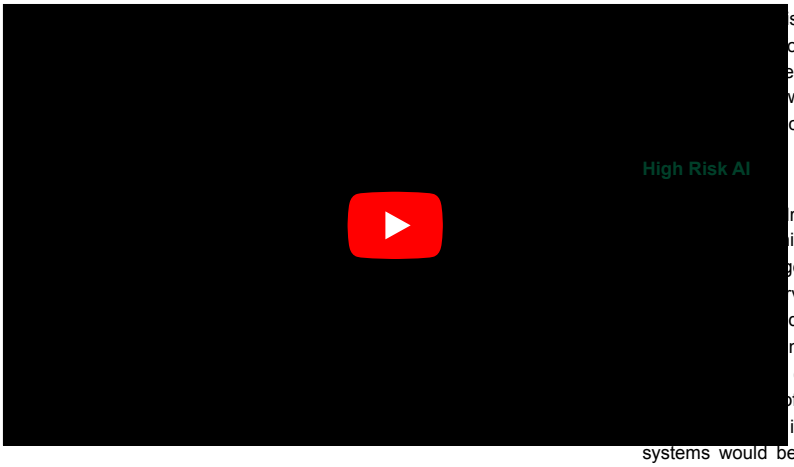
Protecting Fundamental Rights in the Age of AI: How Parliament's latest version of the EU's AI Act safeguards fundamental rights

Written by Florina Pop and Laura Grant

Introduction

As artificial intelligence (AI) technologies continue to advance, risks to fundamental rights undoubtably surface. Amidst this evolving landscape, the EU's Artificial Intelligence Act seeks to act as a safeguard to citizens' fundamental rights. The latest version was adopted by the European Parliament in June 2023 and the next step is the final trilogue negotiations between the Commission, Council, and Parliament, with legislators hoping to have the Act adopted as soon as early 2024. In this case, it will apply at the earliest in 2025.

In terms of fundamental rights, after the publication of the Commission's original proposal in 2021, several concerns were raised regarding rights protection by over 120 human rights and civil society groups. Arguably, Parliament's recent amendments significantly improve the safeguarding of fundamental rights in relation to AI, and these changes have been welcomed. We want to briefly explore some of the Act's major developments and any challenges that may remain regarding rights protection, particularly in the areas of non-discrimination, freedom of expression, and privacy.



Positive Updates to the Act – June 2023

It's important to note that one fundamental change made by Parliament is the definition of an "AI system", bringing it more in line with the OECD's definition and increasing legal certainty on what it is: "a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments."

Unacceptable AI

Arguably one of the most significant developments to the proposal concerning rights protection is Parliament's expansion to the list of prohibited AI systems/practices.

The AI Act takes a risk-based approach, categorising AI systems based on their level of potential risk from "low/minimal risk" to the highest level of risk deemed "unacceptable" in Article 5. There will be a full prohibition on developing and using AI systems that are intrusive and discriminatory, such as:

- "Real-time" remote biometric identification systems (facial recognition) in public spaces;
- "Post" remote biometric identification systems that could, for example, analyse security footage after an event, with the only exception being law enforcement in prosecuting serious crimes with judicial authorisation;
- Biometric categorisation systems using sensitive characteristics (gender, race, ethnicity, citizenship status, religion, political orientation);
- Predictive policing systems (based on profiling, location or past criminal behaviour);
- Emotion recognition systems in law enforcement, border management, the workplace, and educational institutions; and
- Creating facial recognition/biometric databases by untargeted scraping of images from the internet or CCTV footage.

The potential issues in using these systems concern a variety of fundamental rights. For example, using predictive policing means that certain individuals can be targeted, producing biased results that reinforce existing racial or ethnic profiling and discriminatory stereotypes. These systems can also undermine the right to presumption of innocence and underpin systematic inequalities, as a Fair Trials report 'Automating Injustice' points out.

In February 2023, the German Federal Constitutional Court declared predictive policing unconstitutional due to the risk of potential discrimination. The ban on real-time biometric identification is likely to ssue in negotiations, with Member States pushing for orcement in the Council's draft. Nevertheless, from a e, Parliament's landmark ban on these systems is a wards more stringent fundamental rights protection in chnologies.

raft, Parliament added additional AI systems to be igh-risk" category. This includes AI systems used by ge Online Platforms e.g. Instagram, Facebook etc., as rvices Act) to recommend content to online users, and during political campaigns to influence voters. It also n insurance, AI used by children, general-purpose AI, (like ChatGPT and deep fakes– think of those videos f various celebrities or politicians saying something it's not real: this is a deep fake). These generative AI systems would be required to highlight that content is AI-generated, and help users ascertain what is real versus fake.

Deployers (natural/legal person under whose authority the system is used) of high-risk systems now have additional transparency obligations placed on them, building on the Commission's version which focused primarily on **providers** (natural/legal person who develops an AI system with a view to putting it on the market/into service). The new obligations on deployers in Article 29 include protecting the fundamental rights of natural persons regarding AI decision-making. They must inform natural persons when they are subjected to these decision-making systems, their intended purpose, and the types of decisions made. Natural persons will also have the right to an explanation of an AI-made decision under Article 68c, increasing transparency around the use of AI in decision-making.

Going forward, under Article 29a, a **fundamental rights impact assessment** must be carried out prior to deploying a high-risk AI system. It is similar to a data protection impact assessment (DPIA)

under the General Data Protection Regulation (GDPR), which will be carried out in tandem if necessary. The assessment will ensure deployers state how risk mitigation will be undertaken before an AI system is put into use and will take into consideration feedback from the relevant stakeholders likely to be affected by the system. This addition was welcomed by civil society and human rights groups as it will allow increased safeguarding and risk management.

Redress and Remedies

In terms of redress and improved remedies, arguably Parliament's draft has made substantial improvements. The original text of the legislation did not contain any mechanisms for redress or remedies to individuals harmed by AI, which is now a welcome addition to the new draft. As mentioned above, individuals subjected to a decision made by high-risk AI have a right to an explanation if their health, safety, fundamental rights, socio-economic rights or other rights are adversely affected as per Article 68c. Additionally, anyone who believes they have been unfairly affected by an AI system can raise a complaint with the Member State's national supervisory authority (the MS of their residence, place of work, or place of infringement) under Article 68a. Failing that, they can seek judicial remedy. This combined with the AI Liability Directive should help further protect individuals. However, the question does remain as to the practicality of this redress system – how easy will it be for an individual to know they've been affected by an AI system, and to seek and afford legal assistance?

Fines

The Parliament's draft has upped the penalties considerably, from originally 6% of global annual turnover or €30 million for breaching a prohibited practice, whichever is higher, to 7% and €40 million. These figures exceed the penalties in the GDPR significantly and will no doubt act as a major deterrent when it comes to meeting obligations under the Act.

Remaining Challenges and Concerns

Despite the welcomed progress Parliament's draft has on fundamental rights protection, some challenges remain. Unfortunately, the amendments did not address the potential legal loophole in Article 6, which may allow developers of potentially high-risk systems to circumvent obligations. This is due to the wording and the threshold imposed by the Council, which allows developers/organisations to argue that if their system does not pose a "significant" risk to people's health, safety or fundamental rights, it is not considered high-risk. This could introduce legal uncertainty into the Act, and result in fragmentation across the EU with different interpretations of what is considered "significantly high-risk". Although guidelines will be provided specifying the circumstances in which significant risk will arise or not, it remains to be seen whether this wording will be amended during the negotiations phase to the Commission's original language to avoid this hurdle and prevent organisations escaping the obligations of the Act. Although we discussed the new prohibitions on real-time biometric data, concerns remain that this is not enough: calls for a total prohibition on all uses of remote biometric data by both public and private actors in both real time and post have been raised.

Conclusion and Next Steps

In the upcoming trilogue negotiations, it remains to be seen whether the differing positions of the Council and the Parliament can be reconciled. Regardless, it is imperative that the significance of safeguarding fundamental rights remains at the forefront of discussions. While AI presents a plethora of benefits and transformative possibilities, as Ursula von der Leyen said in her 2023 State of the Union address, *"we should not underestimate the very real threats [of AI]".* Serious challenges have severely encroached upon individuals' rights as we have discussed above.

However, the EU's AI Act is already *"a blueprint for the whole world"*, and balancing the advancement of AI with the preservation of fundamental rights is a delicate task that demands careful consideration. It's hoped that the coming negotiations bring a satisfying conclusion from a rights perspective.

Want to learn more about the AI Act and the legal challenges surrounding AI? Then join EIPA's upcoming online course from 25-26th October on ***Artificial Intelligence: Laws, Challenges & Opportunities****! More details can be found here:*

If you're passionate about AI and EU digital policy, make sure to sign up for our newsletter for updates on our upcoming courses. And in the meantime, check out:

- *our free online module on AI & EU Law: definition and developments,*
- *our last blog on An In-Depth Look at the EU's AI Regulation and Liability Directive*

The views expressed in this blog are those of the authors and not necessarily those of EIPA.