Mouvement des Entreprises de France

Proposal for a regulation on Artificial Intelligence (AI Act)

MEDEF comments

July 2021

On 21 April 2021, the European Commission proposed a new regulation on Artificial Intelligence (AI) aiming at providing a harmonized legal framework at European level.

It is essential today to build a European ecosystem for innovation and AI that respects European values. The health crisis has indeed revealed the importance of technological and digital infrastructures and the fact that Europe must equip itself with such infrastructures, in particular AI. To do this, the development of AI must be made available to all companies, whatever their size, whatever their resources.

Indeed, to build a trustworthy, efficient and sustainable AI framework, regulations must benefit citizens, but also European businesses by allowing them to develop and benefit from cutting-edge technologies in order to remain competitive.

This European initiative is all the more important as it aims to prepare the ground for AI regulation worldwide.

While MEDEF welcomes the work carried out by the European Commission and considers that **the risk-based approach adopted in the proposed regulation is the best possible approach insofar as it promotes confidence in AI, this proposal raises many concerns and questions, in particular with regard to:**

- **the legal uncertainty** linked to very broad and insufficiently precise definitions;
- **the lack of consistency, or even the incompatibility,** of this proposal with other European texts (GDPR, Machinery Directive, etc.);
- **the sometimes very heavy or even disproportionate obligations.**

On general provisions

The risk-based approach of the European Commission seems to be the best possible approach as it fosters confidence in AI without hampering its responsible development. It is entirely relevant to define the obligations and requirements according to the risk (high or low risk) of the technology and its use.

Nevertheless, **it is essential to keep a margin of innovation**. Particular attention must therefore be paid to definitions, in particular those of AI systems and high-risk systems, because the related obligations and requirements are very onerous and difficult to implement. **Clear and sufficiently precise definitions are all the more important as they will be called upon to serve as references in other texts. They must therefore not lead to the creation of legal uncertainty**.

Some concepts, such as "known and foreseeable risks", "reasonably foreseeable misuse", "generally acknowledged state of the art", are for example very unclear and can therefore create legal uncertainty leading to different interpretations according to countries or authorities.

On the definition of artificial intelligence

- **Article 3 (1)** defines an AI system as "*software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*".

  If we understand the Commission's objective of making this regulation neutral and adaptable to technological developments, **the current proposed definition of AI (and the list of techniques in Annex I) is very broad in that it can include all types of systems or software applications that do not involve the same risks.** The inclusion of such systems or applications within the scope of the regulation would risk hampering innovation in technology companies, especially smaller ones. However, in a context of international competitiveness, it is essential to encourage technological development and not to prevent SMEs from accessing these markets.

  In general, if AI can involve risks in its implementation, it is mainly with regard to its direct or indirect impact on individuals. However, it should be remembered that many uses of AI systems have little impact on individuals. This is the case, for example, with AI methods for internal modeling needs (for example ALM models for the banking sector) or for corporate scoring.

  It should also be noted that some AI systems even have the potential to increase the productivity of companies or the well-being of the workforce, in particular by efficiently distributing tasks between humans and machines, by providing tools for skills development and providing access to better working conditions, in particular health and safety.

  In this sense, it would be useful, on the one hand, not to put all systems or applications to the same scale. A benefit / risk balance of technological developments should be put in place in order to promote

innovation. On the other hand, the scope should also be reduced by excluding, for example, statistical tools.

- **Annex I** lists the different techniques or approaches that may fall under AI. While some are indeed intrinsically linked and identified with AI (paragraphs a and b), others can also be used in applications that do not fall under AI (such as the methods mentioned in paragraph d). Indeed, "*statistical approaches, bayesian estimation, search and optimization methods*" have been used for decades in various fields of research outside AI.

  Subparagraph d should therefore be deleted so as not to include in the scope of this regulation applications which do not fall within the scope of AI.

- In addition, **Article 4** provides for the possibility for the European Commission to adopt delegated acts to modify the list of techniques and approaches defined in Annex I. Thus, the definition of AI may need to evolve, which is a source of legal uncertainty because it will pose problems of application in the risk-based approach.

On the scope of the regulation

Article 2 expressly excludes AI systems for exclusively military purposes from the scope of the proposed regulation.

Dual-use AI systems (civilian and military) are not mentioned and **should also be excluded from the scope, in particular by deleting the term "exclusively" so that all AI systems for military purposes are excluded from the scope.**

On consistency with other texts

- It seems that the proposal for a regulation was drawn up in disregard of the fact that many regulated products incorporating AI as a safety function, in particular machines subject to Directive 2006/42/EC, are today used in several sectors. However, the methodology adopted by the Machinery Directive is to carry out a risk analysis in order to take the appropriate protective measures. **The proposed regulation, for its part, automatically considers certain AI systems to be high risk, without consideration for the risk analysis carried out by the company under the terms of the Machinery Directive**, which is contradictory.
- Insofar as data is very important for the development of AI, **it is necessary to articulate the proposed regulation on AI with the European texts relating to pre-existing data or under discussion** (GDPR, Data Governance Act, Data Act) in order to ensure the complementarity of these texts and to ensure the absence of contradictions or the overlap of similar obligations (access and sharing of data, obligations in terms of data reliability or profiling, sanctions …).
- **It is also important to take into account sectoral texts (health, finance, automobile, etc.) to ensure consistency between European regulations**. For example, there is a need to link the proposed AI regulation with the regulation on medical devices. If a medical device incorporates an AI component, will there be a cumulative application of these two regulations with two separate compliance schemes? Will medical device regulatory compliance be recognized as equivalent to compliance requirements under the AI Regulation?

On prohibited AI practices

Article 5 provides for a prohibition in principle of certain AI practices. MEDEF shares the Commission's ambition to ban certain AI systems that are likely to represent threats to European values as this helps to build confidence in AI.

On high-risk AI systems

On the definition of high-risk AI systems

- **Annex III** defines high-risk AI systems and **Article 6** provides rules for classifying such systems. It is relevant that AI applications are considered high risk when they meet certain criteria such as the severity and the probability of occurrence of certain serious harm to people (threats to health, life or fundamental rights).
- However, the definition of high-risk AI systems is very broad and many applications will certainly fall within the scope of Title III of the regulation, while the use that is made of them is not necessarily high-risk (for

example in the human resources field). This broad definition risks imposing heavy obligations on many players and thus hampering the technological innovation of French and European players, especially the smaller ones.

- Another difficulty lies in the marketing of a general-purpose AI system which would become a high-risk AI system depending on the use made of it (for example in the field of image or text recognition), especially when the user builds an AI. **The complexity of AI value chains should be taken into account and it should be confirmed that high-risk is defined by the user's use of AI**.
- In addition, **Article 7** provides for the possibility for the European Commission to adopt delegated acts to modify Annex III establishing a list of AI systems considered to be high-risk. While it is indeed necessary to take account of developments in the definition of high-risk AI, the fact that the Commission can do so by delegated acts is a source of legal uncertainty. However, this could discourage companies from developing innovative AI solutions due to the unpredictable evolution of the scope of regulation in the coming years.

  Finally, the criteria listed in Article 7, which empowers the Commission to update the list in Annex III, are sometimes unclear and should be clarified in order to support legal certainty and market predictability. For example, explicit provisions should be introduced for the participation of companies in any future process of updating the list (for example, by renewing the mandate of the High Level Expert Group on AI).

On AI component security

The definition of high-risk AI systems expressly includes AI components. However, it is necessary to clearly articulate the responsibilities of each of the operators, in particular when AI components are offered. Indeed, in terms of responsibility and obligations, in particular for risk and compliance assessment, how to deal with AI bricks offered by suppliers, but assembled by the user? Under Article 26, will the importer of these components similarly have to ensure that the conformity assessments have been carried out by the supplier?

In the automotive sector, the concepts of "*safety component*" and "*road traffic*" need to be clarified, their uncertainty being able to present a problem of legal certainty. If these are AI applications integrated directly into a vehicle, there would be an issue of consistency with the homologation regulations (2018/858). Indeed, some automotive AI applications are not covered by the certification (for example, an in-vehicle voice assistant) because they have no impact on safety. The name used in the proposed regulation lacks precision and risks including these applications in the set of high-risk applications when sectoral legislation has considered that this is not necessary. They would thus be imposed a certification process for all of them. **Therefore, it should be specified what type of application is covered by the name used in the proposal for a regulation, specifying:**

- if these are applications already integrated in the vehicle, which are subject to approval under sectoral legislation and should therefore be excluded from the scope of this Regulation;
- or if these are applications not integrated directly into the vehicle, but which, having an impact on the road infrastructure, would be subject to this Regulation by virtue of Annex III.

Annex III would thus gain clarity. For example, a voice assistant directly integrated into the vehicle has no serious impact on safety and is not considered to be at risk by sectoral legislation. However, by influencing the GPS by transmitting destination choice voice commands, the voice assistant risks being considered high risk by the regulation on AI.

On the requirements for high-risk AI systems

- **Article 10** imposes an obligation to use error-free datasets, which is disproportionate and impracticable. Indeed, while it is necessary to strengthen data learning, it is impossible to guarantee the absence of errors in the datasets used in the systems development processes (in the learning of AI especially). The concept of zero data errors is contrary to even the notion of AI which conceptually incorporates this ability to reproduce human analysis. It seems from the interventions of DG Connect that the authorities do not expect data sets that are perfect but as reliable as possible. **It should therefore be confirmed that the obligation relates more to the constitution of data sets as reliable as possible, for example by asking players to demonstrate methodology and justify the creation of databases, in particular for learning**.
- **Articles 9, 19 and 43** require operators to conduct risk and compliance assessments with all applicable legislation. **It should be clarified what will be the relationship between these obligations and the risk assessment provided for in other texts, in particular in Article 35 of the GDPR. To this end, it will in particular be necessary to specify the role of the Data Protection Officer (DPO) in matters of AI. It should**

also be noted that the risk assessment tool proposed by the French DPA (CNIL) is not suitable and, therefore, impossible to use in the context of AI.

- **Article 14** recalls the need for a human to monitor and control AI. MEDEF shares this objective because it is important to maintain human surveillance at two levels: in the design of the algorithm and in parallel with AI (especially when AI is learning) in order to avoid bias. The double decision is important and brings robustness to the AI validation processes. This human monitoring must be carried out both by a data scientist and above all by a person who is expert in a given area of expertise in order to provide a business perspective.

On providers' and users' obligations for high-risk AI systems

It will be necessary to articulate the responsibilities of each of the players, in particular importers (**article 26**) for risk and compliance assessments when products assembled by the user embed AI components developed by third-party suppliers: the supplier of an AI component must be able to give indicators not only on the performance of its component but also without doubt on the validation and even design methods that it has used. The definition of the area of operation should be as documented as possible.

It should also be clarified that, **in certain cases, the supplier and the user may be the same entity and this could lead to a duplication of obligations** (for example: Articles 29 (4) or 61). It would be useful to consider in the text the possibility for a company to play both roles and thus allow proportionate compliance.

On certification and competent authorities

- If companies are rather in favor of the implementation of certification processes in that they improve user confidence in technologies, they are wondering and worried about the articulation of these new certification requirements with the standardization bodies already in place (ISO standards, CE marking, Machinery directive, etc.).

  How to take into account substantial changes? Can certification be considered after the product has been placed on the market?

  Likewise, will AI systems already in operation have to be certified a posteriori?

- In addition, care must be taken to ensure that designated national authorities have identical approaches to assessment criteria and certification to avoid certain players being subject to more stringent requirements in one country than in another.

On transparency obligations

Article 52 provides for transparency obligations, including the obligation for providers to inform people that they interact with an AI system, even when this is obvious.

The wording of this article is sometimes a little unclear and it might be appropriate to define more precisely the criteria of transparency.

Nevertheless, many companies are already engaged in transparency practices for certain AI systems and, in this regard, transparency obligations therefore seem proportionate and reasonable, although it will be necessary to ensure that consistency with other texts, in particular the GDPR and the Digital Services Act (DSA).

In any case, it should be emphasized that transparency is not always possible, due to trade secrets or intellectual property, but also so as not to hamper the functioning and effectiveness of certain processing operations (for example, for the purposes of fighting against fraud and money laundering).

On innovation

Article 53 provides for the establishment of regulatory sandboxes.

For the development of AI, it is absolutely necessary to have datasets to be able to train AI systems. Regulatory sandboxes are therefore a good thing and all companies should be able to use these sandboxes, especially given the constraints set by the text.

While this right to experiment appears to be an interesting tool, **certain clarifications should be made, in particular with regard to the data used in these sandboxes. In connection with the Data Governance Act, will spaces for exchange and sharing of data between players be provided?**

It should also be remembered that sandboxes require a flexible framework to quickly adapt to any kind of innovative initiative.

On gouvernance

Article 59 provides for the designation of a competent national authority on AI to verify and put in place procedures for the assessment, designation and notification of conformity assessment bodies.

At the national level, there are now many bodies and authorities acting in the digital field and, **before appointing a new authority in charge of AI, it would be advisable, on the one hand, to better define the missions of this new authority in the light of the challenges of international competitiveness, innovation and data processing (personal or industrial) and, on the other hand, to clarify the role of each of these authorities already in place and possibly to rethink the scope of these bodies**.

If the CNIL seems to be a privileged authority because of the many processing of personal data within the framework of AI, it cannot be the only authority in charge of these issues which also relate to innovation, research and processing of industrial or non-personal data.

Furthermore, it is essential that the decisions and doctrines of the national supervisory authorities are harmonized in order to avoid the risks of fragmentation in the application of the regulation on AI.

On market surveillance and control of AI systems in the Union market

Article 64 provides for the possibility for market surveillance authorities to require access to the source code of AI systems for the compliance control of high-risk AI. This obligation to provide the source code is disproportionate, in particular for preventive audits, for cybersecurity reasons, in particular in view of the usefulness of this approach. **Rather than access to the source code, provision should be made for traceability or explicability of the operation of the system**.

On sanctions

Article 71 provides for three levels of administrative fines in the event of non-compliance with the provisions of the regulation:

- 30,000,000 € or 6% annual worldwide turnover for non-compliance with Articles 5 (prohibited practices) and 10 (data and data governance);
- 20,000,000 € or 4% annual worldwide turnover for non-compliance with the other obligations provided for by the regulation;
- 10,000,000 € or 2% annual worldwide turnover for the communication of incorrect or incomplete information to the competent authorities.

The penalties provided for are very high, in particular with regard to obligations that are difficult to implement, or even impossible to achieve (free-of-errors data sets, for example, which is nevertheless an obligation whose non-compliance is particularly serious under the terms of the Article 71).

It is also necessary to take into account the fact that these sanctions are cumulative with those provided for by other texts and in particular the GDPR which already provides for € 20,000,000 or 4% of annual worldwide turnover.