EIPA Briefing 2021/5

The Artificial Intelligence Act Proposal and its implications for Member States

Martina Anzini

Introduction

Artificial Intelligence (AI) is a family of technologies that can optimise existing processes or enable brand-new activities, for example by improving predictive models or by personalising the delivery of services. It presents major new opportunities, but also serious risks.

As part of its digital agenda, the European Commission has therefore proposed harmonised rules regarding AI applications, emphasising that its approach is shaped by EU values and risk-based, ensuring both safety and fundamental rights protection. However, the appropriate balance between fundamental rights protection and public security is expected to remain a controversial issue during the whole legislative process. The governance and enforcement arrangements are also likely to attract particular attention. This Briefing provides a concise overview of the proposal and highlights its main implications for EU Member States.

The AI Act: an overview

Prohibition of unacceptable AI practices

The Commission proposes to ban completely AI systems that:

- manipulate persons through subliminal techniques or exploit the fragility of vulnerable individuals, and could potentially harm the manipulated individual or third person;
- serve for general purposes of social scoring, if carried out by public authorities; or
- are used for running real time remote biometric identification systems in publicly accessible spaces for law enforcement purposes.

Regulation of high-risk AI systems

High-risk AI systems are defined as those that:

- are part of a product falling under the EU product safety regulation, such as toys or medical devices; or
- belong to a list of stand-alone high-risk AI systems laid down by the proposal, such as AI systems assessing the creditworthiness of individuals or used in the context of recruitment.

Providers of such applications must maintain sound risk management systems. They must feed the AI system with training, validation and testing data that meets specific quality requirements and is handled through appropriate data governance and management practices.

Users must comply with the instructions and report to the provider/distributor any serious incident or malfunctioning, which could lead to a breach of fundamental rights.

Conformity assessment

If the high-risk AI system is part of a product which is subject to a third-party conformity assessment under the EU product safety framework, compliance will be addressed in the context of that conformity assessment. If not, compliance can be self-assessed by the provider and demonstrated by reference to either the relevant harmonized standards or the common specifications adopted by the Commission.

Transparency obligations for potentially deceptive AI systems

People can be deceived by some systems (such as chatbots) into thinking that they are dealing with a human. In those cases, the proposal merely imposes transparency requirements to ensure that the affected person is aware of being exposed to an AI application.

Ex post market surveillance

Providers of high-risk AI systems must establish and document an appropriate post-market monitoring system to continuously check compliance with regulatory requirements. They must report serious incidents and malfunctioning to the market surveillance authority of the Member State where the incident or the associated breach of fundamental rights occurred.

Market surveillance authorities must require the relevant operators to take appropriate measures or even to withdraw the AI system when the AI system is in breach of the regulation or when the AI system, while in line with the regulation, presents a risk for health, safety, human rights or a public interest.

Governance

National Competent Authorities must be appointed for the 'application and implementation' of the AI Act. A National Supervisory Authority is to be designated among them to act as market surveillance authority.

The consistent application of the Regulation is to be ensured by a European Artificial Intelligence Board, chaired by the Commission and composed of the European Data Protection Supervisor and representatives of the national supervisory authorities. The Board collects and shares best practices and takes a position on emerging issues for the implementation and enforcement of the regulation.

Penalties regime

Fines for non-compliance can be very high, up to EUR 30,000.000 or, if the offender is a company, up to 6 % of its total worldwide annual turnover for the preceding financial year.

The impact of the AI Act on national legal and administrative systems

Pre-emption of national AI regulatory frameworks

The AI Act, in its current form, would make it impossible for Member States to regulate this technology at national level. This is particularly relevant considering how wide a concept of 'AI system' the regulation embraces.

Some scope for regulatory intervention is nevertheless left to Member States. AI applications for military use are not covered. Also, the proposal leaves room for national discretion in adjusting the

AI regime to the national contexts. A notable example is the penalties regime, which is for the Member States to define, subject to compliance with the Regulation and provided that sanctions are effective, proportionate and dissuasive. Also, Member States can decide not to subject public authorities and bodies to administrative fines.

Monitoring and enforcement

Monitoring and enforcement are the responsibility of the Member States, although the Commission has a role in preventing 'under-enforcement'. Oversight on the compliance of conformity assessment bodies (known as 'notified bodies') with the Regulation is a task for national authorities too, but the Commission can launch an investigation whenever it believes that one of those bodies is in breach of the Regulation. If it identifies a breach, the Commission can request the Member State to adopt 'corrective measures'.

Moreover, each national market surveillance authority must report to the other national authorities and to the Commission any measure it takes to prohibit an AI system, restrict its use or impose its recall. If any other national authority or the Commission disagrees with the measure, the Commission is to consult the national authority which adopted it, and the relevant operator. If the measure is declared justified, all national authorities will have to make sure that it is complied with in their national territory. If the measure is found not to be justified, the national authority that adopted it will need to withdraw it.

This 'Union safeguard procedure' is intended to make up for the lack of a consistent mechanism for the allocation of competences between national market surveillance authorities, such as the identification of a single competent authority for an AI operator that is active on several national markets. However, this also prevents national market surveillance authorities from operating independently. Indeed, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have highlighted that the AI proposal is unclear as to whether national supervisors are meant to be independent, and have proposed that such a requirement be explicitly included in the text.

As to the adaptation required from the national institutional setting, it seems modest. It is not necessary to establish new authorities. However, it could be necessary to provide additional resources to the authorities involved. Indeed, the proposal provides public authorities with significant powers, such as accessing the 'source code' of the AI systems. Since such powers would be empty in the absence of competent agents and appropriate technical facilities, the Regulation expressly requires that those are made available to national authorities.

Compliance with the prohibitions and regulatory requirements

If the current text of the proposal were approved, public bodies, law enforcement authorities and the judiciary would be deprived of the possibility to use AI systems that the Regulation qualifies as unacceptable, except for specific cases.

Also, public operators can be affected by the proposed regulation as providers and users of AI systems. The obligations listed above thus fall on public authorities, depending on the level of risk associated to the AI system under consideration and, when relevant, on whether they qualify as 'users' or 'providers' of such AI system.

Conclusions

If approved in its current form, the AI Act would affect national legal and administrative systems in two main ways. Authorities would be required to have appropriate human resources and technical tools. The Act would also influence modernisation of the administrative and judicial activity and of law enforcement. Indeed, the proposed Regulation curtails options, subjects the use of AI systems in some areas to strict regulatory requirements and makes modernisation efforts relying on AI more resource-intensive.

However, it must be emphasised that the Commission wants not only to regulate the use of AI, but also to promote it. In this regard, the review of the coordinated plan on AI, originally adopted by the Commission and the Member States in 2018, deserves to be mentioned. One of the initiatives is a network of European Digital Innovation Hubs. The network, to be jointly funded by Member States and the Commission, is meant to help the public sector (and SMEs) to scale up their use of AI, thanks to the technical expertise (including training and skilsl development) that such Digital Innovation Hubs offer. Also, Member States are encouraged to use funding under the Recovery and Resilience Facility to increase their investment in AI.

The interplay between the various initiatives of the Commission in the area of AI is meant to vigorously, as well as safely, promote this technology in Europe. Public administrations seem to be right at the centre of those efforts.