Recommendations for the Republic of Slovenia to ensure the protection of fundamental rights when employing artificial intelligence systems in areas that the AI Act exempts or conditionally prohibits

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 AI Act, which regulates the placing on the market and use of artificial intelligence (AI) systems in the European Union, entered into force in August 2024. In February 2025, provisions regarding prohibited practices that represent an unacceptable risk to the safety and fundamental rights of citizens came into force. With this, also some exceptions came into force, which are worrying from the standpoint of protecting fundamental rights.

For example, the AI Act does not apply to the use of AI systems for exclusively military, defense or national security purposes. The exclusion of national security is justified by Article 4(2) of the Treaty on the European Union, which stipulates that, in particular, national security remains the exclusive competence of each member state. At the same time, the list of prohibited practices is primarily a list of conditional prohibitions. Therefore, the concern remains that these loopholes in the regulation could be used to weaken democracy, democratic processes and the rule of law, which would have a frightening effect on public assembly, the right to protest, privacy and other fundamental rights, which are, among other things, guaranteed in the Charter of the European Union on Fundamental Rights (hereinafter: the EU Charter)[1] and the Constitution of the Republic of Slovenia (hereinafter: the Constitution).

[1] Charter of Fundamental Rights of the European Union, UL C 202, 7 June 2016.

Use of AI systems in the field of national security

The definition of national security and essential security interests is primarily the responsibility of the Member States. Although we do not have a clearly defined concept of national security in Slovenian legislation,[2] the Court of Justice of the EU in the combined cases C-511/18, C-512/18 and C-520/18 (La Quadrature du Net) of 6 October 2020[3] set a rough definition of national security. The Court stated that this jurisdiction corresponds to the primary interest, which is to protect the essential functions of the state and the fundamental interests of society, and includes the prevention and punishment of activities that can seriously destabilise the fundamental constitutional, political, economic or social structures of the state and, in particular, directly threaten society, the population or the state, such as terrorist acts in particular. The Court emphasises that deviations in accordance with the provisions on the security of member states refer to exceptional and clearly defined cases, which do not represent a general exception and which should be interpreted restrictively.

Member States are entitled to take appropriate measures to ensure their security. Although the use of AI in the field of national security is not regulated by the AI Act, such measures are not entirely outside the scope of EU law. These measures must comply with the general principles of EU law, including the principle of proportionality, which requires that deviations remain within the limits of what is appropriate and necessary to achieve the objective.[4] Member States must demonstrate that such measures are necessary, proportionate and respect the essence of fundamental rights. This point of view is also represented in the case law of the European Court of Human Rights, which obliges its members that an independent body must verify the necessity and legality of the measures.[5] This may require greater transparency and accountability of national security agencies, which can be challenging given the often confidential nature of their operations.

---

[2] The understanding of this concept in the national framework can be inferred to a certain extent from the Resolution on National Security Strategy (Official Gazette of the Republic of Slovenia, No. 59/19), which defines national interests and national defense goals, but does not represent a binding legal document and does not define the concept of national security as such.

[3] CJEU, joined cases C-511/18, C-512/18 and C-520/18 (*The Quadrature of the Net*) from 6 October 2020, URL: https://curia.europa.eu/juris/document/document.jsf;jsessionid=356695CB12AF6B8B04830FAB2D40762A?text=&docid=232084&pageIndex=0&doclang=SL&mode=lst&dir=&occ=first&part=1&cid=11509485, retrieved on 8/27/2025.

[4] Slepak, Vitaly, National security clause: law and practice of European Union and Eurasia Economic Union, 2019, J. Phys.: Conf. Ser. 1406, URL: https://iopscience.iop.org/article/10.1088/1742-6596/1406/1/012002/pdf, p. 3-4, retrieved on 27/08/2025.

[5] European Court of Human Rights, Janowiec and others v. Russia, no. 55508/07 and 29520/09 of 21 October 2013, URL: https://hudoc.echr.coe.int/eng?i=001-127684, retrieved on 09/02/2025.

Despite the exemption, national security authorities must carefully evaluate the legality of using AI systems for two reasons. Firstly, it is essential to ensure that these systems are used exclusively for national security purposes, as stipulated in point 3 of Article 2(3) of the AI Act. The less serious the perceived threat to national security, the stricter the restrictions become for a measure to be defined as an express use for those purposes. This ensures that surveillance measures are limited to addressing real threats. Secondly, an assessment of the proportionality of the specific measure must be carried out in accordance with the EU Charter and the Constitution, even if the use is outside the scope of the regulation of the AI Act. As part of the proportionality test, appropriateness, necessity and proportionality in the narrower sense are assessed (*strictu sensu*). Appropriateness is likely to be less relevant, as issues relating to it may be caught up in the assessment of exclusive use from the Act itself. Urgency will relate primarily to the scale of the measure. The greater the danger, the more leeway is allowed in terms of extensiveness. For this reason, it will be crucial that Member States and their authorities put in place robust safeguards, transparency measures (depending on how transparency affects the ability to operate effectively) and independent monitoring mechanisms to ensure compliance with fundamental rights. This stems primarily from the assessment of proportionality in the narrower sense. The quality of safeguards must increase depending on how likely unlawful access is.[6]

We also wish to highlight the problematic overlap between national security and law enforcement activities (the prevention, detection, investigation, and prosecution of criminal offences), which are governed by the AI Act. The Act's broad definition of prevention, detection, investigation and prosecution of criminal offences can, in certain cases, be interpreted to overlap with the concept of national security, creating a significant risk of abuse. For example, authorities could subject protests or direct actions to AI surveillance by citing national security, thereby circumventing the limitations imposed by the AI Act. The case of Palestine Action in the UK is a relevant example of this potential conflict. To prevent such misuse, any shared capabilities between national security and law enforcement agencies must be carefully monitored and controlled to ensure full compliance with the AI Act and other EU laws. Furthermore, there must be a clear and strict demarcation between activities that fall under prevention, detection, investigation and prosecution of criminal offences and those that genuinely pertain to national security.

[6] Laag, Emil, Beyond the Scope? The National Security Exemption and AI-Based Surveillance: Examining the Impact on EU Citizens' Rights in the Age of Artificial Intelligence, URL: https://gupea.ub.gu.se/handle/2077/85320, p. 32, 33, retrieved on 27/08/2025.

For these reasons, Member States will find themselves in a complex legal environment, where their exclusive competence in the field of national security is not as absolute as it seems at first glance. When deploying AI for national security reasons they will have to factor in the general principles of EU law.

Taking into account what has been pointed out above, we recommend that Slovenian authorities adopt a resolution or protocol governing the use of AI for national security. This framework must address all the aforementioned complexities, including overlapping jurisdictions. Doing so will ensure that exceptions to prohibited uses are interpreted narrowly, thereby preventing potential abuse and overreach by national security authorities or law enforcement.

The use of high-risk AI systems in the field of prevention, detection, investigation, and prosecution of criminal offences

Even before the final adoption of the AI Act, many critics warned about the dangers of certain AI systems and advocated for their complete ban. However, despite strong resistance, some of these systems remain in the Act as "conditional prohibitions" under Article 5. For example, the EDPS and EDPB warned[7] that the exceptions to these prohibitions are so vast that authorities can almost always find a "high enough" number of suspects to justify deploying these supposedly restricted technologies.

In February 2025, the European Commission published guidelines on prohibited practices,[8] intended to ensure the consistent and effective application of the AI Act across the EU. However, they are non-binding and, more importantly, do not clarify the ambiguous definitions of the exceptions, leaving them wide open to interpretation.

Furthermore, a critical omission highlighted by civil society organisations like the Protect Not Surveil coalition[9] is the Act's failure to address AI in migration and border control. The

[7] EDPB-EDPS 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), URL: https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf, p. 12, retrieved on 27/08/2025.
[8] European Commission, Prohibited Practices Guidelines, 2025, URL: https://digital-strategy.ec.europa.eu/sl/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act, obtained on 30/08/2025.
[9] #ProtectNotSurveil, The EU AI Act, URL: https://protectnotsurveil.eu/#calls, retrieved on 8/27/2025.

list of high-risk systems is also dangerously incomplete, excluding harmful technologies like biometric scanners or predictive analytics tools used to profile and block migrants.

The AI Act also introduces exceptions related to obligations regarding comprehensibility and transparency of use in the context of migration and law enforcement, which undermines effective public control. As a result, affected people, civil society and journalists will not be able to know where and in what contexts some of the most harmful AI systems are being used. We maintain that the use of any system in police or border control procedures is unacceptable if its operations and consequences cannot be fully explained.

At the same time, we warn that accountability mechanisms after incidents and violations of fundamental rights will not bring much comfort to the victims. In most cases, regulation and control only come into effect after the violation has been committed and therefore fail to provide protection beforehand. Victims are often individuals or social groups who are already vulnerable and lack both the information and the capacity to file a complaint.

With regard to the use of remote biometric identification systems in publicly accessible spaces for the purposes of prevention, detection, investigation, and prosecution of criminal offences, the AI Act distinguishes between real-time identification and post-remote identification. The former involves live capture, comparison and identification, while the latter performs these functions retrospectively using previously collected data such as camera footage. The AI Act defines post-biometric identification systems as high-risk and in principle prohibits the use of real-time remote biometric identification systems in publicly accessible spaces for the purposes of prevention, detection, investigation, and prosecution of criminal offences, while still allowing some important exceptions of concern. In Slovenia, we currently have no legislative basis for the use of remote biometric identification in real time in publicly accessible spaces, while post-remote identification is allowed. But the distinction between the use of real-time technology and the post-remote use is arbitrary, and the difference in the conditions of use is huge, since the conditions for the use of the subsequent identification are quite loose. The differences between the two usages appear mainly in terms of the approval process. Article 5(3) of the AI Act stipulates that a judicial authority or an independent administrative authority whose decision is binding must issue approval before remote biometric identification systems are used in real-time publicly accessible spaces. In extreme emergencies, law enforcement agencies can use the technology without approval if they apply for approval within 24 hours. However, as far as post-identification systems are concerned, Article 26(10) stipulates that law enforcement authorities require

prior approval from the same authorities either before using the system or no later than 48 hours after its use. A subsequent request for approval also does not require an urgency requirement. In addition, approval is not required when the system is used to identify a potential suspect.[10]

When using it, there may also be unlawful abuses. Any criminal act can potentially be used to justify using the system for post-remote identification. For example, law enforcement could accumulate images of faces obtained through untargeted scanning and attempt to identify individuals in their databases after the images were captured. Such use would undermine human rights just as real-time identification would: in both cases, law enforcement could, among other things, attempt to identify participants in a public political protest even without the existence of suspicion or evidence that the protesters violated any laws.[11] The use of such biometric applications can therefore lead to mass surveillance and the violation of fundamental rights such as the right to privacy, freedom of expression, and peaceful protest. It also reinforces the power imbalance between those who observe and those who are observed; the fear of being identified even months after participation in a public event can, for example, have a significant impact on the exercise of the right to freedom of expression and assembly. Although the AI Act recognises the risks to the rights of individuals from the use of such biometric technologies for identification, it does not adequately address the risks and provides unclear exceptions to the prohibition of use.

Unfortunately, some governments in the EU are already taking advantage of the legal loopholes allowed by the AI Act to employ mass surveillance. In Austria, the government used a biometric system to identify climate activists at protests, and in Hungary, they passed a law allowing the use of facial recognition technology in pride parades.

Taking into account what has been said, we recommend that those responsible consider more restrictive measures regarding the use of prohibited practices for the purposes of preventing, detecting, and investigating criminal offences, especially in the areas of migration, border management, and the use of remote biometric identification. Above all, they should not, under any circumstances, adopt additional legislation which would approve or permit the use of certain AI systems for the detection, prevention, investigation, or prosecution of criminal acts, if doing so would

[10] Giannini, Tas, AI Act and the Prohibition of Real-Time Biometric Identification, Much ado about nothing?, 10. 12. 2024, URL: https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification/, retrieved on 8/27/2025.
[11] The Human Rights Risks of Facial Recognition AI Tech in Policing and Immigration Must be Properly Recognised in the EU AI Act, Center for Democracy and Technology Europe, https://cdt.org/insights/brief-human-rights-risks-of-facial-recognition-ai-tech-in-policing-and-immigration-must-be-properly-recognised-in-the-eu-ai-act/, retrieved on 8/27/2025.

enable the avoidance of obligations regarding transparency and the right of individuals to be informed from Article 50 of the AI Act.

Article 26(10) of the AI Act regulates post-remote biometric identification and the necessary authorisation for its use, where the restrictions or conditions are milder than in real-time remote biometric identification. The article stipulates that the introducer of the high-risk AI system for post-remote biometric identification must request authorisation from a judicial authority or an administrative authority whose decision is binding and subject to judicial review prior to or without undue delay and no later than within 48 hours of use, unless the system is used for the initial identification of a possible suspect based on objective and verifiable facts directly related to the crime. Member States will have to specify the procedure for this kind of authorisation in more detail. **We recommend that those responsible clearly and strictly define at the legal level the procedure for obtaining permission and the procedure in case of refusal, so that the relevant authorities will be bound by clear restrictions while simultaneously ensuring an adequate level of human rights protection.**

Although we primarily advocate for the need for more preventative measures in law enforcement, and consequently do not support the use of the technologies mentioned above, we understand that such technologies will be used in practice. Considering all the above-mentioned threats to rights and the potential for infringement or unlawful use, **we recommend that all AI systems be made available to public control in a public AI registry. At the same time, the state must also provide an internal system for monitoring the procurement, implementation, and use of AI systems and an efficient system for the immediate suspension of the use of such systems upon any finding of a violation of fundamental rights.**

DANES JE NOV DAN

Pravna mreža ZA VARSTVO DEMOKRACIJE

Danes je nov dan, Inštitut za druga vprašanja (Today is a New Day, Institute for Other Studies) is an independent non-profit organisation founded in 2013 that works at the intersection of technology, democracy and digital rights. By combining the development of open source tools, advocacy and cooperation with communities, we strive for greater transparency of institutions and active involvement of the public in political processes. The institute has the status of an organisation in the public interest in the field of information society. We regularly work on the regulation linked to the responsible use of new technologies, with a special emphasis on artificial intelligence. We contribute to the co-design of national policies, participate in the expert council to discuss issues and provide advice on the implementation of the AI Act and in the process of preparing the National Program on AI 2030. We work in a wider European context as members of the digital rights network EDRi, and we demonstrate our commitment to transparency with projects such as the Public Sector AI Registry.

Contact person: Jasmina Ploštajner, jasmina@danesjenovdan.si

The Legal Network for the Protection of Democracy is an initiative that provides legal support to individuals and organizations who find themselves in legal proceedings due to non-violent public action. With legal opinions, positions and appeals, we protect a democratic, open, free and solidary society.*

Sofinancira Evropska unija

IMPACT 4VALUES

Funded by the European Union. The views and opinions expressed are solely those of the author(s) and do not necessarily reflect the views and opinions of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the EACEA can be held responsible for them.