DIRITTI COMPARATI
Comparare i diritti fondamentali in Europa

AI LEGISLATION IN FLUX: TRACKING EVOLVING MODIFICATIONS OF THE AI ACT

Posted on 19 Settembre 2023 by ***Federica Fedorczyk***

It was back in 2021 when the EU Commission tabled a 'Proposal for a regulation laying down harmonized rules on artificial intelligence' with the specific object, among the others, to ensure that AI systems placed and used on the Union market are safe and respectful of existing law on fundamental rights.

The normative choice of the Regulation stems from the imperative for consistent legislation and the necessity to establish a market environment that fosters innovation while safeguarding the rights of citizens. It reflects a commitment to uphold the digital sovereignty of the European Union, thereby ensuring that Member States have limited room for independent action.

The Proposal strived to balance the numerous risks and benefits the use of AI can provide, using a risk-based approach. The idea behind the risk-based approach can be visually represented by a risk pyramid: at the top there are the applications that are prohibited because they pose an unacceptable risk; then there is the main core of high-risk systems, which, although risky, enable important functions and are therefore allowed at certain conditions; there are then limited risk systems, that will have to comply with 'minimal transparency requirements'; and at the bottom there are minimal or no risk systems, which are allowed without

restriction.
After the Commission adopted the Proposal on 21 April 2021, the Council unanimously adopted its General Approach on 6 December 2022. In May 2023, the European Parliament introduced some amendments, and recently, on 14 June 2023, these amendments were adopted with a substantive majority vote, giving start to the Trilogue negotiations. Once approved, after the end of Trilogue process, the AI Act will be the world's first comprehensive rule on AI.
Comparing to the Commission's version, the Parliament's version contains different changes that mainly concern the definition of AI, the new regulation of foundation models, the extension of prohibited AI systems, AI high-risk classification, the extension of the list of high-risk uses cases, and the introduction of additional and specific obligations on specific subject. Furthermore, the Parliament's proposal increases the penalties for violating the AI Act.
A groundbreaking part of the document approved by the EU Parliament concerns the regulation of Large Language Models (LLMs) also referred to as 'foundation models' or 'large generative AI models' (LGAIMs). In response to the recent proliferation of LLMs in the market and given the uncertainty about the way in which foundation models will evolve, the Parliament has imposed obligations on the providers of foundation models. More specifically, generative foundational models call for increased transparency requirements. Indeed, where contents such as complex text, images, audio or video have been generated by AI, this information must be disclosed in a timely, clear and intelligible manner. The provider must also provide adequate safeguards to ensure that the generative system does not produce content that is illegal or in violation of European standards and must publish summaries of copyrighted data used for training purposes. These additional requirements are justified by the fact that precisely because foundational models require a lot of data, their developers often rely on training data available on the Internet, which is often of poor quality. In fact, the contents generated by these models are frequently incorrect or biased (think of the problem of fake news generated by models such as Chat GPT).

However, scholars have raised concerns: compliance with the required obligations, including the establishment of a comprehensive risk management system prescribed for high-risk uses, seems almost impossible to achieve.
Indeed, providers would be required to identify and analyze all known and foreseeable risks that are most likely to occur to health, safety and fundamental rights, and, based on this analysis, they would have to identify mitigation strategies for each risk.
Consequently, due to the challenges of adhering to the new AI Act regulations, it can be expected that only large and financially robust players such as Google, Meta, and Microsoft/Open AI would be able to afford the costs associated with developing LLMs that are approximately compliant with the AI Act. This would result in a limited pool of companies capable of meeting the regulatory requirements, potentially leading to reduced competition and innovation in the field.
Another significant change in the Parliament's version is the expansion of the list of prohibited AI systems. It is the first of its kind in Europe and the first major ban on such system worldwide, and includes: 'real-time remote biometric identification systems in publicly accessible spaces; post remote biometric identification systems, with the only exception of law enforcement for the prosecution of serious crimes and only after judicial authorization; biometric categorisation systems using sensitive characteristics (e.g. 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, workplace, and educational institutions; indiscriminate scraping of biometric data from social media or CCTV footage to create facial recognition databases (violating human rights and right to privacy).'.
The ban reflects a growing recognition that AI systems must be developed and used in a manner that is both ethically responsible and respectful of fundamental rights. It paves the way for a more transparent, accountable, and equitable approach to law enforcement, promoting a system that upholds fairness and justice. However, in concrete terms, the ban will

probably have demanding consequences. For instance, once the ban on predictive policing will become effective, law enforcement authorities and agencies will be obliged to cease the use of all the predictive policing tools already in use in EU. Therefore, it is possible that authorities may mandate the removal of such tools from operational systems and databases. This action would probably involve first dismantling or reconfiguring the existing infrastructure that supports predictive policing and then providing regular reports on the implementation and progress of the ban.

The Parliament has also adopted some modifications concerning the high-risks AI systems: first, while the Commission proposed to automatically categorize as high-risk all systems in certain areas or use cases, the Parliament adds the additional requirement that these systems must pose a 'significant risk' (Article 3) to be qualified as high-risk. Second, the Parliament has expanded the category of high-risk applications, to include those AI systems that pose a significant harm to people's health, safety, fundamental rights or the environment and those that have the power to influence voters in political campaigns and in recommender systems used by social media platform.

Another change made by the Parliament concerns a new obligation on 'deployers' - previously referred to as 'users', namely those who use AI systems for professional purposes- of high-risk AI solutions. They must undertake a comprehensive 'fundamental rights impact assessment' (FRIA) before putting their systems into use: the aim is to ensure that fundamental rights are protected and the 'minimum' of what the FRIA should include is broadly described in the new Article 29(a).

The ones just described are only the main changes presented in the Parliament's version of the AI Act. It is important to note that these changes will probably be subjected to further modifications during the Trilogue. However, even at this stage, it is possible to analyze the direction that the EU is taking in terms of regulation and the reactions from stakeholders and civil society.

It should be premised that all the amendments regarding the prohibited systems and the high-risks system were not entirely unexpected: they

have been the result of various comments and criticisms that arose over the past year following the text adopted by the Commission.
Indeed, already in 2021, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) jointly expressed their support for the European Commission's proposal on AI, but at the same time they raised specific concerns. They emphasized the need to align the concept of 'risk to fundamental rights' with the principles set out in the GDPR and they called for a comprehensive ban on the use of AI for automated recognition of human features in public spaces, regardless of the context.
Therefore, it is no surprise that the Parliament has done similar changes and has banned the use of biometric identification for both real-time and ex-post use (except in cases of severe crime and pre-judicial authorization for ex-post use) and not only for real-time use, as proposed by the Commission.
However, many representatives of civil society, while appreciating the changes adopted by the Parliament, have pointed out that too little has been done to ensure respect for fundamental values and human rights and claimed a total ban of facial recognition systems.
Furthermore, significant criticism has emerged regarding the Parliament's failure to address the concerning absence of prohibitions on the use of AI systems in the context of migration. In the Parliament's version, there are no explicit bans on discriminatory profiling, risk assessment systems, or profiling intended to restrict, prohibit, or hinder border movements. This 'omission' is seen as a favorable signal to reinforce surveillance system at the borders, further exacerbating the concern surrounding privacy, human rights and equal treatment.
However, the list of prohibited AI practices could be expanded in the future to cover all systems that are proven to pose an unacceptable risk of violating fundamental rights. Such a possibility is provided for the high-risks system, and now also for the list of prohibited systems.
Indeed, the legislative process is not over: in the coming months, substantial negotiations are expected to take place between the Commission, the Council and the European Parliament, that may be

influenced by the looming 2024 European Parliament election scheduled for June 2024. The debate surrounding AI has proven to be far from unanimous, and one highly contentious issue stands out: the real-time biometric identification of individuals in public areas. While the European Parliament seems keen to ban this practice entirely, several Member States are advocating for retaining exceptions, primarily for law enforcement purposes.

The ultimate objective remains to have a final version before the upcoming elections and Spain has made it clear that AI is a top priority during its presidency. Nonetheless, there are numerous complexities and challenges that still need to be addressed in this ongoing process.