



European Center for
Not-for-Profit Law

Open letter

The AI Act Must Protect the Rule of Law

The European Union's bodies are currently engaging in the final stage of negotiations on the Artificial Intelligence Act (AI Act). As representatives of civil society organizations committed to upholding and monitoring the rule of law and democracy in the European Union, we call on legislators to ensure that the AI Act is fully coherent with rule of law standards, including transparency, accountability, and access to justice. Given the current decline of the rule of law in Europe, and the heightened concern over AI's misuse, the Union cannot afford to miss this crucial opportunity and should introduce strong safeguards to protect the full respect of human rights and the rule of law.

Artificial Intelligence (AI) is rapidly transforming our world. Its influence permeates every facet of our lives, from healthcare and education to governance and law enforcement. While the potential benefits of AI are undeniable, it is imperative that we prioritize the protection of our shared values as laid out in the Treaties of the EU and the EU Charter of Fundamental Rights.

The principle of the rule of law, enshrined in Article 2 TEU, is fundamental to the EU. This core value is a precondition for the realization of fundamental rights and other fundamental values. Rule of law requirements mean, among others: transparent, accountable, democratic, and pluralistic law-making process; legal certainty; prohibition of arbitrariness of the executive powers; effective and equal judicial protection, including access to justice, by independent and impartial courts; separation of powers; and non-discrimination and equality before the law. **The rule of law is inextricably linked with the protection of democracy and fundamental rights; the three criteria reinforce each other and therefore the link between the development and deployment of AI systems and the rule of law must be established.**

As AI becomes increasingly deployed by both the private and public sectors, the rule of law requires the EU to adopt robust safeguards to protect the very foundation our Union stands on. The misuse of AI systems, including opaque and unaccountable deployment of AI systems by public authorities, poses a serious threat to the rule of law and democracy. In member states where these are teetering, regulatory loopholes, such as national security and law enforcement exemptions, could be exploited to weaken democratic institutions and processes and the rule of law. The AI Act needs to create a robust, secure regulatory environment grounded in the protection of fundamental rights and rule of law.

A central safeguard for the accountable and rights-respecting exercise of power is the mandatory inclusion of fundamental rights impact assessments (FRIAs), as it appears in the

European Parliament's position on the AI Act. We argue that, similarly to the obligation set out in the Digital Services Act, which requires very large online platforms to conduct risk assessments, AI FRIAs should be considered in the context of an emerging trend toward the development of standards and certifications for responsible AI governance practices. FRIAs should be an obligation for all high-risk AI technologies to ensure that they are deployed in a way that upholds the principles of justice, accountability, and fairness. FRIAs provide a structured framework to assess and avoid potential fundamental rights violations, ensuring that AI technologies respect, promote, and protect these rights.

As states are responsible for the proper implementation of the rule of law framework, that public authorities, including law enforcement, conduct FRIAs is not just a recommendation but a necessary safeguard to ensure that AI systems are designed and deployed in full accordance with the values of the EU and the EU Charter of Fundamental Rights.

Transparency, a cornerstone of democratic governance and a key feature to ensure that rules are made and applied in a clear and predictable manner, as the rule of law requires, must be integral to the FRIA process. The findings and outcomes of FRIAs must be publicly accessible, including for the persons affected by decisions made with the use of the AI systems, and open to feedback and review. This ensures that AI deployers remain accountable to the people affected by the use of the systems and provides a platform for civil society organizations, watchdogs, and the general public to engage in constructive oversight.

This accountability framework can only safeguard the rule of law and fundamental rights if it applies to all high-risk AI systems. Any loopholes or exemptions would undermine legal certainty and lead to the arbitrary exercise of power, which is fundamentally incoherent with the principle of rule of law.

Through amendments to Article 6 of the AI Act in the Council and Parliament texts, a loophole has been created that gives companies and public authorities alike the power to unilaterally decide that their AI system should be exempted from the AI Act requirements, even though it is intended to be used in one of the high-risk areas, such as law enforcement, justice, elections, or essential public services. If a provider chooses to exempt themselves, then all consequent obligations for deployers of such systems will no longer apply either. As a result, public authorities who then deploy such high-risk systems would arbitrarily escape all AI Act obligations to safeguard people affected by AI from the abuse of their fundamental rights.

For the protection of the rule of law, there should be no blanket national security exemption in the AI Act. While national security could in some instances be considered legitimate grounds for restrictions to fundamental rights, any exceptions from AI Act requirements should be assessed on a case-by-case basis, in line with the EU Charter of Fundamental Rights and the jurisprudence of the CJEU. The risks to fundamental rights are arguably the most severe when AI systems are deployed for national security purposes, given the lack of a commonly accepted definition of national security and the ensuing risk of abuse. We have witnessed this when an invasive surveillance software – Pegasus – was used in some EU member states to spy on journalists, civil society and opposition politicians. From the perspective of rule of law requirements, it is therefore imperative that basic safeguards envisioned in the AI Act are equally respected when AI technologies are developed or used for national security purposes.

Furthermore, individuals wronged by undue or improper use of these systems must have access to effective legal remedies.

Therefore,

We call on EU legislators to **mandate FRIAs to be conducted on all high-risk AI systems**, in line with the amendments proposed by the European Parliament in **Article 29a**, and include rules to ensure FRIAs are conducted in an open and transparent manner and their findings subject to public scrutiny.

We call on EU legislators to **reject the European Council's proposed amendment to Article 2 of the AI Act**, which aims to exclude AI systems developed or used for **national security purposes** from the scope of the Act.

We call on EU legislators to return to the original Commission proposal's version of Article 6(2) of the AI Act, thereby removing newly added loopholes which would give AI developers, be it from the public or the private sector, the power to unilaterally exempt themselves from the safeguards set out in the AI Act.

As the EU navigates the complexities of the digital age, it is of the utmost importance that we do not lose sight of our core values. **We call upon EU legislators to heed our requests as a testament to the EU's commitment to protecting the rule of law from AI deployments.** The future of our societies depends on the choices we make today.

Signed,

Europe and International

Access Now

Amnesty International

Centre for Democracy and Technology Europe

Civil Liberties Union for Europe (Liberties)

European Digital Rights (EDRi)

European Center for Not-for-Profit Law (ECNL)

European Civic Forum (ECF)

European Partnership for Democracy (EPD)

European Sex Workers Rights Alliance (ESWA)

Fair Trials

International Commission of Jurists

Open Future

Statewatch

World Organisation Against Torture

Austria

epicenter.works

Belgium

Ligue des droits humains

Bulgaria

Bulgarian Center for Not-for-Profit Law
Bulgarian Helsinki Committee

Croatia

Centre for Peace Studies
Expanse of Gender and Media Culture 'Common Zone'
Gong
Human Rights House Zagreb
Politscope
Zagreb Pride

Denmark

Nyt Europa

Estonia

Estonian Human Rights Centre
Network of Estonian Non-Governmental Organizations

France

Ligue des droits de l'Homme (LDH)
Ligue de l'enseignement
Maison de l'Europe de Paris

Germany

AlgorithmWatch
Bundesnetzwerk Bürgerschaftliches Engagement (BBE)
D64 - Zentrum für Digitalen Fortschritt e. V.
Maecenata Foundation

Greece

Greek Forum of Refugees
Homo Digitalis

Hungary

European House Budapest
Hungarian Civil Liberties Union
Hungarian Helsinki Committee
Ökotárs - Hungarian Environmental Partnership Foundation

Ireland

Irish Council for Civil Liberties
The Wheel

Italy

Assoziatione Antigone
Associazione Ricreativa Culturale Italiana (ARCI)
Italian Coalition for Civil Liberties and Rights (CILD)
European Movement Italy
Hermes Center

Latvia

Centre for Public Policy PROVIDUS

Lithuania

Human Rights Monitoring Institute

The Netherlands

Bits of Freedom

Health Action International

Norway

Elektronisk Forpost Norge (EFN)

Poland

Moje Państwo Foundation

National Federation of Polish NGOs

Panoptikon Foundation

Romania

APADOR-CH

Center for Not-for-Profit Law in Romania (CLNR)

Expert Forum

Fundatia pentru Dezvoltarea Societatii Civile

Slovakia

VIA IURIS

Slovenia

CNVOS

Danes je nov dan, Inštitut za druga vprašanja

Peace Institute

Lega Center for the Protection of Human Rights and the Environment (PIC)

Spain

AlgoRace

GENTIUM

Sweden

Civil Rights Defenders

Turkey

Alternatif Bilisim