ABI Associazione Bancaria Italiana

# Proposal for a Regulation

# Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)

ABI's response

*August 6th, 2021*

## Introductory note

The Italian Banking Association appreciates the opportunity to provide its feedback through the "Have your say" procedure, given the relevance of the topic and the many opportunities offered by Artificial Intelligence (AI) that are emerging on the national and international scene not only in the business sphere, but also in people's daily lives.

ABI believes that it will be relevant to move forward in this area through a common European action that ensures the smooth functioning of the internal market and properly governs the risks, whilst it enables the benefits of AI.

In this sense, to foster the development of AI, ABI points out that an adequate framework of rules can be an important element to mitigate potential negative effects and reduce risks. At the same time, however, an excessively limiting set of rules could slow down the innovation process, reduce the research potential and negatively affect the competitiveness of the European economy.

In other words, it worth questioning whether the introduction of binding rules could really represent the most appropriate instrument to deal with a so fast evolving scenario, or if it might be reasonable to establish an accountable and context-aware approach to the use of AI.

In this regard, ABI thinks it is reasonable to prefer a positive approach aimed at fostering the awareness critical to establishing a contextually responsible approach to AI use. Moreover, ABI is concerned that the proposed Regulation could, at the same time, risk creating unjustified barriers or restrictions on the development of AI based business solutions, reduce research potential, render agile changes to existing applications difficult and ultimately, impact negatively on the competitiveness.
Ensuring legal clarity in the proposal is therefore critical, particularly with respect to the scope, concepts, terms, and oversight.

ABI also believes it would be useful to include transversal mechanisms in the experimentation framework, also regarding a combination of innovative technology not strictly limited to Artificial Intelligence (for example AI and DLT development). Moreover, that could encourage a controlled experimentation framework at the European level, as some states have already done at the national level with national regulatory sandboxes.

The foundation of the ABI position was also built starting from the valuable research activity of ABI Lab, the research and innovation centre promoted by the Italian Banking Association. ABI Lab has established the so-called AI Hub, a context of research and experimentation participated by Italian banks, technological partners and eminent members from the academia. According to ABI Lab research, AI is a core research priority for 83% of the major Italian Banks and there is a wide spread of potential areas of application. Considering

the role of ABI Lab in encouraging the experimentation and the analysis of relevant use cases, we can assert that ABI position also brings out punctual considerations from the real-life experiences.

Following are the main comments on the proposed regulation.

## GENERAL PROVISIONS

With reference to Title I, in which the subject matter of the regulation and the scope of the new rules are defined with the aim of creating harmonized rules for artificial intelligence systems in the EU, ABI noted that a common vocabulary is necessary to facilitate understanding and interpretation of the regulatory framework.

In order to better delineate the perimeter of application of the coming regulatory framework, ABI suggested to promote definitions that are not too broad or generic because this could lead to multiple interpretations or misunderstandings on the perimeter of the same or even include traditional techniques already widely in use and already regulated.

Likewise, the definitional logic used to indicate the role of users of an AI system versus the role of the system vendors themselves appears unclear, especially when a third-party solution is acquired and then customized for use by other users. In addition, the definition of prohibited practices can appear somewhat generic and can lead to multiple interpretations or misunderstandings about the perimeter of those practices.

<u>In detail ABI intends emphasise to the Commission:</u>

- AI Systems definition (Article 3) and the reference to Annex I, related to AI techniques and approaches, appears very wide, including some paradigms (for example statistical approaches, bayesian estimation, search and optimization methods and knowledge bases) on which one could debate if it is always appropriate to mark them as intelligent systems.

- ABI acknowledges that the techniques and approaches mentioned in Annex I are often part of the backbone of AI Systems. However, there are many cases in which the application of those techniques and approaches refers to traditional technologies and does not strictly concerns what is commonly considered Artificial Intelligence.

- To support a clear interpretation of the perimeter of the regulation, ABI suggests enriching the proposed definition specifying the discriminant characteristics that an AI System should show to be really considered as "intelligent". We suggest mentioning the following:

- Adaptivity: the ability of an IT system to improve performance by learning from experience

- Autonomy: the ability of an IT system to perform tasks in complex environments without constant guidance by a human user

The identification of Adaptivity and Autonomy, as the discriminant characteristics that an AI System, derives from the work done by the University of Helsinki and published the online course 'Elements of AI' (https://www.elementsofai.com/eu2019fi). This relevant initiative was endorsed by the EU during the Finnish EU Presidency in December 2019.

- As reported in Recital 6 and Article 3, AI Systems are defined by the ability, for a given set of human-defined objectives, to **generate** outputs such as content, predictions, recommendations, or decisions which influence the environment with which the system interacts. At this regard it is not so clear the meaning of the term "*generate*". To better focus the perimeter of AI Systems, it might be reasonable to refer to data driven systems (systems that – given by human objectives, contexts, data and constraints – create the algorithm or the model autonomously) excluding from the scope any system based on algorithm or model driven systems (systems that basically execute tasks defined and programmed by a human). The reference to data driven systems could be read as the explicit form of the term "*generate*".

- We consider important to mark the difference between decision-making AI Systems (that autonomously execute business decisions) and decision-support AI System (that support a human based decision making). We may state that the introduction of decision-support AI System is less likely to generate significant increase in the overall risk of a business process, also considering that autonomous systems are also subject to Article 22 of GDPR, which already identifies strong requirements.

- Although the EC acknowledges the need to update the list of AI techniques, as set out in Article 4, we believe the definition risks, given the rapid evolution of the context, to be too inflexible and static, raising doubts about the actual perimeter and the future evolution. However, ABI suggests specifying that the update of AI techniques has no retroactive effect on existing AI systems or, alternatively, providing a reasonable period of time to adopt the new provisions.

- As for the list of AI techniques, it would be appropriate to provide for the possibility for the Commission to adopt delegated acts to update the European Union harmonized legislation listed in Annex II.

- In a further twist, the definitional logic used to identify the role of the users compared to the role of the providers of High-Risk AI system seems unclear. Article 28 states that the user shall be considered a provider for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, if it makes a substantial modification to the high-risk AI system. ABI suggests further clarifying which level of modification of the AI solution by the user has the consequence that the user is considered as a provider (e.g., additional training with internal data should not be considered a substantial modification).

- Regarding the "*Provider*", it is defined as an entity that develops an AI system or that has an AI system developed. We believe that the concept of "*has an AI system developed*" should be clarified as it is not clear what it refers to. A more precisely definition would be helpful to avoid misunderstandings and misinterpretations. It might be reasonable to define as provider the subject that has a complete knowledge of the AI system (access to the source code and ability to realise significant change in the design or intended purpose of the AI system) and as user as the party that can parameterize and train the AI system.

- Finally, the definition of "*deep fakes*" ex Art. 52(3) should also be included in Article 3 (Definitions).

## PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES

Concerning the prohibited practices of artificial intelligence listed in Art. 5 of this proposals ABI suggests promoting definitions that are not too broad or generic. This to better delineate the perimeter of application of the forthcoming regulatory framework.

Definitions too vague could lead to multiple interpretations or misunderstandings on the perimeter of the same. ABI considers that the definition of prohibited practices can appear rather generic and can lead to multiple interpretations or misunderstandings on the perimeter of the prohibited practices.

Following those considerations, we would suggest providing concrete exemplification of use cases to be identified as prohibited practices. Clarity and concreteness at this regard are essential condition to avoid excessively constrains the research and experimentation process, which is essential to sustain innovation.

## HIGH-RISK AI SYSTEMS - CLASSIFICATION

About the High-Risk AI Systems Classification ABI notices that the proposal only circumscribes several High-Risk purposes, leaving out a deep analysis of

the possible use cases and capabilities within each AI initiative. A more gradual approach to recognizing the High-Risk type is suggested to be able to capture the different nuances of potential risk.

In detail, we could highlight the following cases:

- In the context of creditworthiness and credit scoring, not all the possible applications of AI Systems introduce the same potential risk for the fundamental rights of individuals. In particular, ABI believes that the application of AI System to determine corporate and small and medium enterprises access to credit should not be considered as High-Risk. This consideration will also bring to exclude from the High-Risk classification any ancillary application of AI System within a credit institution. For example, some of the applications that can reasonably be considered as lower risky for individuals may include:

  - AI application that aims only at speed up credit disbursement process does not introduce High-Risks for individuals, because the AI Systems is not used to automatically decide whether or not a credit request should be refused.
  - AI tools that can be used in the valuation of collateral can also be considered as a lower risk application, given the fact that it is not exactly creditworthiness assessment, rather a background tool in the process.
  - AI tools used in any phases following the initial disbursement of the loan, because there is no impact in the decision of access to credit (AI Systems used only for internal process efficiency).
  - AI instruments focused on other process than credit (such as anti-fraud and anti-money laundering) that can be used as ancillary tools in the overall credit process.

- Another key point concerns the application of AI Systems for employment, workers management and access to self-employment. Even strongly supporting the intention of protecting individual rights, especially when referring to employment and work, ABI believes that it may be not fully appropriate to mark every kind of those applications as "High-Risk", considering that they do not necessarily impact on fundamental rights. Indeed, AI systems are often used as a supporting tool (for example using screening or filtering applications), only to improve the internal processes, and not linked to ultimate decisions on hiring, promotion and termination of work-related contractual relationships.

- In addition, the generic reference to *"monitoring and evaluating performance and behavior of persons in such relationships"* could lead some interpreters to include artificial intelligence systems used by banks as part of their internal control processes, whose purpose is very different from that of deciding on the recruitment or tasks of workers. For this reason, ABI suggests adding point 4 letter b) "*excluding*

*systems used by regulated entities in their internal control framework*" to Annex III.

- The same consideration could also regard AI applications for task allocation. When used merely as a tool for process improvement (or for activity routing to internal workers based on the most appropriate skill set, such as it already happens in contact centers), task allocation should not be considered as High-Risk.

- Moreover, more information about the cases that fall within the scope of the article on Biometric identification could be provided. ABI considers important that authentication (different from identification) is excluded from the High-Risk applications. Regarding identification, ABI also considers it important to indicate whether the identification for customer onboarding falls within the cases list in Annex III, point 1. In addition, ABI believes that the notion of remote biometric identification system defined in recital 8 as an *"AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used"* is unclear. More clarifications and concrete examples to understand the cases excluded from the scope could be useful.

Finally, referring again, but more broadly, to creditworthiness and credit scoring, ABI remarks the need for ensuring a well-coordinated and harmonized supervisory landscape. It could be observed that the banking sector is subject to strong sectoral regulation, which ensures consumer protection, risk management and financial stability in all services provided to customers, including those applications that could include the use of technologies such as AI. Furthermore, the interaction with the review of the Consumer Credit Directive, the Mortgage Credit Directive and the European Banking Authority Guidelines on loan origination needs to be outlined.

## HIGH-RISK AI SYSTEMS – requirements

High-Risk AI Systems are subject to many requirements, some of them appears to be quite strict, including those related to Data set. AI Providers and AI users are required to put in place a demanding governance activity, with a relevant impact on internal processes, IT architectures and organizational settings. Given the impact of those requirements on the organizational settings of providers and users of High-Risk AI systems, it is very important to understand how these general principles will be applied and assessed. Considering the need to ensure a level playing field among different

member states it is paramount that the compliance assessment for High-Risk systems will follow common standards.

Regarding Data set requirements, the "*qualitative*" assessment asked in the Article 10.3 is extremely difficult to be implemented.

ABI considers relevant to specify the meaning of "*relevant, representative, free of errors and complete*". In particular "*free of errors*" seems to be an unrealistic requirement and it is not clear whether it is referred to "data collection and errors recording" or instead to "detection of potential biases".

Furthermore, "*Relevant, representative and complete*" should be intended with respect to the specific use case. Since it is still highly disputed, also at scientific level, how to achieve such a result, practical clue for providers and users on how to avoid bias amplification, how identify which data are relevant, representative and how to control errors could be provided.

ABI suggests clarifying and making explicit that the provisions of Article 10 should be contextualized and proportionately adopted with reference to the state of the art of the technological maturity and to the specific context of adoption, not in absolute terms.

Also, explainability and human oversight are complex and debated matters. A clarification on how explainability should be pursued and about the strategies that should be preferred in defining of human oversight "as appropriate to the circumstances" could be useful.

In any case, ABI recognizes that is fundamental to promote a responsible approach to High-Risk AI systems, but we are worried that an excessively bonding set of obligations may slow down and getting costlier the deployment of innovative services, while speed and efficiency are essential to compete in the digital era.

At this regard, ABI believes that an appropriate, accountable, and proportional approach to the different AI solutions' features should be followed, making a further distinction among the High-Risk applications, with requirements proportional to the risk. A proportional context-based approach linked to possible use cases and capabilities within each AI initiative might be desirable to capture the different nuances of potential risk.

AI systems are subject to many requirements, some of which appear to be quite stringent; in particular, the requirements inherent in information bases for systems defined as High-Risk appear very restrictive. This would necessitate strong governance activities. Even recognizing that it is critical to promote a responsible approach to AI systems, the concern is that overly constraining regulation may slow down innovation within the EU. In this regard, ABI is hopeful that an approach proportional to the different

characteristics of AI solutions and the specific application context can be followed.

## CODES OF CONDUCT

The Commission and the Member States shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems other than High-Risk AI systems.

The Commission and the Board shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems of requirements related for example to environmental sustainability, accessibility for persons with a disability, stakeholders' participation in the design and development of the AI systems and diversity of development teams based on clear objectives and key performance indicators to measure the achievement of those objectives.

While agreeing with the need to have a framework that considers the creation of codes of conduct, ABI believes that the development of code of conduct should maintain a perspective aimed at promoting the awareness around AI systems within the different stakeholders, representing a tool to enhance cultural development and accountability. The requirements for High-Risk AI systems are likely to be disruptive applied to Non-High-Risk AI systems and impose disproportionate obligations.

To support innovation, it is important that codes of conduct shouldn’t introduce barriers or friction to innovation process aligning of non-High-Risk systems with High-Risk ones, in areas where there is almost no threat for fundamental rights. To this extent, they should not be expected to discourage the adoption of the AI system and limit experimentations scope and projects capabilities.

## PENALTIES

Administrative fines are detailed in Article 71 of the Proposal, which provides for different levels of penalties applicable to infringements of this Regulation, such as the GDPR model.

The highest penalty relates to non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5 and cases of non-compliance of the AI system with the requirements laid down in Article 10.

Lower limits are laid down for the non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 5 and 10 and for the supply of incorrect, incomplete or misleading

information to notified bodies and national competent authorities in reply to a request.

As in the Regulation 679/2016/UE, the European Commission continues to provide for the instrument of administrative sanctions, defining a wide range of penalties, limited to the maximum but not the minimum, which combines several violations, depending on the severity.

However, the non-punctual reference to the precise obligations makes it very difficult to focus specifically a particular precept. In other words, in article 71 there are continuous references to entire articles, or even, as in the case of paragraph 4, "*to the requirements or obligations laid down in the regulation*" instead of referring to a specific duty or prohibition set out in the regulation.

Furthermore, it is not clear whether the sanctions will be directly applicable or whether member states will be able to modulate the scope of the administrative sanctions.

Finally, we wish to express our concerns that sanctions are potentially very heavy. We believe it is necessary to reflect the impact of such sanction on the business viability of any business entity or business initiative. The risk is that overwhelming penalties may bring to negative and undesired impacts.

## CONCLUSION

In conclusion, precisely because ABI considers Artificial Intelligence a catalyst for energy and investment, demonstrated by the growing trend of investments in the field of AI, also thanks to the significant investments that the banking sector has made over the years, ABI recommends that these investments should not be compromised by the introduction of new rules that could erode the past with further investments.

At the same time, ABI highlights the importance to act strongly to ensure the same conditions among entities which operate in the area of credit score/ worthiness (level playing field).

According to ABI, the value that AI systems could bring towards a radical transformation of the way we live and consume should be highlighted, spreading awareness that allows people to overcome beliefs dictated by prejudice and polarization, accepting different points of view.

Therefore, a risk-based regulation should also consider the positive impact that AI solutions will be able to generate (e.g., the reduction in operational risk and internal fraud risk that are typically conveyed by AI-enabled smart automation solutions) and not only investigate the negative impacts.

In addition, ABI points out that there is a problem of overlap with existing regulations. For example, the area of credit is over-regulated (Consumer

Credit Directive, CRD, CCD e MCD, EBA on loan origination, etc.), so ABI recommends that where regulations already exist to protect risks for individuals, additional requirements should not be introduced that could further hinder innovation and competition in the Eurozone. It is also important that there are no overlapping or conflicting requirements between the AI regulation and the GDPR.

ABI recommends providing a gradual approach towards the final adoption of the legislation, promoting any voluntary initiatives also in the experimental context and supporting a progressive cultural change.