WilhelmGilliéron
AVOCATS

Artificial intelligence regulations: an overview

2023 will have been the year in which the general public became aware of the potential of artificial intelligence (AI) systems, particularly since the launch of ChatGPT.

Faced with the challenges posed by AI, regulatory efforts are taking shape, starting with the proposed European Regulation on AI, whose final trialogue session will be held on December 6, 2023. While many hope to see this regulation come into force in 2024, voices are being raised to doubt this in view of the important points on which a consensus is struggling to emerge, particularly when it comes to foundation models.

Nevertheless, as the year draws to a close, it seems appropriate to provide an overview of our efforts in this area, without presuming to go into detail.

I.   EU AI Act

The European Union appears to be leading the way in this area. Once it comes into force, and like the RGPD, the AI Regulation will have extraterritorial effects, since it will apply to any supplier marketing such systems within the EU, as well as to users whose results (*outputs*) following the use of such systems would be used within the EU. Many Swiss companies will therefore be subject to this regulation.

The regulations are based on risk assessment, distinguishing four categories of systems:

1.   Systems presenting an unacceptable risk are banned, by which the proposal means systems using subliminal techniques, those exploiting the vulnerability of certain groups (children, the elderly) or those used to calculate social credit. It remains to be seen whether the use of real-time biometric identification systems in public spaces should be banned outright, or whether certain exceptions should be made to this ban, a point on which the opinions of European institutions differ.

2.   The proposal defines high-risk systems as those implemented in sectors considered particularly sensitive (technical infrastructures, education and training, human resources, access and entitlement to essential services, law enforcement, administration of justice and democratic processes, border control and migration), or those integrated into products already subject to certain safety regulations (such as toys, transport, etc.). The possibility of obtaining certain exceptions, and the conditions of these exceptions, remains a point of discussion.

3.   Limited-risk systems, essentially subject to a transparency obligation, including chatbot systems, those capable of detecting emotions, and generative tools such as LLMs (large language models). Here too, the exact way in which these systems will be regulated remains under discussion, and could be the major sticking point, with France, Germany and Italy now opposed to the issue being addressed within the Regulation.

4.   Systems presenting little or no risk, which are not covered by the proposal, even if the adoption of codes of conduct by the players concerned is recommended.

The regulations essentially target high-risk systems, imposing certain requirements on developers and, to a lesser extent, on distributors, importers and users of these systems during their development and marketing.

Without going into detail here, these developers will have to set up a risk assessment and quality management system, provide technical documentation and information on the data used, and register in a database maintained by the European Commission. In any event, the system should always be capable of being stopped by human intervention.

The question of how the regulation is to be implemented remains a matter of debate. While the Parliament is in favor of appointing one authority per country and a central authority at European level, the Commission is in favor of the possibility of having several competent authorities within a single country, while the institutions differ as to the weight that the European body should play in relation to the national authorities.

Echoing the approach adopted for the RGPD, the regulations provide for hefty fines in the event of non-compliance, since the fine can go up to the greater of 6% of global sales or €30 million in the event of marketing a prohibited system, respectively 4% or €20 million in the event of failure to meet most of the obligations.

Negotiations are being closely monitored, but have not yet reached a conclusion, with some fearing that the Regulation could become a brake on innovation, favoring American and Chinese competition to the detriment of Europeans, particularly SMEs, by imposing overly stringent requirements that would prove too costly to comply with. To be continued in the coming days.

II.   USA

On October 30, 2023, President Biden issued an Executive Order entitled " *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence* ". The aim of this Executive Order is to foster innovation while ensuring safety, privacy and fairness in the development and use of AI in the United States, while encouraging international cooperation.

Unlike the European approach, the US approach is not to pass a federal law that would be binding on everyone, but to establish a set of

principles and guidelines that federal agencies must adhere to when designing, acquiring, deploying and overseeing AI systems. Particular emphasis is placed on creating strict standards for the screening of biological synthesis, helping to prevent the risks associated with the use of AI in the design of hazardous biological materials. Added to this is the encouragement of a framework for cooperation and coordination between the various stakeholders, including the private sector, academia, civil society and international partners.

While commendable, the decree highlights the sectoral approach still favored in the U.S. over the horizontal approach sought in the European Union, and the absence of any desire to adopt a formal law at federal level. It is therefore to be feared that the various states will continue to adopt scattered legislation in different areas, such as the State of Colorado in the field of insurance or the City of New York in the field of employment, resulting in a patchwork that is difficult for companies to follow. To be watched out.

III.   China

In China, the Internet watchdog is the *Cyberspace Administration of China* (CAC), a powerful authority in this field. The CAC was one of the first agencies to adopt regulations on specific issues. This was the case for :

- March 1st, 2022: regulation of algorithmic recommendations.

- November 25, 2022: regulation of synthetic data.

- July 13, 2023: regulation of generative tools.

The latter regulations include concerns common to Western countries, such as transparency, security and data governance to avoid bias, while others are specific to China, such as the ban on inciting social unrest and the need to obtain a license from the CAC. Of particular interest is the requirement for developers to take measures to combat addiction, or not to develop algorithms with such an objective (it should be noted that such a requirement only applies to in-house developments, not those destined for foreign markets). The regulations are backed up by criminal sanctions, including the possibility for the CAC to impose a penalty if it deems it appropriate, even if the regulation does not so provide...

In addition to these regulations, China has announced its intention to adopt a general law governing the development and deployment of these systems.

IV.   Other

Legislative efforts are also taking shape to varying degrees in Brazil, Mexico, Japan and Singapore. Although there is no law in the formal sense enacted or in the process of being enacted in Singapore, this state has set up an interesting governance framework around the adoption of these systems called "AI Verify".

This framework, like the one adopted in the USA by NIST, is an important frame of reference, which some experts consider, along with the many standards adopted today by institutes such as ISO/IEC, to be more appropriate tools than the adoption of laws in the formal sense.

V.   Conclusion

All in all, we can see that numerous initiatives are taking shape to frame the development and deployment of AI systems within different countries.

While approaches differ, a certain uniformity is emerging with regard to the main principles, as reflected by the [G7](#)'s adoption of an agreement on the subject in [Hiroshima on October 30, 2023](#).

Awareness of the challenges involved in the development and deployment of these systems, highlighted at various recent summits held in November 2023, should lead to greater international cooperation in this area.

While it is difficult to know what the best approach is, it seems clear that a purely national approach is a very poor safeguard, and a source of questions from the point of view of international competitiveness, as reflected in the discussions surrounding the adoption of the AI Regulation within the European Union.

We can only hope that, after the isolated steps taken in 2023, 2024 will be the year of international consultation and cooperation in this field. To be continued.