Artificial Intelligence (AI) Systems Not Covered by the AI Regulation

Constantino, J.E.; van der Linden, Tina

DOI
10.1007/978-3-031-98406-8_9

Publication date
2025

Document Version
Final published version

Published in
The European Artificial Intelligence Act

Artificial Intelligence (AI) Systems Not Covered by the AI Regulation

Jorge Constantino and Tina van der Linden

Contents

1 Introduction 212
2 National Security, Military & International Cooperation 213
2.1 National Security and Intelligence Agencies 213
2.2 Military Purposes 216
2.3 Foreign Authorities and International Organisations 219
3 Society 222
3.1 Transportation 222
3.2 Personal Non-professional Activity 225
3.3 Research 226
3.4 Free and Open Source Licences 227
4 Conclusion 229
References 232

Abstract The AI Act brands itself as the first-ever legislation that uniformly regulates the use of AI systems in European society across all sectors. However, this branding from the AI Act appears not to be one hundred per cent accurate. Rather, the AI Act has brought exemptions to its 'uniformed' rules on the use of AI systems in the European Union. This chapter analyses the exemptions of certain AI systems from the EU AI Act, particularly focusing on national security, military, interna-

J. Constantino
TU Delft, Faculty of Technology, Policy and Management, Delft, The Netherlands

T. van der Linden (✉)
Hogeschool Utrecht, Utrecht, The Netherlands
e-mail: tina.vanderlinden@hu.nl

V. L. Raposo (ed.), *The European Artificial Intelligence Act*, Law, Governance and Technology Series 78, https://doi.org/10.1007/978-3-031-98406-8_9

tional cooperation, research, and personal use, and discusses the implications for fundamental rights and legal accountability.

1 Introduction

For various reasons, the AI Act does not cover some categories of Artificial Intelligence (AI) systems. In this chapter, we provide an overview of these categories of AI systems and mention one or more examples of each of them. For each category, we discuss the reason why they are not covered, and review other rules that might apply to them. Next, studying the legal doctrine, we investigate if these AI systems pose any risks to fundamental rights and European values, and whether the rules that do apply to them sufficiently address such risks.

As we have no less than seven categories of AI systems to discuss, and the topic is still quite new, we have chosen to reflect on the limitations of the AI Act and the challenges that these limitations may represent to a democratic society. By our legal analysis, we hope to contribute to the legal doctrine and other scholars interested in the European AI Act's legal, societal, and technological impact. This chapter starts by looking into the exemptions for AI systems used for national security, military, and international cooperation in the context of fighting crime. AI systems used in the context of national security are excluded from the domain of the AI Act to avoid interference with Member States in matters of national security. Moreover, excluding military AI systems may be based on the specificities of the Member States' and the common Union defence policies found under the Treaty of the European Union and public international law. Lastly, AI systems deployed in the context of international arrangements with foreign authorities and international organisations are also excluded to promote cooperation in exchanging information and evidence to combat crime.

This chapter also analyses AI systems used or deployed in society, such as AI systems in the context of transportation, personal non-professional activities, research, and under free and open source licences. The AI Act is ambiguous regarding excluding AI systems in transportation. We argue that, in essence, transportation is not an exemption but rather a different way of putting the requirements for these high-risk AI systems in dedicated legislation that is already in place. We note that AI systems for personal non-professional activity are not covered by the AI Act provided the deployer is a natural person. However, these AI systems may (depending on their functionality) be covered by other rules in order to safeguard fundamental rights at stake. To support innovation, AI used in the research context is also excluded from the scope of the AI Act. Similarly, AI systems used under 'free and open source licences' are excluded to avoid hampering innovation. However, it is not really clear what is meant by the term 'free and open source licences'. In both cases, we note that these exemptions pose further challenges, loopholes, and legal uncertainty because the exemptions may be misused. We offer conclusions

outlining that while the introduction of AI is good for society's development, the AI Act may have missed the opportunity to present a coherent approach to minimising the risks of AI in critical aspects where fundamental rights are at stake due to current loopholes (intentionally or unintentionally) provided by the AI Act.

2 National Security, Military & International Cooperation

2.1 National Security and Intelligence Agencies

In this section, we note that AI systems used within the context of national security, military, and international cooperation are part of the exempted categories as expressly stated in Art. 2(3) AI Act, establishing that this legal instrument *'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.*'

The AI Act has justified the exclusion of AI systems for national security purposes on the basis that national security '*remains the sole responsibility of Member States in accordance with Article 4(2) TEU [Treaty of the European Union] and by the specific nature and operational needs of national security activities and specific national rules applicable to those activities*'.[1] The background provided by the European legislator suggests that the AI Act is mindful not to intrude in matters of national security, military, and international cooperation in the context of fighting crime and threats to the stability of the region, democracy, and European values. It appears that the European Commission tried to avoid legal challenges by Member States regarding the lack of competence of Union law in matters of national security. However, in *La Quadrature du Net and Others v Premier ministre and Others*,[2] a court case involving telecommunication service providers storing and processing personal data (allegedly) to comply with national security purposes, the CJEU ruled that the TEU does not render 'EU law [such as the AI Act] inapplicable'.[3] Thus, the ruling from the CJEU may serve as an argument that although State Members have the right to establish their own national security frameworks, the TEU does not require the AI Act to exempt AI systems in the context of national security or defence.

Furthermore, the AI Act justifies exempting AI systems used for national security under the premise that security and intelligence units, namely secret services and national defence, are governed under their own national frameworks.[4] Can this be a

[1] Consideration 24 AI Act.

[2] CJEU 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791.

[3] CJEU 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, § 99.

[4] Consideration 24 AI Act.

sufficient explanation for the unwillingness of the AI Act to regulate AI systems in the context of defence and national security? Maybe, the legislators' intention was not to overregulate certain sectors. For example, in the Netherlands,[5] the Dutch National Intelligence and Secret Services (AIVD) is bound by its legal framework, the Intelligence and Security Services Act 2017 ('*Wiv*' 2017). Under this legal framework, the AIVD is allowed to use (and request) data and algorithmic tools (arguably AI) for the sole purpose of protecting national security and the democratic legal order.[6] Similarly, the AIVD must implement technological and human components respecting legal requirements such as data accuracy, completeness, data quality, and deploying trustworthy algorithmic models.[7] Thus, one may argue that these unique requirements applicable exclusively to the Dutch military, intelligence and secret services may be the same or similar requirements as the ones stated under Articles 14 (human oversight) and 15 (trustworthiness of AI technologies) of the AI Act; therefore, in the Dutch example, there is no need to further regulate AI in the context of national security and defence.

The previous example may advocate for the exemption of AI systems in the context of national security among democratic states that adhere to the rule of law. However, what about states that may have a record or are being challenged for questionable practices in their intelligence units?[8] The unwillingness of the AI Act to provide a coherent uniform framework across all Member States has left unattended accountability gaps regarding legal and moral responsibility for the development and deployment of AI tools for national security purposes.[9] The decision of the AI Act not to regulate AI systems in the context of defence and national security neglects fundamental rights issues and undermines the AI Act's human-centred approach. The current gap in the AI Act allows room for an environment where AI for national security purposes may be developed under disharmonious legal and ethical frameworks in the European zone. Thus, it is plausible that exemptions on AI systems used in the context of national security might bring future challenges to democratic values and fundamental rights.[10]

The Committee on Artificial Intelligence (CAI) from the Council of Europe (CoE) proposes a different approach, only exempting AI systems that protect 'essential' national security interests,[11] inevitably sparking discussion on what can be considered 'essential'. In any case, the CAI stresses that the exemptions for national security purposes need to be consistent with international law, including human rights law obligations and the democratic order.

---

[5] The jurisdiction the authors are most familiar with.

[6] Articles 8, 9 *Intelligence and Security Services Act* 2017 ('*Wiv*' 2017).

[7] Article 24 *Wiv* 2017.

[8] Omtzigt (2023); In 't Veld (2022); Sartor and Loreggia (2022).

[9] Smuha et al. (2021), p. 19.

[10] ECNL (2024).

[11] Art. 3 of the 18 December 2023 Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, 1680ade043 (coe.int). An earlier alternative draft proposed to allow the signatory Parties to choose for themselves: 1680abde66 (coe.int).

AI systems used in intelligence and security domains undoubtedly offer advantages to fight threats to national security. For example, it is claimed that traditional Open Source Intelligence (OSINT) search techniques are being replaced by AI-powered OSINT to provide more efficiency national security and cyber defence.[12,13] Similarly, the AIVD is building up knowledge and skills regarding resilient AI tools,[14] to be able to advise key decision-makers. The AIVD is also investigating AI from an academic research approach by collaborating with different Dutch universities.[15]

Despite the good intentions and efforts to deploy AI for a good cause, we must stay alert regarding the risks of AI systems (e.g., bias, cyber-attacks, inaccuracy, etc.). In particular, AI systems used in intelligence and security domains that have not been properly tested or scrutinised against cyber vulnerabilities due to different secrecy policies. Moreover, there is not assurance that AI systems used under this context do not violate citizens' fundamental rights.[16] For example, using OSINT powered by AI models will bring legal, ethical, and organisational challenges to intelligence and security agencies.[17] The rise of ChatGPT, deep fakes, and unfiltered data and information present a risk to national security operations and citizens' fundamental rights.[18] Suppose that an OSINT AI-powered provides inaccurate information to intelligence practitioners, flagging the wrong person. A warrant will be requested to deploy surveillance and build a profile against this person. In the worse case scenario, he or she may subsequently be wrongfully prosecuted for a crime never committed and paying legal expenses as well as suffering emotional harm.[19] This extreme example, shows that some fundamental rights may be at stake: for example, privacy, health, or a fair trial (including the right to an explanation for algorithmic outputs). How can the AI Act, seeking to protect fundamental rights, include such a blanket exemption for everything falling under 'national security'?[20]

The national security exemption umbrella can also be problematic because national security does not have a uniform meaning and is broadly used to indicate different agencies such as national secret services, military intelligence, and even police enforcement intelligence units.[21]

In summary, the AI Act should have followed a more coherent and holistic approach to protect fundamental rights in the context of national security

[12] Eijkman and Weggemans (2013), p. 285. CTIVD (2021).

[13] Summary of Report Automated OSINT: tools and sources for open source investigation, CTIVD No. 74 (2021). Virginia Commonwealth University (2023).

[14] Dutch government (2024), p. 41.

[15] Strategisch Actieplan voor Artificiële Intelligentie (2019), p. 50. See also: NWO (2022).

[16] Virginia Commonwealth University (2023).

[17] Smuha et al. (2021), p. 19.

[18] Intelligence College in Europe (2023); el Rahwan (2023).

[19] Dias (2020); Safi (2018).

[20] See for instance, Recitals 43, 59 AI Act.

[21] Smuha et al. (2021), p. 19.

exemptions.[22] Uniformity and specific guidance -or harmonised rules- are needed in the intelligence and security domains to assess the use of algorithms and AI tools in the light of accountability principles such as necessity and proportionality, as well as continuous oversight.[23] If the stability of the international legal order is one of the bases for international intelligence and security cooperation, harmonised rules across all Member States should apply to intelligence and security domains. The AI Act would have been an excellent opportunity to regulate the use of AI in intelligence and security domains to establish clear boundaries to protect the international legal order and fundamental rights.

2.2 Military Purposes

Sadly, war is again everyday's business. Where only a few years ago, from a European perspective, we discussed use of AI for military purposes in a hypothetical, detached way,[24] it is now a very harsh reality close to home. Both in Gaza[25] and in Ukraine[26] AI is used for military purposes, as we speak (write).

The AI Act '*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*', art. 3(3) AI Act. It should be noted that general purpose AI (in particular: large language models) can also be very useful for military purposes.[27]

It is not just Hollywood-style 'killer robots' that we are talking about here, although autonomous drone swarms resemble them.[28] It is also facial recognition software,[29] and software for generating targets for military strikes on the basis of massive amounts of data,[30] all deeply worrying.[31]

The reasons for excluding military AI systems from the scope of the AI Act are explained by Consideration 24: '*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*

[22] ECNL (2024).

[23] Constantino and Wagner (2024).

[24] See for example Hallaq et al. (2017).

[25] McKarnan and Davies (2024).

[26] Bergengruen (2024).

[27] Roscoe (2024).

[28] Weber (2024).

[29] Bergengruen (2023).

[30] The 'Lavender' AI application, as described by Abraham (2024). See also McKarnan and Davies (2024).

[31] Gault (2023).

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'.

So, AI for military purposes should be regulated by public international law, in particular international humanitarian law, that has indeed a number of regulations in place that would apply to such AI:[32]

- 1907 Hague Regulations (Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907)
- Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Geneva, 12 August 1949
- Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea. Geneva, 12 August 1949
- Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949
- Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949
- Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977
- Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977
- Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the Adoption of an Additional Distinctive Emblem (Protocol III), 8 December 2005.

There are also some non-binding documents, specifically on AI for military purposes.[33]

Use of AI in a military context literally comes with threats, not just for human rights and European values. Human life, and human 'well-being' in an almost cynical sense (seeing the immense suffering from news footage in Ukraine and Gaza) are at stake, regardless of whether or not AI is used. AI has the potential to make things worse: more victims, more casualties, more destruction—but it depends of course on how it is used. A case can also be made for the position that use of AI

[32] Overview copied from International Humanitarian Law – International Justice Resource Center (ijrcenter.org).

[33] Stanley-Lockman and Christie (2021); AI Task Force (2019).

potentially leads to better military decision making—and therefore it would be irresponsible not to use it.[34]

In general, there are worries about the extent to which an AI could comply with IHR. Can it correctly distinguish between combattants and non-combattants?[35] Can it adequately deal with notions like proportionality?[36] Who is accountable for decisions and actions taken by military AIs?[37] Is there a risk of them going rogue (as we see in films), getting out of control?[38]

Then there is the risk of AI developed for military purposes (so outside of the purview of the AI Act) being repurposed for non-military use, e.g. by the (military) police, in prisons, during riots. Consideration 24 tries to address these worries: '*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*'.

It is probable that a repurposed military AI system would be used then as a high-risk system, meaning that it would need to comply with all the requirements for high-risk AI systems and it would need to get a CE marking. Are there any guarantees that these obligations will indeed be complied with? What happens if not?

In general, enforcement of international humanitarian law is problematic if it is not complied with by the states engaged in a military conflict.[39] If it is enforced at all, it is (years) after the fact, and not in a way that is of any use to the people suffering from violations. We are not confident at all that the deterrent effect of the possibility of maybe, later, having to face an international tribunal to be held accountable for war-crimes (committed with or without the help of AI) is strong enough to keep warriors from committing them. And use of AI does make it harder to determine who is responsible for certain actions.

A lot still needs to be done in this field. Time is running out, as can be seen in the news every day. The 'Stop killer robots'-initiative is still active.[40] The REAIM conference[41] concluded with a Call to Action:[42] '*We encourage multi-stakeholder dialogue on best practices to guide the development, deployment and use of AI in the military domain to ensure an interdisciplinary discussion throughout of good practices and policies on responsible use of AI in the military domain*'. Well, yes. In

[34] Meerveld et al. (2023), p. 13.

[35] Winter (2022), pp. 9–10.

[36] Winter (2022), pp. 15–17.

[37] Boutin (2023).

[38] Gadek (2024), pp. 119–121.

[39] Zyberi (2018).

[40] Stop Killer Robots started as an initiative in 2012—but the discussion on killer robots was sparked by a warning published in 2007: Sharkey (2007). See Stop Killer Robots - Less Autonomy, More humanity.

[41] Held in The Hague on 15–16 February 2023, both authors attended.

[42] REAIM (2023).

November 2023 the UN General Assembly adopted the first ever resolution on autonomous weapons, stressing the '*urgent need for the international community to address the challenges and concerns raised by autonomous weapons systems*'.[43] This is rather a job for politicians involving negotiations, diplomacy, power-play and so on, than for us lawyers. At the end of the day, in international law (and especially in cases where an armed conflict is at stake) we reach the limits of what law can do. But we should never stop trying!

2.3 Foreign Authorities and International Organisations

The AI Act also provides exemptions regarding the use of AI systems in the context of international agreements for law enforcement and judicial cooperation with the Union or with Member States. This exemption covers third countries and international organisations engaged by the Union or Member States to carry out an activity in the context of international cooperation for law enforcement or administration of justice purposes. For example, under this umbrella we may situate cooperation with international organisations or third countries such as Europol, Interpol, Eurojust, The European Public Prosecutor's Office (EPPO), and providers of surveillance and espionage tools such as the case of Israel (Pegasus Spyware).[44]

The AI Act has justified this exemption based on the need for future cooperation with foreign partners in the exchange of information and evidence to basically prosecute crime, whether in the context of law enforcement or administration of justice.[45]

Unlike AI exemptions for national security and military purposes, exemptions regarding the cooperation with international organisations in the context of law enforcement and judicial cooperation require that the third country or international organisation, engaged in such cooperation, provides adequate safeguards regarding the protection of fundamental rights and freedoms of individuals.[46]

The exemption is accompanied by the caveat that the third country or international organisation must be compliant with the protection of fundamental rights and freedoms of individuals. It may be inferred that the AI Act allows law enforcement or judicial agencies, which ever has jurisdiction, to 'police' the fulfilment of this caveat by the third country or the international organisation providing AI systems. In other words, the agency that engages a third country or international organisation to develop an AI system for them has also the power to decide if this third country or international organisation, working with them, complies with the protection of

[43] United Nations General Assembly (2023).

[44] Marzocchi and Mazzini (2022); In 't Veld (2022). 2022 https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf; https://www.sophieint-veld.eu/nl/pega-draft-report.

[45] Consideration 22 AI Act.

[46] Art. 2 (4) AI Act.

fundamental rights and freedoms of individuals.[47] Strange situation to be judge and party in one's own case.

However, contrary to the provisions of the AI Act, Article 82 of The Treaty on the functioning of the European Union (TEU) outlines that, for instance, judicial cooperation in criminal matters is within the jurisdiction of the European Parliament and the Council. The Article invokes the European Parliament and the Council to introduce measures that support the rights of individuals in criminal proceedings in a way that supports the maximum protection for individuals (victims and perpetrators). Thus, it is strange that the AI Act has decided to exclude the regulation of AI systems in the context of judicial cooperation. It seems inconsistent with the mandate of the European Parliament and the Council. On the other hand, the Committee on Artificial Intelligence (CAI) appears to be more concerned than the AI Act regarding the deployment of AI systems in the context of international cooperation. The CAI has proposed to regulate the use of AI systems commissioned by public authorities -for instance, law enforcement and judicial agencies- to third parties to develop systems in accordance with the CAI framework.[48]

The fact that third-countries or international organisations are granted special treatment raises concerns whether they may be shielded under a blanket of impunity for illegal deployment of AI systems in the European Union.[49] These exceptions could give rise to clever or subtle ways to implement high-risk AI systems in the European Union through third countries or international organisations under the excuse that they are systems for law enforcement or judicial cooperation within the context of Article 2(4) of the AI Act.[50] Of course, this circumvention to allow the use of high-risk AI systems in the context of law enforcement or judicial cooperation from public authorities in third countries or international organisations brings great risk to conflict with Union laws that, for instance, protect the right to privacy or the right to a fair trial.

The exclusion of AI systems under Article 2(4) also raises questions whether the European Union, its Member States, and crime-control organisations are measured under the same rule which requires public authorities and public organisations to be accountable and transparent in their decisions.[51] Particularly, this exception from Article 2(4) appears to be inconsistent with Consideration 38 which acknowledges that the actions of law enforcement authorities using AI systems are characterised by a degree of power imbalance which impacts a person's fundamental rights.[52]

The exemptions to AI systems in the context of international cooperation for law enforcement and administration of justice represent a threat to fundamental rights and European values. For instance, core fundamental rights contained in the EU

[47] Consideration 22 AI Act.

[48] Article 3 Committee on Artificial Intelligence (CAI).

[49] Raposo (2022), p. 101.

[50] EDPB-EDPS (2021), p. 8.

[51] Docksey and Propp (2023), p. 12; Naarttijärvi (2019), p. 35.

[52] Consideration 38.

Charter of Fundamental Rights are likely to be affected: human dignity (art. 1); respect for private life and protection of personal data (art. 7 and 8); right to equal treatment (art. 21) right to a fair trial, defence and presumption of innocence (art. 47, 48).

Similarly, in the international context, the Council of Europe has warned about the introduction of AI systems for law enforcement and judicial purposes, affecting the fundamental rights of people caught in the criminal justice system. In this vein, it is worth acknowledging UNESCO's assessment regarding countries lacking an adequate understanding of the societal risks of AI systems used to administer justice.[53] Based on these international authorities it can be argued that the deployment of AI systems for law enforcement and administration of justice, whether in the European Union or outside, needs to have appropriate and effective regulation because of the imminent risks to fundamental rights.[54]

Similarly, we need to take into account the 'supply chain' effect in this exception. Third countries and or international organisations can also engage industry suppliers to provide cutting edge technology.[55] In this scenario, it is unclear whether suppliers of AI technologies would also be covered under the foreign authorities and or international organisations exemption. The issue with this exemption is that the line becomes blurry when third countries or international organisations engage or hire private suppliers to develop AI systems for law enforcement or judicial cooperation purposes. Where do these suppliers of AI systems to foreign authorities fall under? Would the Brussels effect apply to them? Are they covered under the 'immunity' blanket of the AI exceptions? Or is it open to future legal challenges and further legal uncertainty in these domains? These loopholes of course represent more legal uncertainty to providers and users of AI systems. Similarly, these loopholes can seriously undermine the adequate protection of fundamental rights.

The Act does not question whether high-risk AI systems used by third countries or international organisations in the course of international cooperation or law enforcement, have measures in place to combat, or at least minimise, the irresponsible or inappropriate use of AI systems to collect biometric data.[56] For instance, there is no guarantee, or at least evidence, that third countries or international organisations have the same standards for respect to the right to a fair trial, a fair defence, and presumption of innocence, cherished by the EU Charter of Fundamental Rights.[57] One may rightfully question whether in the course of a fair trial, the information gathered through AI systems used by third countries and provided to the European Union or its Member States or its European agencies, qualifies as information that is free from bias or inaccuracies.[58] And one may question whether the

[53] UNESCO (2023).

[54] Cilevics (2020).

[55] Powell and Oswald (2024).

[56] Compare with Consideration 20.

[57] EU Charter of Fundamental Rights Articles 47, 48.

[58] Consideration 38.

AI products used in third party countries and international organisations are robust AI systems that can assure compliance with fundamental rights.

A way to overcome the shortcoming of article 2(4) may be by allowing the use of information within the meaning of Article 2(4), provided that there is a judicial authorisation that would warrant the deployment of high-risk AI systems against EU citizens.[59] For example, in extreme cases where there has been previous criminal history and plausible likelihood of re-offending in scenarios where the imminent re-offending would endanger the life of another.

In summary, the current exemption for AI systems in the context of international cooperation with law enforcement and the administration of justice does not look promising because the information or evidence collected by these high-risk AI systems used in third countries or international organisations could lead to false criminal accusations against innocent people.[60] Arguably, the AI Act could also be misleading in terms of protecting people's rights because on one hand, it says that its core purpose is to protect citizens in the Union from harmful use of AI. However, on the other hand, it opens a secret door to deploy information within the course of law enforcement and judicial cooperation against people in the Union, and perhaps many of these people are unaware that they are innocent targets of wrecked surveillance tools used by public authorities in third countries.[61] The exemptions provided for military, national security, law enforcement purposes, judicial cooperation, or foreign authorities, and the loopholes that these exemptions may bring seem to be incompatible with the aim of the AI Act which is to provide a harmonised horizontal legal framework to ensure a minimum standard across all Member States to protect citizens from harmful AI systems.[62]

3 Society

3.1 Transportation

After large language models, transportation may be one of the first fields in which the general public will see AI in action on a big scale. Self driving cars have been a tech-dream of decades, and after many years of development and testing under real life circumstances, they seem to be on the edge of being introduced on our public roads—except that that has also been true for quite a few years.[63] Anyway, self driving taxis are already being used on public roads in the US.[64] In addition to all the

[59] Human Rights Watch (2021).

[60] Human Rights Watch (2021).

[61] Dambly and Beelen (2022).

[62] Compare with Considerations 1, 2, and 3.

[63] Badue et al. (2021).

[64] Lu (2023).

technical challenges (in particular in the transitional period with still large numbers of human driven cars), there are serious open questions about their regulation, in particular regarding the assignment of liability for the accidents that will still happen[65] (even if self driving cars appear to be much safer than human driven cars).[66] Civil liability is mostly a matter for member states. There is however the proposed Artificial Intelligence Liability Directive, introducing a rebuttable presumption of causality in order to help victims harmed by AI (art. 4 AILD). Also, the AILD will help victims getting access to relevant evidence (art. 3 AILD).

At first glance, art. 2(2) AI Act seems to exclude all AI systems used in means of transportation from the AI Act. This provision is formulated in a very difficult to read and ambiguous way. High-risk AI systems already covered by the eight 'legislations' (six Regulations and two Directives) mentioned explicitly in Section B of Annex I,[67] all addressing means of transportation,[68] are not covered by the AI Act. Except that: such high-risk AI systems are required to undergo a third-party conformity assessment (art. 6(1)), and sandboxes only apply if all the requirements for high-risk AI systems have been integrated under that particular applicable Union harmonisation legislation (art. 57).

The other articles that do apply concern amendments to those legislations (art. 102–109 AI Act), basically inserting the requirements for high-risk AI (Chapter III section 2) into those legislations. And evaluation and review by the Commission of the list set out in Annex III and of the list of prohibited AI practices laid down in Article 5 (art. 112 AI Act).

So, in essence, this is not really an exemption, just a different way of putting the requirements for these high-risk AI systems in the dedicated legislation that is already in place.

The reason for this is explained in Consideration 49: '*As regards high-risk AI systems that are safety components of products or systems, or which are themselves products or systems falling within the scope of (…) it is appropriate to amend those acts to ensure that the Commission takes into account, on the basis of the technical and regulatory specificities of each sector, and without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities established therein, the mandatory requirements for high-risk AI systems laid down*

[65] van Wees (2022).

[66] Nees (2019) proving that the 'safer than human' standard is not tenable.

[67] Under the heading of 'other Union harmonisation legislation' meaning not based on the New Legislative Framework in contrast to the legislations mentioned under Section A of Annex I.

[68] Civil aviation security; the approval and market surveillance of two- or three-wheel vehicles and quadricycles; the approval and market surveillance of agricultural and forestry vehicles; marine equipment; the interoperability of the rail system; on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles; type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users; and finally common rules in the field of civil aviation.

in this Regulation when adopting any relevant delegated or implementing acts on the basis of those acts'.

So, the other rules that apply to high-risk AI systems in this field are the eight legislations mentioned (as amended by articles 102–108 of the AI Act), and all the delegated and implementing acts based upon them.[69]

Which threats to fundamental rights and European values might result from using such systems? One could think of a support system (be it for pilots, tractor-drivers or someone else) having been designed for the typical, standard user (a white male?), and not working optimally with other kinds of users. Or one could think of the violation of driver and passenger privacy resulting from the mandatory installation of eCall systems in motor vehicles which allows locating and hearing the people involved in the accident.[70] Finally, fundamental rights and European values may be compromised by whatever approach to the unsolvable ethical trolley-problem is implemented.[71] Or even by who decides which approach will be implemented.[72]

It is not really clear how such threats are addressed in these regulations—one of the main reasons being that the rules are created in a very obscure way, lacking democratic accountability e.g. by standardisation organisations.[73] It is not clear that the assessment of the risks for fundamental rights can be entrusted to, basically, the industry itself.

As the AI Act itself, the regulations do '*not appear to ensure that fundamental rights interferences by AI are subjected to demanding tests of necessity and proportionality for narrowly defined purposes, nor to consistently allocate legal responsibility for the wrongs and harms of AI in an appropriate manner*'.[74]

So, it cannot really be assessed if there is a gap here. Many things are unclear—which in itself may be considered a gap.

[69] For an overview of all EU legislation on transport, see EUR-Lex: https://eur-lex.europa.eu/summary/chapter/32.html.

[70] Wisman (2019), p. 183 ff. See the proposed Commission Delegated Regulation of 14.2.2024 amending Regulation (EU) 2015/758 of the European Parliament and of the Council as regards the standards relating to eCall, C(2024) 823 final.

[71] The trolley problem forces an actor to choose between victims, thereby exposing the inconsistency of our moral intuitions. Feffer et al. (2023), p. 5980.

[72] Interestingly, German legislation already contains a provision saying that in case of an inevitable accident, no distinctions between humans shall be made (except in the number of human lives at stake). See Straßenverkehrsgesetz, § 1e, 2(2)(c), § 1e StVG - Betrieb von Kraftfahrzeugen mit autonomer... - dejure.org.

[73] Wisman (2019), p. 217 ff.

[74] Smuha et al. (2021), p. iii.

3.2 Personal Non-professional Activity

We do not want the law to intrude too much in what we do in our private sphere: in our homes, not in any professional capacity. Enforcement would severely violate privacy, probably disproportionate to the harm or risk caused by such activity (serious crime excepted of course). The GDPR allows us to keep our own address book (art. 2(2)(c) GDPR), copyright law allows us to make home-copies of copyrighted material (art. 2(2)(b) Copyright Directive). In the same vein, the AI Act does not apply to deployers who are natural persons using AI systems in the course of a purely personal non-professional activity (art. 2(10) AI Act.[75] Obligations of providers of these systems are unaffected.

Such personal AI systems may well involve or affect other people or society at large, in addition to the user him- or herself. We use four brief examples: having intelligent personal home assistants (IPHAs) in one's house,[76] posting content on social media to amplify an urban myth, using Personal AI[77] to answer private emails and chat-messages, and finally using social robots for company and sex.

Of course, these AI systems may (depending on their functionality) be covered by other rules, both addressing the provider of such systems and/or the private person using the system for their own purposes. If personal data are processed by an IPHA, the GDPR may still apply.[78] IPHAs and social robots are required to meet certain cybersecurity standards. The DSA addresses providers of social media platforms, obliging them (to some extent) to police their end-users' behaviour.[79] Criminal law, and the upcoming CSAM Regulation, may be relevant for social media and other online communication providers and for providers of sex robots. Social media have, for their users, an ambiguous relation to freedom of expression (art. 10 ECHR).[80] On the one hand they offer great opportunities for people to express themselves, and also for receiving tons of information. However, social media also offer opportunities to abuse this freedom, by insulting, harming, threatening others, doxing, incitement to hatred, etc. So, both criminal law and tort law may cover some uses of social media.

Use of AI by natural persons in the course of a purely personal non-professional activity may cause risks; both for other natural persons and for society at large. For instance, a visitor may not be aware of the fact that the host has an IPHA in his home, and that any conversation is potentially recorded and listened into by its

[75] The literal wording is: 'This Regulation does not apply to obligations of deployers who are natural persons using AI systems in the course of a purely personal non-professional activity'. But how can a regulation (not) apply to obligations?

[76] De Conca (2021a).

[77] Such as Personal AI | AI Digital Twins.

[78] De Conca (2021b), pp. 237–238.

[79] Art. 34–36 DSA.

[80] Helberger et al. (2020).

provider, resulting in potentially grave privacy data protection violations.[81] In turn, it is foreseeable that the consequences of these breaches may pose chilling effects to society because one's private home may no longer be regarded as private.

On a societal scale, our freedom of thought may be at stake, if we are under constant surveillance and if our data exhaust is used to manipulate us, for commercial or political purposes.[82] Fake news can be used to cause polarisation in societies, to manipulate election results.[83] Personal use of social media can contribute to such effects. Chatbots that continue to 'learn' from their use can be poisoned with such fake content—really hard to trace and to get rid of. Societal harm (such as: reduced social cohesion) can also be the result of addictive AI: again, social media.[84] Private use of sex robots may lead to misogyny, to lower thresholds for sexual violence towards and abuse of humans including children.[85]

All of these dangers are not really effectively addressed by the other rules that are applicable to such personal AIs. With the DSA, Europe tries to bridle the spread of fake news by social media. Criminal law tries to deter rape, sexual violence and sexual child abuse.

In our view, the fact that for use of personal AI in communication with others, not even transparency (art. 52 AI Act) is required is a serious gap in the regulation. Also, the fact that, for instance, guests in a house are not necessarily informed of data-collection by IPHAs. The law is struggling with the systemic risk that fake news filter bubbles created by social media pose to democratic societies.

Of course, including AI used by natural persons for private purposes in the AI Act would not by itself solve all of these issues. Maybe we need to admit that law can only do so much. Not every challenge presented by use of technology can be dealt with by law, or by law alone.

3.3 Research

The purpose of the AI Act is, among other things, to '*improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI) … and supporting innovation*'.[86] AI is good, for citizens, for business and for the public interest,[87] and we need to make sure that Europe reaps its benefits. At the same time, we want to ensure '*a high level of protection of health,*

[81] De Conca (2021a), pp. 257–273.

[82] Alegre (2022).

[83] Stachofsky et al. (2023).

[84] González-Bailón and Lelkes (2023), pp. 174–175.

[85] Sterri and Earp (2021).

[86] Art. 1 and Consideration 25 and 97 AI Act.

[87] According to the sheets used by Lucilla Sioli, Director for Artificial Intelligence and Digital Industry DG CNECT, European Commission in her presentation introducing the proposal for the AI Act in a CEPS webinar on 23 April 2021, AI-Presentation-CEPS-Webinar-L.-Sioli-23.4.21.pdf.

safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union'.[88] Innovation shall not be stifled.[89]

That is why AI used for research (art. 2(6) AI Act)[90] and research to develop AI (art. 2(8) AI Act)[91] are not covered by the AI Act. Art 2(8) AI Act is quick to add that '*testing in real world conditions shall not be covered by that exclusion*'. Also, AI tools that may be used in research but that can also be used for other purposes than research, will fall under the AI Act.[92] Academic research is typically covered by specific rules, such as codes of conduct for research integrity.[93]However, in practice it may be hard to distinguish between research and early stages of product development (which would not be covered by the research exemption). Research may be intended to lead to product development and commercialisation of such a product—where do we draw the line? This legal uncertainty might actually hamper innovation.[94]

There is also the risk that very harmful AI is actually used under the disguise of research. If this is done in internal processes of an organisation, e.g. in the use of their discretionary power, if only to see what the results would be (which could be called 'research'), how could such use ever come to light and be challenged by people harmed by such use? Use of risk-assessment models to decide who to investigate comes to mind here.

So: the lack of a definition to clarify what is meant by research, and how it can be distinguished from other activities, can be seen as gaps.

3.4 Free and Open Source Licences

AI systems released under free and open source licences are not covered by the provisions of the AI Act, unless they are placed on the market or put into service as high-risk AI systems or as an AI system that falls under article 5 (prohibited AI practices) or article 50 (transparency obligations for chatbots, deepfakes and the like), says article 2 (12) AI Act. It is not really clear what is meant by 'free and open

[88] Art. 1 AI Act.

[89] Davies (2023).

[90] Stapleton (2024).

[91] Just a random example: Wang and Aouf (2024).

[92] Consideration 25 AI Act.

[93] Such as, among others: Netherlands Code of Conduct for Research Integrity, Netherlands+Code +of+Conduct+for+Research+Integrity_2018_UK.pdf (nwo.nl), supplemented by rules on use of generative AI: NWO's preliminary position on generative AI in the application and review process | NWO.

[94] Panteli et al. (2024).

source licences'.[95] It is striking that Consideration 89 refers to 'free and open-source tools, services, processes, or AI components other than general-purpose AI models', while this restriction to non-general-purpose AI models does not appear in art. 2(12). So, an open-source general-purpose AI model is not covered by art. 51–55 AI Act, even if it comes with a (potential) systemic risk.

An example (admittedly a general-purpose AI model) is Cohere Aya, a massively multilingual generative language model that follows instructions in 101 languages.[96] Other examples can be found on Hugging Face.[97]

Such systems are excluded from applicability of the AI Act in order not to hamper innovation.[98] Depending on how open source is understood (does it include the datasets used for training and testing?) transparency seems to be covered to some extent. And maybe the assumption is that for 'serious', professional and/or commercial applications that are not 'high risk' but that can nevertheless have serious consequences, no free and open-source software would be used?

Of course, all other law applies to whatever these open source systems are used for, such as: administrative law for use by government agencies, consumer protection law for use by commercial enterprises, non-discrimination law, contract law, tort law, data protection law (in particular art. 22 GDPR), law of criminal procedure, etc.

Threats to fundamental rights by use of these systems include everything the AI Act aims to protect against: '*ensuring a high level of protection of health, safety, fundamental rights (…), including democracy, the rule of law and environmental protection, against the harmful effects of AI systems*'.[99]

To some extent these threats are indeed addressed by existing (pre-AI Act) legislation such as the GDPR—except that enforcing such legislation is particularly challenging when AI is used, which is why the AI Act was proposed in the first place. For instance, as a social media user, how do you know how the content that is presented to you was selected by an open source algorithm? How could you ever challenge this selection? As a lookalike of a blacklisted shoplifter: how do you know that you are mistakenly being 'recognised' by open source facial recognition software, and therefore under increased surveillance while strolling through the shopping mall? And that therefore you were 'randomly' (not) chosen for inspection by shop security personnel? As someone who is put on a list of potential insurance fraudsters due to a high-risk score calculated by an open source model: even if you can find out that you are actually on that list, how can you ever challenge that, or disprove your risk score?

[95] See Downing (2024), who renames them 'mystery licenses'. On the legal aspects of open source AI see Riddiough (2023), and the discussion on open source AI on the Open Source Initiative at Open Source AI Deep Dive – Open Source Initiative.

[96] See Üstün et al. (2024), pp. 25–36 (their approach to safety, toxicity and bias).

[97] Hugging Face, The AI community building the future, at Hugging Face – The AI community building the future.

[98] See Castro (2024).

[99] Art. 1 AI Act.

This is a gap: natural persons subjected to decisions by AI systems released under free and open source licences are not entitled to the right to explanation of individual decision making given by art. 86 (however limited that right may be, see subsections 2 and 3).[100] And this is an inconsistency: for an affected person, what is the difference between being harmed by a 'normal' AI or by an AI system released under a free and open source licence? You are harmed, maybe you do not (or cannot) even know that an AI system was used to harm you, and even if you do know this, you have no right to an explanation under the AI Act.[101]

4 Conclusion

We can conclude that the AI Act has purposely or inadvertently left some gaps in regulating AI systems in the context of national security, military, foreign authorities, transportation, personal non-professional activity, research, and free and open source licences.

For instance, in the realm of the AI Act, AI systems for national security are excluded on the basis that national security remains the sole responsibility of Member States.[102] However, the complexities of technologies such as AI systems used for national security and intelligence purposes are not strangers to the common risks that AI may pose to society. In particular, if AI systems have not been properly tested or scrutinised against flaws that may well jeopardise citizens' fundamental rights. In this context, the AI Act undermines the whole human-centred AI approach. The AI Act missed the opportunity to provide a more coherent and holistic approach to protecting fundamental rights in the context of AI systems deployed by intelligence and security sectors.

Similarly, AI tools are currently being deployed for military purposes, such as the case in Ukraine[103] and Gaza.[104] Nonetheless, the AI Act does not apply to AI systems deployed exclusively for military, defence or national security purposes. The reasons for excluding military AI systems from the scope of the AI Act are also based on Article 4(2) TEU and the common Union defence policy that are subject to public international law.[105] Like AI systems for national security and intelligence purposes, AI in a military comes with threats, not just for human rights and European values, but in essence for human life. This gap provided by the AI Act could best be filled by international humanitarian law. However, unfortunately it is true that enforcement of international humanitarian law is problematic if it is not complied

[100] Depending on the situation, art. 12–22 GDPR may still be of help.

[101] But again maybe under art. 22 GDPR.

[102] Art. 4(2) TEU.

[103] Bergengruen (2024).

[104] McKarnan and Davies (2024).

[105] Chapter 2 of Title V TEU.

with by states engaged in a military conflict.[106] Thus, we need to start with multi-stakeholder engagement to find best practices to guide the development and deployment of AI systems for military purposes.

AI systems in the context of international agreements with third countries or international organisations for law enforcement and judicial cooperation with the Union or with Member States are also covered under the exemption umbrella. The exemption finds its justification in the need for future cooperation with foreign partners in the exchange of information and evidence to fight crime. The AI Act has established that third countries or international organisations need to provide adequate safeguards regarding the protection of fundamental rights and freedoms of individuals. However, there is no guarantee or evidence, that third countries or international organisations have the same standards in regard to safeguards for fundamental rights and core values. Thus, the exemption in this category presents risks to fundamental rights and European values such as human dignity, respect for private life and protection of personal data and right to a fair trial.

Self driving cars have been a tech-dream for decades, which is why the transportation sector may be one of the first fields in which the general public will see AI in action on a big scale. Despite the technological excitement about self driving there are serious matters to be addressed. One of them is the assignment of liability for motor-vehicle accidents. Hence, the AI Act appears to have left civil liability matters to be taken care of by member states.[107] However, transportation appears not to be an exemption, instead it is a different way of putting the requirements for these high-risk AI systems in legislation that is already in place.[108] At first glance, the threats to fundamental rights and European values that these technologies may bring is for instance the violation of driver and passenger privacy resulting from the mandatory installation of eCall systems in motor vehicles.[109] Similar to the previous categories, it is not really clear how such threats are addressed in the AI Act or other regulations referred by the AI Act,thus, creating a lack of democratic accountability. Many things remind unclear, which in itself may be considered a gap.

The AI Act is not applicable to natural persons deploying or using AI systems, as long as it for purely personal non-professional activity.[110] The exemption may find a solid ground on the basis that ‘my home my castle’, therefore, the state cannot or should not interfere in the intimate sphere. However, AI systems that are used in the context of purely personal non-professional activity still have the means to affect other people or society at large. For instance, the use of intelligent personal home assistants (IPHAs) presents issues of consent and privacy regarding home guests being unaware of the fact that the host has IPHAs in their home, and that any

[106] Zyberi (2018).

[107] Art. 2(2) AI Act.

[108] Consideration 49.

[109] Wisman (2019), p. 183 ff.

[110] Art. 2(10) AI Act.

conversation is potentially recorded and listened into.[111] Subsequently, we may be victims of surveillance, exposing our data without our consent, at the risk of being manipulated or used for commercial or political purposes.[112] The effects regarding the use of these technologies are in some cases regulated by other legal frameworks such as the GDPR or criminal law. Nonetheless, the AI Act -a uniform legal instrument- has left a significant gap in this area. Of course, including AI used by natural persons for private purposes in the AI Act would not by itself solve all of these issues. Perhaps, we may face reality that not every challenge presented by the use of technology can be dealt with by law alone.

Of course, AI is good, for citizens, for business and for the public interest.[113] That is why AI systems used for research purposes are not covered by the AI Act.[114] However, in practice it may not be easy to distinguish between purely academic or scientific research and early stages of product development for future commercialisation -which should not benefit from this exemption. Where do we draw the line? There is lack of a definition in the AI Act to ascertain what is meant by research, and how it can be distinguished from other activities. Thus, it is wise to not to let the innovation hype take over from our freedoms, our democracy, and what it means to be a human.

Lastly, in broad terms, AI systems deployed under free and open source licences are not governed by the provisions of the AI Act. It is unclear what is meant by 'free and open source licences'.[115] However, this exemption excludes high-risk AI systems or AI systems falling under prohibited practices.[116] This category exemption is not free from threats to democratic values, the rule of law, and of course fundamental rights.[117] For instance, natural persons subjected to decisions by AI systems under the free and open source licences umbrella may not entitled to the right to explanation.

The above gaps found in the AI Act pose questions about whether the Act itself undermines all the work and effort it put into preparing a framework to protect humans from harmful (untrustworthy) AI. We have exposed some potential risks to fundamental rights, democratic values, and the rule of law. These gaps and risks need to be urgently re-addressed in order to ensure 'a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the "Charter"), including democracy, the rule of law and

[111] De Conca (2021a), pp. 257–273.

[112] Alegre (2022).

[113] According to the sheets used by Lucilla Sioli, Director for Artificial Intelligence and Digital Industry DG CNECT, European Commission in her presentation introducing the proposal for the AI Act in a CEPS webinar on 23 April 2021, AI-Presentation-CEPS-Webinar-L.-Sioli-23.4.21.pdf.

[114] Art. 2(6)(8) AI Act.

[115] See Downing (2024), who renames them 'mystery licenses'. On the legal aspects of open source AI see Riddiough (2023), and the discussion on open source AI on Open Source AI Deep Dive – Open Source Initiative.

[116] Art. 5 AI Act.

[117] Art. 1 AI Act.

environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation' in the course of 'the development, the placing on the market, the putting into service and the use of artificial intelligence systems' (Consideration 1)—in other words, to achieve the very purpose of the AI Act.

References

Abraham Y (2024) 'Lavender': the AI machine directing Israel's bombing spree in Gaza, 972 Magazine 3 April 2024, 'Lavender': The AI machine directing Israel's bombing spree in Gaza (972mag.com)

AI Task Force (2019) Artificial Intelligence in Support of Defence, September 2019, Report of the AI Task Force September 2019.pdf (defense.gouv.fr)

Alegre S (2022) Freedom to think: protecting a fundamental human right in the digital age. Atlantic Books

Badue C, Guidolini R, Carneiro RV, Azevedo P, Cardoso VB, Forechi A, Jesus L, Berriel R, Paixao TM, Mutz F, de Paula Veronese L (2021) Self-driving cars: a survey. Expert Syst Appl 165:113816. https://www.sciencedirect.com/science/article/pii/S095741742030628X

Bergengruen V (2023) Ukraine's 'Secret Weapon' against Russia is a controversial U.S. Tech Company, Time, 14 November 2023, Ukraine's 'Secret Weapon' Against Russia Is Clearview AI | TIME

Bergengruen V (2024) How tech giants turned Ukraine into an AI War Lab, Time, 8 february 2024, Tech Companies Turned Ukraine Into an AI War Lab | TIME

Boutin B (2023) State responsibility in relation to military applications of artificial intelligence. Leiden J Int Law 36(1):133–150. https://doi.org/10.1017/S0922156522000607

Castro D (2024) The EU's AI Act creates regulatory complexity for open-source AI, Center for Data Innovation 4 March 2024, The EU's AI Act Creates Regulatory Complexity for Open-Source AI – Center for Data Innovation

Cilevics B (2020) Justice by algorithm–the role of artificial intelligence in policing and criminal justice systems. Report of Committee on Legal Affairs and Human Rights, Council of Europe. https://pace.coe.int/en/files/28723/pdf

Constantino J, Wagner B (2024) Accountability and oversight in the Dutch intelligence and security domains in the digital age. Front Polit Sci 6:1383026. https://doi.org/10.3389/fpos.2024.1383026

CTIVD (2021) Toezichtsrapport nr. 72 over de inzet van bijzondere bevoegdheden ter ondersteuning van een goede taakuitvoering van de AIVD en de MIVD, https://www.ctivd.nl/binaries/ctivd/documenten/rapporten/2021/04/15/rapport-72/CTIVD+NR72+Toezichtsrapport.pdf

Dambly P, Beelen A (2022) Europe: Analysis of the Proposal for an AI Regulation, (MAIEI, 2022), https://montrealethics.ai/europe-analysis-of-the-proposal-for-an-ai-regulation/

Davies P (2023) 'Potentially disastrous' for innovation: Tech sector reacts to the EU AI Act saying it goes too far. Euronews.next, 15 December 2023, 'Potentially disastrous' for innovation: Tech sector reacts to the EU AI Act saying it goes too far | Euronews

De Conca S (2021a) The enchanted house: An analysis of the interaction of intelligent personal home assistants (IPHAs) with the private sphere and its legal protection. PhD Tilburg University, online available at Microsoft Word - Enchanted House printer copy.docx (uvt.nl)

De Conca S (2021b) Smart home for lawyers: IoT in the home and its implications for the GDPR. Tijdschrift voor Internetrecht 2021(6):231–241. Article UDH:IR/17009. https://den-hollander.info/artikel/17009

Dias A (2020) The colleague, the girl, the police: Student framed and imprisoned over terror offences tells whole story for the first time, 21 April 2020, ABC.net, The colleague, the girl,

the police: Student framed and imprisoned over terror offences tells whole story for the first time - triple j (abc.net.au)
Docksey C, Propp K (2023) Government access to personal data and transnational interoperability: an accountability perspective. Oslo Law Rev (1):1–34
Downing K (2024) Choose your own adventure, the EU AI Act and Openish AI, at choose your own adventure: the EU AI Act and Openish AI – Law Offices of Kate Downing (katedowninglaw.com), 6 February 2024
Dutch government (2024) The Government-wide vision on generative AI of the Netherlands, 17 January 2024, at Government-wide vision on generative AI of the Netherlands | Parliamentary document | Government.nl
ECNL (2024) Packed with Loopholes: why the AI Act fails to protect civic space and the rule of law, European Center for Non-for-profit Law, 2024, Packed with loopholes: why the AI Act fails to protect civic space and the rule of law | ECNL
EDPB-EDPS (2021) Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), edpb-edps_joint_opinion_ai_regulation_en.pdf (europa.eu)
Eijkman Q, Weggemans D (2013) Open source intelligence and privacy dilemmas: is it time to reassess state accountability? Secur Hum Rights 23(4):285–296, online available at Microsoft Word - 03 Eijkman Weggemans v2.doc (cyberwar.nl)
el Rahwan A (2023) European research about using Artificial Intelligence and Interoperability for Solving Challenges of OSINT and Cross-Border Investigations, Border Security Report 10 February 2023, European research about using Artificial Intelligence and Interoperability for Solving Challenges of OSINT and Cross-Border Investigations - Border Security Report (border-security-report.com)
Feffer M, Heidari H, Lipton ZC (2023) June. Moral machine or tyranny of the majority? In: Proceedings of the AAAI Conference on Artificial Intelligence, vol 37, no 5, pp 5974–5982
Gadek G (2024) Unreliable AIs for the military. In: Schraagen JM (ed) Responsible use of AI in military systems. Chapman and Hall/CRC, pp 101–123. https://doi.org/10.1201/9781003410379
Gault M (2023) Palantir Demos AI to fight wars but says it will be totally ethical don't worry about it, 26 April 2023, Palantir Demos AI to Fight Wars But Says It Will Be Totally Ethical Don't Worry About It (vice.com)
González-Bailón S, Lelkes Y (2023) Do social media undermine social cohesion? A critical review. Soc Issues Policy Rev 17(1):155–180. Do social media undermine social cohesion? A critical review - González-Bailón - 2023 - Social Issues and Policy Review - Wiley Online Library
Hallaq B, Somer T, Osula A-M, Ngo K, Mitchener-Nissen T (2017) Artificial intelligence within the military domain and cyber warfare. In: 16th European Conference on Cyber Warfare and Security (ECCWS 2017), Dublin, Ireland, 29–30 June 2017. Published in: Proceedings of 16th European Conference on Cyber Warfare and Security. The Title of the Paper Goes Here, in Title Case and Title Style (warwick.ac.uk)
Helberger N, Van Drunen M, Eskens S, Bastian M, Moeller J (2020) A freedom of expression perspective on AI in the media–with a special focus on editorial decision making on social media platforms and in the news media. Eur J Law Technol 11(3). A freedom of expression perspective on AI in the media – with a special focus on editorial decision making on social media platforms and in the news media | European Journal of Law and Technology (ejlt.org)
Human Rights Watch (2021) How the EU's Flawed Artificial Intelligence Regulation endangers the Social Safety Net: Questions and Answers, https://www.hrw.org/news/2021/11/10/how-eus-flawed-artificial-intelligence-regulation-endangers-social-safety-net
in 't Veld S (2022) Draft Report Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware. European Parliament, https://www.sophieintveld.eu/download/getFile/5073
Intelligence College in Europe (2023) French seminar on open-source intelligence (OSINT), March 2023, Intelligence College in Europe (intelligence-college-europe.org)

Lu Y (2023) 'Lost Time for No Reason': how driverless taxis are stressing cities. The New York Times, 20 November 2023, 'Lost Time for No Reason': How Driverless Taxis Are Stressing Cities - The New York Times (nytimes.com)

Marzocchi E, Mazzini M (2022) Pegasus and surveillance spyware. Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies PE 732.268, Pegasus and surveillance spyware (europa.eu)

McKarnan B, Davies H (2024) 'The machine did it coldly': Israel used AI to identify 37,000 Hamas targets. The Guardian, https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes

Meerveld HW, Lindelauf RHA, Postma EO, Postma M (2023) The irresponsibility of not using AI in the military. Ethics Inf Technol 25(1):14

Naarttijärvi M (2019) Legality and democratic deliberation in black box policing. Technol Regul 35–48. http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-164827

Nees MA (2019) Safer than the average human driver (who is less safe than me)? Examining a popular safety benchmark for self-driving cars. J Safety Res 69:61–68. https://www.sciencedirect.com/science/article/pii/S0022437518304511

NWO (2022) Two grants awarded within the KIC call for 'Data and Intelligence', 16 May 2022, Two grants awarded within the KIC call for 'Data and Intelligence' | NWO

Omtzigt P (2023) Pegasus and similar spyware and secret state surveillance, Report 15825, Council of Euorpe, (20 September 2023), https://pace.coe.int/en/files/29415 or https://pace.coe.int/pdf/aa984c36c6453ff2f5ae7a2079f90285ffeb19690007cea2c849692eaf5d7ef5?title=Doc.%2015825.pdf

Panteli T, Hommerson S, van de Weijer C (2024) Why the AI act is a huge triumph and how we can make it work. Research Professional News 21 March 2024, Why the AI act is a huge triumph and how we can make it work - Research Professional News

Powell R, Oswald M (2024) Assurance of Third-Party AI Systems for UK National Security. Centre for Emerging Technology and Security Research Report, 01.17.2024_assurance_report.pdf (turing.ac.uk)

Raposo VL (2022) Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence. Int J Law Inf Technol 30(1):88–109

REAIM (2023) Call to Action, https://www.government.nl/binaries/government/documenten/publications/2023/02/16/reaim-2023-call-to-action/REAIM+2023+Call+to+Action.pdf

Riddiough J (2023) Licensing and Legal Considerations for Open-Source AI, 7 March 2023, Licensing and Legal Considerations for Open-Source AI - AI Models

Roscoe J (2024) Russia, China, North Korea, and Iran Used GPT for 'Malicious Cyber Activities', OpenAI Says, Vice.com February 15, 2024, Russia, China, North Korea, and Iran Used GPT for 'Malicious Cyber Activities', OpenAI Says (vice.com)

Safi M (2018) University of NSW student wrongly accused of terrorism offences plans to sue police and media, The Guardian, 23 November 2018, University of NSW student wrongly accused of terrorism offences plans to sue police and media | Australia news | The Guardian

Sartor G, Loreggia A (2022) The impact of Pegasus on fundamental rights and democratic processes. European Parliament, (December, 2022), https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf

Sharkey N (2007) Robot wars are a reality. In: The Guardian, 18 August 2007, Robot wars are a reality | Noel Sharkey | The Guardian

Smuha NA, Ahmed-Rengers E, Harkens A, Li W, MacLaren J, Piselli R, Yeung K (2021) How the EU can achieve legally trustworthy AI: a response to the European Commission's Proposal for an Artificial Intelligence Act (August 5, 2021). Available at SSRN: https://ssrn.com/abstract=3899991 or https://doi.org/10.2139/ssrn.3899991

Stachofsky J, Schaupp LC, Crossler RE (2023) Measuring the effect of political alignment, platforms, and fake news consumption on voter concern for election processes. Gov Inf Q 40(3):101810

Stanley-Lockman Z, Christie EH (2021) An Artificial Intelligence Strategy for NATO, 25 October 2021, NATO Review - An Artificial Intelligence Strategy for NATO

Stapleton A (2024) The best AI tools for research papers and academic research (Literature review, grants, PDFs and more), Academia Insider, The best AI tools for research papers and academic research (Literature review, grants, PDFs and more) – Academia Insider

Sterri AB, Earp BD (2021) The ethics of sex robots. In: The Oxford handbook of digital ethics, pp 1–22

Strategisch Actieplan voor Artificiële Intelligentie 2019, Rapport SAPAI (overheid.nl)

UNESCO (2023) Global Toolkit on AI and the Rule of Law for the Judiciary, CI/DIT/2023/AIRoL/01, https://unesdoc.unesco.org/ark:/48223/pf0000387331

United Nations General Assembly (2023) Seventy-eighth session, First Committee, Agenda item 99, General and complete disarmament, L56.pdf (reachingcriticalwill.org)

Üstün A, Aryabumi V, Yong ZX, Ko WY, D'souza D, Onilude G, Bhandari N, Singh S, Ooi HL, Kayid A, Vargus F (2024) Aya model: an instruction finetuned open-access multilingual language model. arXiv preprint arXiv:2402.07827

van Wees KAPC (2022) Civil liability for autonomous vehicles in the Netherlands. In: Netherlands Reports to the Twenty-first International Congress of Comparative Law, 23–28 October 2022, Asunción (Paraguay). In press

Virginia Commonwealth University (2023) Artificial Intelligence (AI) Challenges and Advantages in National Security, 6 December 2023, Artificial Intelligence (AI) Challenges and Opportunities in National Security (vcu.edu)

Wang C, Aouf N (2024) Explainable deep adversarial reinforcement learning approach for robust autonomous driving. IEEE Transactions on Intelligent Vehicles

Weber J (2024) Autonomous drone swarms and the contested imaginaries of artificial intelligence. Digital War, pp 1–4. Autonomous drone swarms and the contested imaginaries of artificial intelligence | Digital War (springer.com)

Winter E (2022) The compatibility of autonomous weapons with the principles of international humanitarian law. J Conflict Secur Law 27(1):1–20. https://doi.org/10.1093/jcsl/krac001

Wisman THA (2019) The quest for the effective protection of the right to privacy: on the policy and rulemaking concerning mandatory Internet of Things systems in the European Union, PhD-Thesis, Vrije Universiteit Amsterdam. complete+dissertation.pdf (vu.nl)

Zyberi G (2018) Enforcement of international humanitarian law. Human Rights Institutions, Tribunals and Courts: Legacy and Promise (Springer, 2018), pp 377–400, https://www.duo.uio.no/bitstream/handle/10852/66318/zyberi.pdf