DIRITTI COMPARATI
Comparare i diritti fondamentali in Europa

WHATEVER IT TAKES? THE AI ACT REGULATORY CRUCIBLE

*Posted on 22 Gennaio 2024 by **Federica Paolucci***

Introduction

The European Union will seemingly be the first to adopt a regulation on Artificial Intelligence. After a 36-hour negotiating marathon, EU policymakers have reached a political agreement on the AI Act, the proposal for a regulation of the European Parliament and the Council on laying down harmonised rules on artificial intelligence. Although there are a number of uncertainties as to whether Europe will be able to create a globally applicable regulatory model, the AI Act indeed represents an archetype with which the use and application of artificial intelligence systems will have to be compared.

The European Union's AI Act, a landmark regulation on Artificial Intelligence, is on the horizon, marking a crucial step in shaping global AI governance. The actual shape of the text is the result of years of work, culminating when the Commission published the proposal in April 2021; then, the workload passed to the Council and the European Parliament. They both amended the text right up to the last vote by the latter in June 2023, which marked the beginning of the trilogues. The negotiations addressed 21 open issues, covering open source, foundation models, governance, national security, and prohibited practices. Though the press received the political agreement with great fanfare, the last word on the AI

Act has not yet been said. It is recent news that during the last COREPER (Committee of Permanent Representatives), France, Germany, and Italy voted against implementing the AI Act and pushed for further discussion in February's meetings. This does not mean that the AI Act will be blocked, but it is undoubtedly an indication that the agreement is being carefully considered by the member states, especially where they hope to have some leeway in their favour.
Thus, at the moment, it is impossible to make any sort of predictions about the content and the outcome of the finalised version. Besides the Q&A published by the Commission and the press release disseminated by the European Parliament, the content of the agreement is still kept secret by the institutions (in fact, the last documents available date back to the agreement reached by the European Parliament at first reading). For this reason, this comment will briefly identify the main features of the document, on what we know so far, and will attempt to recapitulate the changes that have taken place with respect to the regulation of facial recognition uses, which were, among others, the subject of intense debate at the amendment and trilogue stage.

The AI Act ID card

The versions of the AI Act highly differ from one another, as scholars pointed out. Starting with a robust market-oriented approach from the European Commission, the Council and the European Parliament tried to temperate this direction by adapting the initial proposal to the value framework of the Union – i.e., further elaborating the mechanism of the fundamental rights impact assessment – and to the challenges uprisen during the institutional work.
On the first aspect, the AI Act relies on a conceptualisation of AI regulation that pursues innovation – e.g., by regulating the development, marketing and use of this technology – while protecting fundamental rights. The Regulation aims at facilitating the 'placing onto the market and the putting into use and service of artificial intelligence in conformity with Union values' (Rec. 2 and 3), trying to contrast the excessive and uncontrolled use of AI while also looking at its technological and economic value towards market consistency.

On the second aspect, it is worth mentioning that the AI Act derives its normative technique from the Reg. EU 2016/679, the General Data Protection Regulation (hereafter, GDPR), based on a risk-based approach. The Commission had already presented its interest in pursuing an approach to ensure the development and uptake of lawful and trustworthy AI through 'risk-based' and proportionality assessments in the 2020 White Paper on Artificial Intelligence. According to this model, the intensity of the rules, compliance measures, and constraints imposed differ depending on the risks derived from a given AI system or its use. Under the GDPR, this system made possible the protection of fundamental rights through the regulation of protection of the internal market and the creation of enforcement mechanisms reaching well beyond EU borders. As a matter of fact, the choice of high-risk use cases seems to be very episodic and appears to be a reaction to the challenges mentioned above. Challenges that, as in the case of ClearviewAI and the rapid escalation of ChatGPT, made the legislator consider these AI systems more carefully. While it is positive that, during the regulatory design phase, it swiftly addressed a pressing issue that posed a significant risk to individual protection, it prompts contemplation about what will transpire once the process concludes and the text is finalised. Will the AI Act be trustworthy, stretched and future-proof enough to be applicable to new or no popular uses of artificial intelligence? This holds particularly true if one considers the need for mandatory AI safety standards and the reconciliation with other normative frameworks – e.g., product safety – on which it is hoped the trilogues focused.

What happened to face recognition technologies?

As far as what was publicly shared, one of the topics that heated the debate in the trilogues has been the regulation of biometric recognition technologies, of which the most infamous use is face recognition (FRT): a technology that enables automatic identification and recognition of an individual both real-time and *ex post.* This AI use became particularly known to the general public after the Clearview AI scandal and grasped the EU legislator's fears due to its potential in law enforcement.

Thus, the regulation of face recognition technologies has undergone

concrete and significant turns. The AI Act is imposing regarding FRT dedicated norms that will not just complement the applicability of the previous ones but will stand over them. Therefore, while providing that the rules in question must 'continue to comply with all requirements resulting from Article 9(1) of Regulation (EU) 2016/679, Article 10(1) of Regulation (EU) 2018/1725 and Article 10 of Directive (EU) 2016/680 – Law Enforcement Directive (LED) – as applicable' (Rec. 24), the AI Act is strictly mandating the conditions upon which FRT can be placed in the market and put into service.

Considering the potential backlashes on the protection of fundamental rights of this technology – primarily but not exclusively, the right to privacy and data protection as protected by the CFEU – FRT was labelled with the highest level of risk. As mentioned above and observed by scholars, the EU has followed this approach in various policies targeting the digital ecosystem to adapt the enforcement of rules based on concrete risk scores. Unlike the GDPR, it does not leave concrete evaluations of risks to the programmers or deployers of given systems. The AI Act impose an *ex-ante* evaluation of risks that, as anticipated, makes one wonder about its capability to become a 'framework of compliance' that does not overburden the AI programmers and does not excessively impair innovation.

Speaking of facial recognition technology, this falls under the 'unacceptable risk' label, as anticipated. Besides the LED and the GDPR, the proposal builds on the soft law documents, in particular, on the White Paper on AI, the recommendations of the 'High Level Expert Group on AI', as well as the international guidelines, such as those of the CAHAI elaborated within the Council of Europe.

Therefore, the AI Act was awaited to clarify the application of FRT within the EU. The purpose was to create a proportional approach to balance the safety and protection of fundamental rights without blocking them. Hence, while waiting for the final text, it is good to recapitulate the approach that the European Union has pursued so far regarding the regulation of FRTs to understand the outcome of the negotiations better.

First, the Commission's proposed approach was to consider the use of

'biometric identification systems' particularly intrusive, and it established a few exceptions, almost based on the GDPR's one, art. 9. Second, the Council's compromised text added the distinction between 'real-time' and 'remote biometric identification systems' and extended the list of objectives for law enforcement to use 'real-time' biometric identification. Lastly, the European Parliament's compromised text provided for further harmonisation while recognising the risks related to the use of FRT.

If, initially, the proposed text distinguished between 'the placing on the market' and the 'putting into service' of FRT, the EP compromise text is ripped off it. However, it still distinguishes biometric identification systems from 'remote' (Art. 3, para 36) to 'real time' (Art. 3, para 37). As was observed by other scholars, the distinction creates more confusion than clarity. This applies also to the list of exceptions to the general prohibition of using biometric systems in publicly available spaces. Notably, the Commission's proposal allows for Member States to authorise specific uses, such as to prevent serious crimes, search for missing children, prevent a particular or imminent to the life or physical safety of natural persons, and the detection, localisation, identification, or prosecution of a perpetrator of a crime, or suspect of a crime, with a sentence of at least three years. Lastly, the prohibition does not touch on the use of 'remote biometric identification' for non-law enforcement purposes, which regulation falls under the GDPR.

From this fast overview, two main issues are evident. First, the AI Act does not list criteria for when AI poses unacceptable risks to society and individuals; it just states the presumption of risk. As scholars pointed out, besides the listed prohibited uses, further expansion of Art. 5 scope of application will amount to an amendment of the Act. This choice is considered arbitrary and worrisome since it only examines part of the AI life cycle.

Secondly, this lack of clarification leads to the biggest challenge of the AI Act, which seems to be its enforceability. Thus, even though the EP version of the text is under Art. 59, imposes on the Member States an obligation to establish or designate a national supervisory authority (NSA) that will act as market surveillance authority; it needs to be better specified how

the centralisation of this system will work, considering that Member States have different attitudes to the use of FRT – i.e., France is trying to apply FRT in the next Olympics.

Conclusion

In the press release of 9 December 2023, the European Parliament specified that a deal was found on the banning of FRT use with respect to biometric categorisation (together with emotion recognition), but it also introduces exemptions for law enforcement agencies, and exclusions of sensitive operation data from transparency requirements. Nonetheless, this approach will seemingly influence the use of FRT, even beyond the AI Act, both from a territorial and material scope of application. As has been repeatedly stated, all judgment is suspended in view of the actual publication of the text. What can still be said, however, is that the compromise has made proportionality prevail at the expense of the bans proposed by Parliament. The difficulty for the legislator will now be to construct the safest of balances that can avoid the creation of invasive surveillance systems. The EU still needs to prove that it did 'whatever it takes' to protect fundamental rights.