POSITION PAPER

Artificial Intelligence Act

On 21 April 2021, the European Commission presented a Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE AND AMENDING CERTAIN UNION LEGISLATIVE ACTS – THE ARTIFICIAL INTELLIGENCE ACT. The proposal builds upon existing communications, publications and the 2020 White paper on AI "A European approach to excellence and trust" accompanied by a report on the safety and liability implications of AI, the Internet of Things (IoT) and robotics.

In addition to the BusinessEurope position paper, this document complements FEDIL's contribution to the Commission's proposal for an Artificial Intelligence Act by highlighting issues of particular importance for its members. It focuses on the need for a balanced approach to foster innovation (I.) as well as for a proper risk-based approach (II.) to be translated in the requirements for high-risk AI (II.A) and in the obligations for actors in its supply chain (II.B).

GENERAL COMMENTS

The European Commission's President, Ursula von der Leyen, and many Member States are increasingly proclaiming the idea of "technological sovereignty" of the EU. FEDIL believes this concept should support the creation of appropriate framework conditions that facilitate the development of the EU's capabilities in strategic areas and encourage the development and use of new emerging technologies such as like Artificial Intelligence (AI). ***The AI market is cross-border and global. Therefore, we fully agree with the Commission that it is positive to address these issues as much as possible at EU level in order to avoid fragmentation of the EU's Digital Single Market.***

The definition of AI for the purpose of a regulation is of utmost importance as there are different types of definitions, which could potentially have different impacts on the development and use of AI. We agree that the definition of AI must be future-proof and allow for accommodating technical progress. Yet, the definition and the list of techniques currently proposed in Annex I of the Artificial Intelligence Act (hereafter "AI Act") could potentially include any computer software and thereby become too broad. This does not provide for the necessary legal certainty.

To succeed in the digital transition, we must firm up our technological capabilities while avoiding heavy regulatory burdens that could harm long-term EU competitiveness. *While we fully support the goal of achieving trust in the application and use of AI, the AI Act must strike the right balance with the constant need for innovation in AI. This balance is essential for our businesses and the EU do be first movers in new emerging technologies. To prevent a negative impact on the sector's dynamism in Luxembourg, we must avoid building barriers to new use cases and underlying technologies' development. It is thus important to avoid any undesirable administrative burden that would hinder the needed investments in the development of AI systems.*

POSITION PAPER

Artificial Intelligence Act

SPECIFIC COMMENTS

I. For more innovation

Our technology capabilities in Europe and in Luxembourg need to be strengthened by confronting our engineering competences with new internet technologies. A strong and innovative technological base is the precondition for businesses to compete globally. Yet, we still observe that actual research is not well translated in European market solutions. To bring research forward this way, ***Europe must allow for bold ideas and encourage the development of testing facilities and regulatory sandboxes.***

We welcome the Commission's proposal on AI regulatory sandboxes. It allows companies to test their innovations while making sure they respect European values before being launched on the EU internal market. However, the resources, infrastructures, and skills this will require must not be neglected. Especially, the competences and skills to build such AI regulatory sandboxes should be encouraged in the EU. We will have to ensure that such facilities become a reality and will be equally accessible to companies across the EU, not only in the most digitally advanced areas.

Moreover, it is essential to preserve the experimental and confidential nature of regulatory sandboxes as intended by the Council's communication 11/2020[1]*.* ***To successfully identify crunch points and support innovation, companies need an area to test their AI systems before undergoing more restrictive compliance processes.*** *This is true for small-scale providers and users – and we support the Commission's focus – but must as well take into account bigger companies' needs for experimenting with AI.*

II. For a risk-based approach

Our members welcome the general risk-based approach and the intention to apply specific rules proportionally to the risks of the AI system. However, we do not believe that the focus on the high risk has been well translated in the Commission's proposal of a "high-risk" category of AI systems. According to the proposal, AI in certain domains and sectors would always be considered as high-risk. This is problematic especially where stand-alone ***practices are defined in a very open-ended way, making the scope too broad and unpredictable, thereby disproportionately overregulating AI for certain uses.***

We do not agree that the use of AI applications in the employment, self-employment or workplace context, as well as for the purposes of remote biometric identification is always posing significant risks to the health and safety or fundamental rights of persons. While we understand the risks related to AI systems taking final decisions in the areas laid down in Annex III, this is not the case where the AI system does not take the actual final decision.

[1] https://data.consilium.europa.eu/doc/document/ST-13026-2020-INIT/en/pdf

In contrary, where AI is used only as a decision support system supporting a human decision, it does not present the high-risk stipulated otherwise but can increase the well-being of individuals and the respect of their fundamental rights.

It is important to consider the probability of causing damage as well as the opportunity of using AI. *Possible losses arising from hindering or considerably slowing down the development or the deployment of a promising AI system stemming from the areas listed in Annex III must be considered. In fact, compliance with the proposed requirements would represent a heavy burden put on SMEs or start-up's that explore the deployment of AI systems, the use of tools with a machine learning component such as OCR language processing or an improved search engine with a risk to slowing down the uptake of AI, especially, in the context of the workplace.*

In addition, it is important to guarantee coherence and consistency as well with the expected security and safety levels through other regulation. For example, in the area of the management and operation of critical infrastructures.

A) For workable requirements on high-risk AI systems

Assuming that the determination of high-risk use of AI is appropriate, relevant and proportionate, we believe that prior market conformity assessment procedures should take place to ensure mandatory requirements are complied with. In this case, we agree with the setting up of a validating, labelling and certification process before an AI system is ready to be applied, used and put on the EU internal market. Nevertheless, a conformity assessment would have to be done in a relatively swift way to avoid significant impact on the placing of the AI system on the market, especially considering how fast the technology is evolving.

As regards the specific requirements high-risk AI systems would have to comply with, the current proposal will not allow for an application to all use cases of AI system and must therefore foresee some amendments:

- ***Data governance****: Enhancing training data is essential. However, instead of laying down the specific data governance techniques,* ***the proposal should focus on compliance with the output of the AI system*** *as it is currently being prepared under ISO Standardisation ("investigation would be necessary to assess whether the impact of [...] bias is positive, neutral or negative, according to the system goals and objectives." A similar approach should be adopted at EU level.*
  More specifically, ***as long as there are humans in the loop, it is impossible to fully guarantee that "training, validation and testing data sets" are always "relevant, representative, free of errors and complete".*** *This goes beyond the very nature of machine learning.*

- ***Record-keeping**: We acknowledge the importance of tracing back a problematic decision making by AI systems and therefore support more transparency through proactive information sharing. Yet, it must be considered that **the storage of the change log (audit log) is technically difficult for providers of AI systems and should be limited in time.** While the proposed article 11 specifies what needs to be put into the log, the conditions are not always workable. According to our members, keeping every piece of information would decrease the quality of more important data while creating important costs and gigantic data bases that could conflict with GDPR rules. Furthermore, it must be noted that datasets are often modified, altered, or even removed after the training of a model. In practice, they will therefore not be relevant or existing when a potential damage occurs. It is therefore very important for our industry to apply this kind of requirement only where the application of AI scores a very high level of risk.*

- ***Human oversight**: According to the proposed article 14, human oversight shall be attributed to individuals with a high level of technical skills. To fulfil this requirement, **companies need data scientists and domain specialists.** First, we would like to highlight again the challenges related to digital skills more generally and the growing skills gap in this area of expertise.*
  *Second, the article as it is currently phrased will be very difficult to implement outside of the use-cases where there is a central system in the company e.g. for critical infrastructure or the management of manufacturing plants. Therefore, we recommend amending the article to better reflect on the users' obligation as laid down in article 29. Indeed, we agree that the only way to effectively apply this requirement is for **the user to implement the human oversight measures indicated by the provider.***

- ***Accuracy, robustness and cybersecurity:** As AI filters into our society, the need for security and explainability grows. The proposal rightly foresees accuracy, robustness and cybersecurity amongst requirements to be fulfilled by high-risk AI systems.*
  *First, we are convinced that **cybersecurity must be dealt with separately** as it does not cover the same issues and needs. Testing must be constantly undergone and upgraded. Regular updates, also on the quality of the data itself, accompanied by an effective enforcement method via regulators or agencies would furthermore support technical robustness of AI.*
  *Second, **the nature of AI, which is constantly evolving and learning after it has been put on the market, as well as the influence of the end-user or operator must be better considered.***
  More generally, the proposed article 15 seems to mix up challenges such as adversarial examples or data poisoning, which are of the area of research and development, with concepts such as resilience that are more in line with the application of AI in critical infrastructures or machinery.

B) For adequate obligations

FEDIL supports the Commission's approach to install a certain ***dialogue between different actors in the high-risk AI system's supply chain****. As regards the specific obligations of the provider under the proposed article 16, we confirm they are needed in the context of a high-risk AI system.*

However, some clarifications on the distinction between responsibilities are necessary to ***consider the ability to comply with the various kinds of requirements*** *when being a user in a deployer role or a provider of a high-risk AI system. While it is common sense that requirements should apply to providers of AI systems before putting their high-risk AI systems on the market,*

- *It is unclear how the user will be able to monitor whether the requirements have been implemented by a provider, especially when the provider is based outside the EU.*
- *It is unclear how the user will be able to determine whether the AI system used is to be considered "high-risk". The CE marking does not automatically indicate that an AI system is high-risk, as it to be put on products according to various other EU legislation. Even if the user is defined as a "professional" it doesn't completely resolve the problem that he might not be capable of fully understanding the AI system.*
- *It is unclear how the provider, who has an AI system developed by someone else, will be able to comply with the requirements without the technical knowledge about AI. There is a risk that these types of providers will not have AI developed anymore, minimising the speed of transformation, thereby hindering the uptake of AI in the EU.*
  This is true also for importers who have no specific qualifications on AI. They might avoid importing AI as the economic interest will shrink due to resources to be spent on applying complex requirements.

As mentioned above, the obligation to keep logs needs to be clarified. In article 20 as proposed, the provider seems to have control over the logs. In this case, many AI systems would not be feasible. Indeed, the control of the log depends on the types of systems e.g. for cloud systems, it will be challenging for the providers to keep the logs and from a software engineering point of view, it will always be the user that defines what is to be put into the log.