PACKED WITH LOOPHOLES: WHY THE AI ACT FAILS TO PROTECT CIVIC SPACE AND THE RULE OF LAW

April 2024

CIVIL LIBERTIES UNION FOR EUROPE

European Center for Not-for-Profit Law

EUROPEAN CIVIC FORUM

Publisher

Civil Liberties Union for Europe e.V
Ebertstraße 2. 4th floor
10117 Berlin , Germany
www.liberties.eu

Authors

Jonathan Day (Liberties)
Karolina Iwańska (ECNL)
Eva Simon (Liberties)
Kerttu Willamo (ECF)

The unaccountable and opaque use of Artificial Intelligence (AI), especially by public authorities, can undermine civic space and the rule of law. In the European Union, we have already witnessed AI-driven technologies being used to surveil activists, assess whether airline passengers pose a terrorism risk or appoint judges to court cases. The fundamental rights framework as well as rule of law standards require that robust safeguards are in place to protect people and our societies from the negative impacts of AI.

For this reason, the European Centre for Not-for-Profit Law (ECNL), Liberties and the European Civic Forum (ECF) closely monitored and contributed to the discussions on the EU's Artificial Intelligence Act (AI Act), first proposed in 2021. From the beginning, we advocated for strong protections for fundamental rights and civic space and called on European policymakers to ensure that the AI Act is fully coherent with rule of law standards.

The European Parliament approved the AI Act on 13 March 2024, thus marking the end of a three-year-long legislative process. Yet to come are guidelines and delegated acts to clarify the often vague requirements. In this article, we take stock of the extent to which fundamental rights, civic space and the rule of law will be safeguarded and provide an analysis of key AI Act provisions.

Far from a golden standard for a rights-based AI regulation

Our overall assessment is that **the AI Act fails to effectively protect the rule of law and civic space**, instead prioritising industry interests, security services and law enforcement bodies. While the Act requires AI developers to maintain high standards for the technical development of AI systems (e.g. in terms of documentation or data quality), measures intended to protect fundamental rights, including key civic rights and freedoms, are insufficient to prevent abuses. They are **riddled with far-reaching exceptions**, lowering protection standards, especially in the area of law enforcement and migration.

The AI Act was negotiated and finalised in a rush, leaving significant gaps and legal uncertainty, which the European Commission will have to clarify in the next months and years by issuing delegated acts and guidelines. Regulating emerging technology requires flexibility, but the Act leaves too much to the discretion of the Commission, secondary legislation or voluntary codes of conduct. These could easily undermine the safeguards established by the AI Act, further eroding the fundamental rights and rule of law standards in the long term.

CSOs' contributions will be necessary for a rights-based implementation of the AI Act

The AI Act will enter into effect in stages, with full application expected in 2026. The European Commission will develop guidance and delegated acts specifying various requirements for the implementation, including guidance on the interpretation of prohibitions, as well as a template for conducting fundamental rights impact assessments. It will be crucial for civil society to actively contribute to this process with their expertise and real-life examples. In the next months, we will publish a map of key opportunities where these contributions can be made. We also call on the European Commission and other bodies responsible for the implementation and enforcement of the AI Act to proactively facilitate civil society participation and to prioritise diverse voices including those of people affected by various AI systems, especially those belonging to marginalised groups.

5 flaws of the AI Act from the perspective of civic space and the rule of law

1. Gaps and loopholes can turn prohibitions into empty declarations

The AI Act introduces prohibitions of certain AI applications deemed unacceptable in light of fundamental rights. While it is important that this view is recognised by the Act, the prohibitions are riddled with loopholes, which calls into question how effective they will be in protecting civic space and fundamental rights. The AI Act also fails to ban some uses of AI advocated for by civil society, even when they have already been found to violate human dignity, freedom, equality, democracy, the rule of law or fundamental rights.

The most significant prohibitions include:

- Real-time remote biometric identification in public spaces (e.g. face recognition) in the area of law enforcement (with vast exceptions);
- Biometric categorisation to infer sensitive information about people (e.g. their race or sexuality), with a blanket exception for law enforcement;
- Creating or expanding facial recognition databases through scraping of facial

images from the internet or video surveillance footage;

- Emotion recognition in education or employment;

- Predictive policing when it is based on profiling individuals (as opposed to predicting crime based on criminal statistics from a certain neighbourhood) and only when it is not supporting an assessment by a police officer.

However, the prohibitions are likely to become empty declarations because of far-reaching exceptions.

When it comes to biometrics, the AI Act opens the door for the police to use real-time face recognition for the purpose of searching for missing persons or victims of abductions, preventing terrorist attacks or identifying suspects of serious crimes. These **extensive exceptions ultimately undermine the whole purpose of the ban** and could lead to infringements of the freedom of peaceful assembly, for example by allowing the authorities to identify, harass or arrest people taking part in protests. While under existing data protection laws national authorities have already issued decisions prohibiting specific uses of face recognition, we see the risk of EU governments using the AI Act to legitimise them through national-level legislation. Although such systems would technically have to undergo a fundamental rights impact assessment, they could be used without this safeguard in urgent cases and, as we explain in point 3 below, the public would in any case not have access to these assessments. **This creates the potential for abuse and does not constitute an accurate safety net against harmful application of biometric surveillance.**

Biometric categorisation systems that assign individuals to categories based on their biometric data (e.g. face, gait) would also not be prohibited in law enforcement. This includes systems such as that introduced in France for the purpose of identifying security threats during the 2024 Paris Olympic Games. Similarly, systems that purport to recognise emotions have only been banned in the areas of employment and education. Despite existing evidence of serious harm and doubtful scientific basis of 'emotion recognition', it will still be possible to use such systems in the area of law enforcement, migration or justice. The AI Act also fails to prohibit any use of AI in the area of migration, despite a mass of evidence of inherently discriminatory risk assessment systems or emotion recognition applied against asylum seekers, migrants and refugees. Risk assessment and identification systems that are discriminatory can be used at EU borders, and predictive analytics may also be used to forecast migration movements and facilitate pushbacks. Moreover, AI used by the EU's migration-related databases, like Eurodac, the Schengen Information System and ETIAS, will not have to comply with the law before 2030.

It's important to note that AI systems that violate other pieces of EU legislation, such as the GDPR, the anti-discrimination directive or the unfair commercial practices directive, are still not allowed, even if they are not explicitly mentioned on the prohibition list of the AI Act. However, these laws do not have

prohibition lists, and so enforcing them would in most cases require litigation and a case-by-case assessment of their general principles. In the past this has not been effective to prevent fundamental rights violations.

2. AI companies' self-assessment of risks jeopardises fundamental rights protections

Most of the AI Act requirements will apply to so-called 'high-risk' AI systems, which require close oversight to prevent societal and individual harm. However, an important loophole has been inserted into the Act, which practically allows companies and public authorities to go around the list of high-risk systems included in the Act. Here we name a few of such systems:

- Systems which rely on biometrics and which do not fall into prohibited practices (for example, some uses of remote biometric identification in law enforcement and all such uses in other areas or emotion recognition systems outside the areas of employment and education);
- Systems used for evaluating eligibility for public benefits;
- Polygraphs and systems used by law enforcement authorities to investigate criminal offences;
- Systems used by migration authorities to assess or evaluate the risk posed by visa or asylum applicants;
- Systems used for influencing the outcome of an election or voting behaviour.

The European Commission will review and, if needed, update this list once a year.

Providers of high-risk AI systems will be required to, for example:

- Assess and monitor risks to health, safety and fundamental rights;
- Ensure the use of high-quality data for training algorithms and prevent bias;
- Maintain up-to-date technical documentation and provide accurate and comprehensive information to deployers (e.g. public authorities procuring the system).

However, the final version of the AI Act includes a **dangerous loophole** that gives companies and public authorities alike the power to unilaterally decide that their AI system doesn't pose a significant risk to people's health, safety, or rights, even if they fall into one of the high-risk categories. If a provider chooses to exempt themselves, then all consequent obligations for deployers of such systems will similarly no longer apply. We are concerned about situations where AI providers argue that their system only performs preparatory tasks, even though it could influence decision-making about people. Furthermore, the responsibility to investigate all self-exempted AI systems would fall on the newly established national and EU authorities, which might lack the financial and human resources to do it effectively.

The final version of the AI Act is **likely to lead to a fragmented application of the law**, leaving it to Member States and national authorities to close the loopholes and monitor the self-assessment activities of AI developers and deployers. We will closely examine the guidelines and delegated acts in order to narrow the loophole created during the opaque trilogue negotiations.

The AI Act also specifies that people will have the right to submit complaints about AI abuses and receive information on the use of high-risk AI systems that affect their rights; however, competent authorities are not obliged to respond to such requests - they only have to take them into account when conducting investigations.

3. Standards for fundamental rights impact assessments are weak

The effective protection of civic space and the rule of law requires that public authorities and companies do not use AI without verifying that the technology does not violate fundamental rights or negatively impact democracy. Without such checks, AI systems can easily lead to racial discrimination in access to public benefits, unlawful surveillance of protesters, compiling innocent people in law enforcement databases or restricting the right to asylum. This is why we advocated for the inclusion of a mandatory fundamental rights impact assessment (FRIA) for public authorities and companies who plan to use high-risk AI systems, e.g. the police, courts, municipalities, banks or schools. The findings of such assessments should be publicly available so that the public and civil society can keep companies and public authorities accountable. Civil society and people affected by an AI system, especially those belonging to marginalised groups, should be able to meaningfully contribute their views and expertise in this process in order to improve the identification and mitigation of impacts.

We successfully convinced EU institutions of the need for FRIAs. However, we see three important shortcomings in the final text:

- While the AI Act requires deployers of high-risk AI systems to list potential impacts on fundamental rights, there is **no clear obligation to assess whether these impacts are acceptable or to prevent them, where possible** (deployers only have to specify which measures will be taken once risks materialise). As opposed to our recommendation from the open letter, neither will public authorities have to assess how a proposed system might impact the rule of law.

- The requirement to consult external stakeholders, including civil society and people affected by AI, in the assessment process was also removed from the final text. This means that **CSOs will not have a direct, legally binding avenue to contribute** to impact assessments.

- Although in principle deployers of high-risk AI systems will have to publish the

summary of the results, **this will not apply to law enforcement and migration authorities** who will not even have to reveal that they use risky AI in the first place. This information will only be included in a non-public database, severely limiting constructive public oversight and scrutiny. This is very concerning because the impacts on civic space and the rule of law are arguably most severe in these two areas, as evidenced in the past by the use of biometric surveillance against protesters or by subjecting asylum seekers to dystopian and unreliable biometric lie detectors.

Some of these shortcomings can hopefully be addressed by the newly established European Commission's AI Office, which will develop a template providing more detail on the practical implementation of FRIAs. We will closely monitor and contribute to this process.

4. The use of AI for national security purposes will be a rights-free zone

The opaque and unaccountable deployment of AI systems by intelligence authorities poses a serious threat to the rule of law and democracy. Regulatory loopholes, such as national security and law enforcement exemptions, could be exploited to weaken democratic institutions and processes and the rule of law, especially in those Member States where civic space, the rule of law and democracy have already been eroded.

Despite these concerns, supported by the UN High Commissioner for Human Rights, **a blanket exemption for national security was introduced in the AI Act** at the last stages of opaque trilogue negotiations. The AI Act will automatically exempt AI systems developed or used solely for the purpose of national security from scrutiny, regardless of whether this is done by a public authority or a private company. In practical terms, this means that governments could **invoke national security to introduce otherwise prohibited systems**, such as mass biometric surveillance. They could do so without having to apply any technical or fundamental rights safeguards, paving the way for the widespread use of poorly developed and inherently harmful systems. As observed in Member States such as France and Hungary, the justification of protecting national security has already been used to restrict the freedoms of association, assembly and expression to expand the surveillance powers of the police.

Such a broad exemption is not justified under EU treaties and goes against the established jurisprudence of the European Court of Justice. While national security can be a justified ground for exceptions from the AI Act, this has to be assessed case-by-case, in line with the EU Charter of Fundamental Rights. The adopted text, however, makes national security a largely digital rights-free zone. From the point of view of the rule of law, we are concerned about the opacity surrounding national security measures and limited, if not non-existent, oversight. It's unclear what pathways currently exist to verify if the use of an AI system for national security is justified and in line

with fundamental rights, and for the public or people affected to challenge that.

The EU has also set a worrying precedent regionally and globally. A case in point: the final text of the AI Act tipped the scales for including a similarly broad and unjustified exemption for national security in the recently finalised Council of Europe Convention on AI.

5. Civic participation in the implementation and enforcement is not guaranteed

Meaningful and accessible mechanisms for the engagement of civil society and people impacted by AI systems will be crucial for effective and rights-based implementation and enforcement of the AI Act.

The Act, however, does not go far enough to guarantee the right to participation. Notably, public authorities or companies will not be required to engage with external stakeholders when assessing fundamental rights impacts of AI. Individuals whose rights have been violated will have the possibility to file complaints, but CSOs will be able to represent them only when consumer rights are involved. In other words, CSOs could file a complaint on behalf of a group of people harmed, e.g. by credit scoring systems, but not on behalf of protesters whose civic freedoms have been violated by the use of biometric surveillance in the streets.

The only formal way for civil society to participate in the implementation and monitoring of the AI Act will be through membership in **the advisory forum to the newly established AI Office and AI Board**. The former will be set up within the European Commission to contribute to the implementation, monitoring and supervision of the AI Act, while the latter will gather representatives of national supervisory authorities enforcing the AI Act. The advisory forum, whose members should represent commercial and non-commercial interests equally, will assist these bodies in their tasks and provide recommendations. When setting up the advisory forum, it will be crucial for the Commission to actively facilitate and encourage meaningful civil society participation and to ensure proper representation of fundamental rights expertise.

The AI Act limitations showcase the need for a European Civil Dialogue Agreement

The legislative process surrounding the AI Act was marred by a significant lack of civil dialogue - the obligation of the EU institutions to engage in an open, transparent, and regular process with representative associations and civil society. To date, there is no legal framework regulating the European civil dialogue, although civil society has been calling for it in various contexts. Since the announcement of the AI Act, civil society has made great efforts to coordinate horizontally to feed into the process, engaging diverse organisations at the

national and European levels. In the absence of clear guidelines on how civil society input should be included ahead of the drafting of EU laws and policies, the framework proposed by the European Commission to address the widespread impact of AI technologies on society and fundamental rights was flawed. Throughout the preparatory and political stages, the process remained opaque, with limited transparency regarding decision-making and little opportunity for input from groups representing a rights-based approach, particularly in the Council and during trilogue negotiations. This absence of inclusivity raises concerns about the adopted text's impact on society at large. It not only undermines people's trust in the legislative process and the democratic legitimacy of the AI Act but also hampers its key objective to guarantee the safety and fundamental rights of all.

However, in contrast to public interest and fundamental rights advocacy groups, market and for-profit lobbyists and representatives of law enforcement authorities and security services had great influence in the legislative process of the AI Act. This imbalanced representation favoured commercial interests and the narrative of external security threats over the broader societal impacts of AI.

Contact

European Civic Forum
Rue du Congrès 13,
1000 Bruxelles, Belgium
(+33) (0)1 80 05 19 12
contact@civic-forum.eu

European Center for Not-for-Profit Law Stichting
Riviervismarkt 5, 2513 AM, The Hague, Netherlands
info@ecnl.org
(+31) 639 029 805

The Civil Liberties Union for Europe e. V.
Ebertstraße 2. 4th floor
10117 Berlin
Germany
info@liberties.eu
liberties.eu