As explained in *Zakharov v Russia*, it is necessary to consider:
1) the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, and
2) availability of remedies at the national level, with the understanding that the degree of scrutiny of the ECtHR depends on the effectiveness of such remedies.

security are conducted in secrecy almost by default, criteria such as this one might also prove useful in future AI-related cases.

Second, in surveillance cases, the ECtHR found it problematic when authorities had direct access to communication data (i.e. when access was possible without further assistance from the service providers). According to the court, such systems are particularly prone to abuse, and 'the need for safeguards against arbitrariness and abuse appears therefore to be particularly great'.[43] Similarly, issues of national security authorities' direct access to various sources of data, with the aim of cross-referencing and intelligence analysis, should be analysed with these considerations in mind. Dangers of abuse are particularly relevant here, as the use of AI could greatly enhance the possibility of reviewing and analysing communication data.

Third, when it comes to the activities of national security agencies, probably the most important safeguard is an effective oversight mechanism. Security services have always had, and continue to have, fundamental importance for functioning of the state. All European countries have these institutions and task them with various duties, from intelligence collection to protection of the national security, economic well-being, and other critical interest of the state. However, since these services, due to the nature of their work, mostly operate in secret, it is also widely recognised in Europe that their proper oversight is fundamental to ensuring that these institutions both contribute to the protection of the populations they serve and respect the rule of law and human rights.[44] National practices of European countries regarding oversight of these services vary greatly, but some important elements have been identified by the ECtHR. As repeatedly stated by the court, the most important factors in this context are the (1) the independence of the supervisory authorities, their competences, and their powers and (2) the possibility of effective public scrutiny of these authorities' work.[45] In addition to the ECtHR, very useful guidance regarding the effectiveness of oversight arrangements is provided by the Venice Commission.[46]

See *Case of Zakharov v Russia* App. No. 47143/06, 04 December 2015, paras. 170–172.

[43] *Case of Zakharov v Russia* App. No. 47143/06, 04 December 2015, paras. 268–271.

[44] Commissioner for Human Rights, 2015, p. 5.

[45] See, for instance, *Case of Ekimdzhiev v Bulgaria* App. No. 70078/12, 11 April 2022, paras. 334–347.

[46] Venice Commission, 2015.

To conclude this section, we are of the strong opinion that the ECHR remains as relevant as always, and it provides a very adequate tool for addressing human rights issues posed through the use of AI in the national security domain.

3.4. Personal data-protection law

As elaborated in section 2, be it intelligence analysis, behavioural analytics, detection of cybersecurity threats, or content moderation, AI will be about processing data. For that reason, it is impossible to outline the legal framework for the use of AI without considering the legal framework governing the use of data. While the European law might not address AI as a technology in the context of national security, it does not necessarily follow that the situation is the same regarding the regulation of data.

When it comes to data regulation, there are multiple sources of the EU and Council of Europe law that might be relevant. However, initially, it is important to start with a very basic but crucial distinction—between personal and non-personal data. Namely, what the EU and CoE legal frameworks regulate is personal data. Non-personal data are regulated only minimally in the EU's legal order and not at all in the CoE's.

In essence, data processing by AI systems for national security purposes will come into the scope of personal data protection law, provided that the following conditions are fulfilled:

1. The relevant source of personal data-protection law is applicable to processing of data in national security situations.
2. Data being processed are "personal."
3. Personal data are being "processed" in a manner that falls within the scope of relevant source of law.

3.4.1. Relevant sources of personal data-protection law and their applicability to national security situations

In the context of the Council of Europe's legal framework, the relevant source of personal data-protection law is the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108).[47] It is also the first comprehensive international legal instrument for personal data protection on the European continent, and for that reason alone, it deserves to be mentioned first. However, looking from

[47] Council of Europe, 1981.

the perspective of enforceability, there are important differences between that convention and the EU's General Data Protection Regulation (GDPR; see below), with the most relevant one being that the GDPR is a regulation and is therefore directly applicable in all EU member states. On the other hand, Convention 108 is an international treaty that needs to be transposed into national legislation to become effective. In terms of substance, legal solutions from Convention 108 are in most part in harmony with the GDPR. Therefore, while Convention 108 is extremely important in relations with third countries, its relevance for the EU member states is partially reduced, as the GDPR will be the one applied in practice. On the other hand, for non-EU member states, Convention 108 remains particularly important as currently the only functioning data-protection mechanism with global aspirations. Considering that both the CoE AI Convention and Convention 108 are open for accession to countries that are not parties of the Council of Europe, the later convention can also serve as an important data-protection standard in the context of the use of AI.

When it comes to its scope of application, Convention 108 does not contain an exception for national security purposes, but its state parties have the right to limit the application of certain provisions when such limitation is necessary for, *inter alia*, national security purposes. Such limitations can impact the application of data-protection principles, notification obligations, transparency obligations, data subjects' rights, some provisions on transborder flows of data, and powers of supervisory authorities.[48] However, even where such exceptions are made, Convention 108 explicitly requires that personal data-processing activities undertaken for national security purposes must be subject to independent and effective review and supervision, as prescribed by the domestic law of every party.[49]

On the side of the EU law, there are several sources of EU law applicable to the processing of personal data. However, for the purpose of this study, it is not necessary to provide a comprehensive analysis of the whole EU acquis in this sector. Rather, we consider it necessary to focus on the following sources:

[48] Council of Europe, 1981, Article 11.
[49] Ibid.

- The *GDPR*,[50] which is generally applicable to all personal data-processing situations, as well as several sources of sectoral legislation, including the
- *Directive on Privacy and Electronic Communications* (e-Privacy Directive)[51] and
- *Law Enforcement Directive* (LED).[52]

As mentioned above, the first key question here is whether the abovementioned sources are applicable to processing of data in the context of national security. It appears on first sight that this is not the case. Namely, the GDPR prescribes in Article 2(2)(a) that it does not apply 'in the course of an activity which falls outside the scope of Union law', which is of course related to Article 4(2) of the Treaty on EU, and which, to remove any doubt and pursuant to Recital 16, includes 'activities concerning national security'. However, this relatively clear provision is complicated by the fact that Article 23 of the GDPR allows member states to restrict by way of a legislative measure the scope of the personal data-protection principles, obligations of data controllers, and rights of data subjects under certain conditions and for the purposes of, *inter alia*, national security.[53] As shall be seen from the explanations below, the relationship between these provisions gives some ground to arguments that activities pertaining to national security are not *fully* excluded from the scope of the GDPR, as then there would be no need to create additional room for the exceptions in Article 23.

[50] 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), OJ L 119, 4.5.2016.

[51] 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), OJ L 201, 31.7.2002, pp. 37–47.

[52] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp. 89–131.

[53] Pursuant to Article 23 of the GDPR, every such restriction must (1) respect the essence of the fundamental rights and freedoms and (2) be a necessary and proportionate measure in a democratic society to safeguard one of the legitimate aims listed therein.

Essentially, the same structure is found in the context of the LED, with its Article 2(3)(a) excluding processing of personal data 'in the course of an activity which falls outside the scope of Union law'[54]; at the same time, some specific national security exceptions are provided in Articles 13, 15, and 16. The same goes for the e-Privacy Directive, which contains a general national security exception in Article 1(3). But there is an additional exception in Article 15 that allows member states to restrict some rights protected under the directive when pursing, *inter alia*, national security objectives. Article 15 therefore brings into question Article 1(3), because if national security situations would be fully excluded on the basis of that Article, why would Article 15 be necessary? In such circumstances, the CJEU had to interpret the scope of the national security exception, which was done in a relatively narrow manner. Namely, the position of the CJEU has been 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.[55]

In other words, the mere fact that a decision concerns state security cannot result in EU law being inapplicable.[56] On these grounds, the CJEU

[54] However, the interesting thing with this exception is that a slightly different explanation is provided in that directive's Recital 14, which stipulates that

> Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security… [and] activities of agencies or units dealing with national security issues … should not be considered to be activities falling within the scope of this Directive.

Namely, it could be inferred from this recital that the intention of the drafters was broader, namely, to exclude from the scope all activities of agencies or units dealing with national security. Still, it appears that this distinction did not result in any different interpretations regarding the scope of the e-Privacy Directive, compared to other sources of personal data-protection law.

[55] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others v. Premier ministre and Others*, 06 October 2020, para 99, and the cases cited there. See also Klamert, Kellerbauer, and Tomkin, 2019, p. 45.

[56] C-300/11, *ZZ v. Secretary of State for the Home Department*, 04 June 2013, para 38.

concluded in cases such as *Tele 2 and Watson*,[57] *La Quadrature du Net* (quoted above), and others that the processing of personal data for, *inter alia*, purposes of national security falls within the scope of the e-Privacy Directive.

This leads us to question how it is possible to differentiate between cases of processing of personal data for national security purposes, which would be covered by general exceptions such as those in Article 2(2)(a) of the GDPR and Article 1(3) of the e-Privacy Directive, and those which, while somehow related to national security, are still within the scope of personal data-protection rules. One important criterion developed in the case law of the CJEU regarding surveillance of electronic communications is whether personal data needed for national security purposes are being processed with or without the involvement of private parties. Namely, we see from the cases cited above that when private parties (e.g. service providers) are required to undertake certain activities in the context of national security activities, the e-Privacy Directive remains applicable. On the other hand, situations in which member states directly implement measures that derogate from personal data-protection rules, without imposing processing obligations on private parties, should according to the CJEU remain outside the scope of EU personal data-protection rules.[58] In *La Quadrature du Net and others*, the CJEU (even though it was not directly relevant for the case) made it explicit that the same criteria would be applicable in the context of the GDPR, arguing in the context of exceptions that the GDPR should not 'apply to processing operations carried out "by competent authorities"…', but 'that the processing of personal data carried out by individuals for those same purposes falls within the scope of that regulation'.[59]

Coming back to the processing activities relevant from the perspective of national security, the abovementioned standards could be relevant in the context of activities of security agencies. Provided that the CJEU maintains its approach of differentiating between activities undertaken by national authorities themselves and those imposing obligations on other parties, it

[57] Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 21 December 2016, paras. 65–81.
[58] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others v. Premier ministre and Others*, 06 October 2020, para. 103.
[59] Ibid., para. 102.

would follow that at least in cases where security authorities are "tapping into" data sources held or operated by private entities, the EU personal data-protection rules would apply. On the other hand, those rules would not apply in cases where authorities collect and process data fully by themselves. The challenge, from the national security perspective, is that in many cases, data held or collected at the point of private entities will be relevant for national security authorities. For instance, collection of information from electronic communications networks, from systems of essential or important entities that are subject to private law in the context of cybersecurity, or even from open sources such as the internet would come within the scope of EU personal data-protection rules. The situation might be more complicated with data held by other public authorities, such as those contained in public registries, but if the exception is interpreted narrowly, it would not come as a surprise that tapping into these sources is subject to personal data-protection law.

3.4.2. Notion of personal data and processing of personal data

Having concluded that activities in the domain of national security can, in many cases, be subject to EU data-protection rules, the crucial next element for the applicability of those rules is the notion of personal data. Pursuant to Article 4(a) of the GDPR,[60] personal data are 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.

The definition in Convention 108 is compatible with this one; therefore, we can say that the concept of personal data in the convention corresponds to the one in the GDPR and other sources of EU law.

By simplifying this considerably, it can be said that personal data encompass (1) any information that is (2) related to (3) an identified or

[60] A substantially identical definition is found in Art. 3(1) of the Law Enforcement Directive.

identifiable (4) natural person.[61] All of these elements have been extensively analysed in academic works and case law, so there is no need to repeat here what is already elaborated elsewhere. It is sufficient to say that any information that does not have to be private or sensitive in any standard meaning of those words will be considered "personal" if it "relates" to a natural person. As the CJEU explained in the *Nowak* case, the condition of "relates to" is satisfied where the 'information, by reason of its content, purpose or effect, is linked to a particular person'.[62] It appears that in providing this explanation, the CJEU also considered the earlier opinion of WP29, pursuant to which information is personal data if (1) it is 'about a person' or (2) if it is processed with a purpose to 'evaluate, treat in a certain way or influence the status or behaviour of an individual' or (3) if its processing 'is likely to have an impact on a certain person's rights and interests'; this impact does not have to be major, as it is sufficient that the individual may be treated differently from other persons as a result of the processing of data.[63] Putting these criteria in the context of national security operations, it seems reasonable to conclude that they will frequently be satisfied, as such operations are very likely to seek to evaluate individuals in some way or have an impact on a person's rights or interests. In such circumstances, it is reasonable to anticipate that the EU law on personal data protection might apply generally.

Once it is concluded that an information is personal data, the relevant law will apply further under the condition that such data are processed. The notion of "processing" is even broader than the one of "personal data," so that it includes 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means' (GDPR).[64] The definition of processing in Convention 108 is substantially the same.[65] In theory, there is one small exception regarding the type of processing, namely when it is done on unstructured data and by non-automatic means.[66] However, since we are talking about the processing by means of AI, such an exception is fully inapplicable in this context.

[61] Article 29 Working Party, 2007.
[62] C-434/16, *Peter Nowak v Data Protection Commissioner*, 20 December 2017, para. 35.
[63] Article 29 Working Party, 2007, pp. 10–11.
[64] GDPR, Art. 4(2).
[65] Council of Europe, 1981, Art. 2(b).
[66] GDPR, Art. 2(1).

3.4.3. How might the personal data-protection law impact the use of AI systems in the national security domain?

Provided that the conditions elaborated above are satisfied, the EU personal data-protection rules might become applicable to data processing in the context of national security. What consequences that might bring will of course depend on the particular elements of each specific case. However, in general, the following seems especially relevant.

First, all personal data processing must have a legal basis under Article 6(1) of the GDPR. In the context of national security activities, that legal basis should come in the form of legislation specifically authorising certain forms of data processing. Likewise, any restrictions that can be imposed for national security purposes, based on Article 23, would also have to be established by a legislative measure and, at the same time, satisfy the principle of proportionality.

Second, data-protection principles such as data minimisation, storage limitation, and purpose limitation (see Article 5 of the GDPR) would also apply to processing in the context of national security. This is provided that their application is not excluded based on national legislation in line with Article 23 and is subject to the standards and requirements mentioned above.

Third, data subjects' rights, unless derogated by national law, would become enforceable. For instance, individual citizens could try to enforce their right to access their personal data (Article 15 of the GDPR) or exercise their rights in relation to automated individual decision-making, including profiling (Article 22).

Fourth, data-processing operations done for the purpose of national security would come under the supervision of national data-protection authorities, in addition to any other oversight mechanism that might exist under national law.

The situation on the side of CoE law is slightly more complicated when it comes to human rights protection for personal data.

The important caveat here is that while Convention 108 corresponds to the GDPR, the ECHR does not correspond fully to these sources of data-protection law. Namely, the right to personal data protection is not an autonomous right under the ECHR. In the context of the ECHR, personal data processing can, under certain conditions, be protected under Article 8, which deals with the more general right to privacy (or precisely, to the

protection of personal and family life, home, and correspondence). On the other hand, the Charter of Fundamental Rights of the EU provides in its Article 8 for a standalone right to personal data protection, together with some explicit requirements regarding the scope of protection.[67]

Moreover, the ECtHR does not have the power to supervise the application of Convention 108 directly, while the CJEU has the power to interpret the GDRP and sectoral EU data-protection legislation. The ECtHR therefore applies only the ECHR and, where appropriate, interprets it in light of Convention 108.

Therefore, the ECtHR will afford protection in cases concerning personal data when it finds that there is a case under Article 8 that goes beyond simply verifying whether data are "personal" in the sense of Article 2(a) of Convention 108. While the ECtHR has in many cases extended the protection provided under Article 8 of the ECHR to personal data-processing situations, such an outcome is not inevitable. In other words, the mere fact that personal data are being processed does not mean, per se, that Article 8 of the ECHR has been interfered with.

In its case law, the ECtHR found in many cases that certain categories of data or the manner of their processing merit protection under Article 8.

For instance, in *Rotaru v Romania*, the ECtHR reasoned that information about persons' life merits protection under Article 8 'when systematically collected and stored in a file held by agents of the State'.[68] On the contrary, in *Mehmedovic v. Switzerland*,[69] the ECtHR did not consider that Article 8 has been interfered with, even though personal data have been processed, because the sparse information concerning the applicant, gathered coincidentally and without relevance to the investigation, in no way constituted systematic or permanent gathering of data.[70]

---

[67] Art. 8 of the Charter of Fundamental Rights of the EU reads as follows:
Protection of personal data
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

[68] *Case of Rotaru v. Romania* App. No. 28341/95, 04 May 2000, para. 44.

[69] *Case of Mehmedovic v. Switzerland*, App. No. 17331/11, 17 January 2019.

[70] Ibid., para 18.

In numerous cases, the ECtHR found that a specific category of data merits protection, such as data about gender identification, sexual orientation and sexual life (*Drelon v. France*),[71] processing of global positioning system data (*Uzun v Germany*),[72] and use of geolocation devices installed on a car and obtaining of geolocation data from telecommunication services providers (*Ben Faiza c. France*).[73] There is abundance of ECtHR case law in which various methods of obtaining data through surveillance measures gave rise to Article 8 considerations.[74] In the very important case of *Glukhin v Russia* (2023), the ECtHR found that processing of biometric personal data using facial-recognition technology interferes with Article 8.[75] Likewise, in *Shimovolos v Russia*, the ECtHR found that collecting information about a person's movements by train or air through the so-called Surveillance Database also interferes with Article 8 of the ECHR.[76] In *Catt v the United Kingdom*,[77] the court reached the same conclusion regarding the collection and retention of the applicant's personal data in the co-called Extremism Database.

Admittedly, the number of cases in which the ECtHR explicitly declined to afford Article 8 protection to personal data-processing situations is rather small. However, it does follow from the court's case law that something additional is needed, in addition to personal data being processed, to trigger the application of Article 8. Therefore, as the ECtHR explained in *S. and Marper v the UK*, 'the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8'. However, it is important to note here that it is processing of 'data relating to the private life' and not 'personal data' that trigger the application of Article 8, and these concepts are not synonymous. Therefore, the court went on to explain that

> in determining whether the personal information retained by the authorities involves any of the private-life aspects …, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature

[71] *Case of Drelon v. France*, App. Nos. 3153/16 and 27758/18, 08 December 2022.
[72] *Case of Uzun v. Germany* App. No. 35623/05, 2 September 2010.
[73] *Case of Ben Faiza v. France* App. No. 31446/12, 08 February 2018.
[74] See ECHR, 2024.
[75] *Case of Glukhin v. Russia* App. No. 11519/20, 04 October 2023.
[76] *Case of Shimovolos v. Russia* App. No. 30194/09, 21 June 2011, paras. 64–66.
[77] *Case of Catt v the United* Kingdom App. No. 43514/15, 24 April 2019.

> of the records, the way in which these records are used and processed and the results that may be obtained.[78]

However, with all these reservations, we consider it highly unlikely that the processing of personal data using AI for national security purposes would be characterised by the ECtHR as something that does not interfere with the right protected under Article 8 or 10 of the ECHR.

4. Conclusions

While the possible uses of AI in the national security domain seem almost unlimited, possibly the greatest impact is expected regarding the data processing for intelligence analysis and analytics. Considering how those activities might be subject to legal limitations, the following picture emerges.

To begin, impacts of the AI Act and CoE AI Convention are likely to be very limited when AI is used for national security purposes, since both documents seek to exclude their application to national security matters in a very broad manner. The most important factor here is that both the convention and regulation seek to extend the exception to not only public authorities but also private entities undertaking certain activities in the national security domain. In such circumstances, we see two major legal frameworks that might prove influential.

First, it is to be anticipated that the ECHR will play a major role in ensuring that the uses of AI for national security purposes remain in line with the requirements of democratic society. As elaborated in section 2, an overview of the existing ECtHR case law indicates that the court does not have difficulty in applying the convention's rules for emerging technologies. Moreover, there is abundance of relevant legal standards from the existing case law, most importantly in cases dealing with surveillance and personal data processing, which might be influential if applied by analogy to the use of AI systems.

Second, in the context of EU law, the most important conditions and safeguards related to the use of AI for national security purposes might come through the application of personal data-protection rules. Our research indicates that while there is lot of uncertainty when it comes to the

[78] *Case of S. and Marper v. United Kingdom* App. Nos. 30562/04 and 30566/04, 04 December 2008, para. 67.

application of personal-data rules to national security situations, existing case law indicates that the application of those rules is not fully excluded. On the contrary, it is to be expected that personal data-protection law might prove to be very effective, at least when private entities are involved in data-processing operations.

Bibliography

[1] Benzie, A., Montasari, R. (2022) 'Artificial Intelligence and the Spread of Mis- and Disinformation', in Montasari, R. (ed) *Artificial Intelligence and National Security.* Springer, Cham, pp. pp. 1-18; https://doi.org/10.1007/978-3-031-06709-9_1.

[2] Dieu, O., Montasari, R. (2022) 'How States' Recourse to Artificial Intelligence for National Security Purposes Threatens Our Most Fundamental Rights', in Montasari, R. (ed) *Artificial Intelligence and National Security.* Springer, Cham, pp. 19-45; https://doi.org/10.1007/978-3-031-06709-9_2.

[3] Ferdin, J. J., F., Regin, R., Chinnusamy, K., Suman Rajest, S., Paramasivan, P. (eds.) (2024) *Explainable AI Applications for Human Behavior Analysis*. Hershey, PA: IGI Global Scientific Publishing, https://doi.org/10.4018/979-8-3693-1355-8.

[4] Jurić, M. (2024) 'Legal Aspects of Military and Defence Applications of Artificial Intelligence Within the European Union', in Zombory, K., Szilágyi, J. E. (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*, Miskolc-Budapest: Central European Academic Publishing, pp. 395-436.

[5] Jensen, B., Whyte, C., Cuomo, S. (2019) Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence, *International Studies Review*, 22(3), pp. 526–550.

[6] Klamert, M., Kellerbauer, M., Tomkin, J. (2019) *Commentary on the EU: Treaties and the Charter of Fundamental Rights*. 2nd Ed, Oxford: Packmm.

[7] Montasari, R. (ed) (2022) *Artificial Intelligence and national security*. Springer, Cham; https://doi.org/10.1007/978-3-031-06709-9.

[8] Palmiotto, F. (2025) The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation. *European Journal of Risk Regulation*, 1–24; https://doi.org/10.1017/err.2024.97.

[9] Szappanyos, M. (2023) 'Artificial Intelligence: Is the European Court of Human Rights Prepared?', *Acta Humana – Emberi Jogi Közlemények*, 11(1), pp. 93–110; https://doi.org/10.32566/ah.2023.1.6.

[10] Article 29 Working Party (2007) *Opinion 4/2007 on the concept of personal data*, [Online]. Available at: https://ec.europa.eu/justice/article-29/documentation (Accessed: 10 September 2024).

[11] Babuta, A., Oswald, M. Janjeva, A. (2020) *Artificial Intelligence and UK National Security: Policy Considerations. RUSI*, [Online]. Available at: https://static.rusi.org/ai-national-security-final-web-version.pdf (Accessed: 10 September 2024).

[12] Council of Bars & Law Societies of Europe (CCBE) (2019) *Recommendations on the protection of fundamental rights in the context of 'national security'*, [Online] Available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf (Accessed: 10 September 2024).

[13] Council of Europe (1950) *Convention for the Protection of Human Rights and Fundamental Freedoms*, [Online]. Available at: https://www.echr.coe.int/documents/d/echr/convention_ENG (Accessed: 10 September 2024).

[14] Council of Europe (1981) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, [Online]. Available at: https://rm.coe.int/1680078b37 (Accessed: 10 September 2024).

[15] Council of Europe Commissioner for Human Rights (2015) *Democratic and effective oversight of national security services*, [Online]. Available at: https://rm.coe.int/1680487770 (Accessed: 10 September 2024).

[16] Council of Europe (2024) *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law,* [Online]. Available at: https://rm.coe.int/1680afae3c (Accessed: 5 March 2025).

[17] ECHR (2024) *Personal data protection* [Online]. Available at: https://prd-echr.coe.int/documents/d/echr/FS_Data_ENG (Accessed: 5 March 2025).

[18] European Court of Human Rights (ECtHR) (2013) *National security and European case-law*, [Online]. Available at: https://rm.coe.int/168067d214 (Accessed: 10 September 2024)

[19] Taddeo, M., Ziosi, M., Tsamados, A., Gilli, L., Kurapati, S. (2022) *Artificial Intelligence for National Security: The Predictability Problem*, *[*Online]. Available at: https://cetas.turing.ac.uk/sites/default/files/2022-09/research_report_ai_predictability_problem_vfinal_3.pdf (Accessed: 10 September 2024).

[20] Venice Commission (2015) *Report on the Democratic Oversight of Security Services*, [Online]. Available at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e (Accessed: 10 September 2024).