

Unipol position paper on the EU Artificial Intelligence Act

Bologna, 6 August 2021

Introduction

Unipol welcomes the possibility to share its views on the Artificial Intelligence Act (AIA) and we would like to seize this opportunity providing some targeted comments and proposals.

On a general note, we acknowledge that the ambitious legislative initiative undertaken by the Commission could help building trust around the use of AI systems as it aims to strengthen the protection of EU fundamental rights, which could be undermined by an unregulated use of AI.

In our view, an appropriate and proportionate set of minimum rules governing the development and use of certain AI systems could effectively help in establishing more trust and transparency for the use of AI systems and, thus, foster the innovation.

That being said, we note that the provisions on the scope of high-risk AI systems are overly broad, whereas the provisions on the related requirements are unduly prescriptive and, thus, could severely hinder the use of AI and hamper the EU digital economy.

First studies foresee that *“The AIA will cost the European economy EUR 31 billion over the next five years and reduce AI investments by almost 20%. A European SME that deploys a high-risk AI system will incur compliance costs of*

Unipol Gruppo S.p.A.

Sede Legale: via Stalingrado, 45 - 40128 Bologna (Italia) - unipol@pec.unipol.it - tel. +39 051 5076111 - fax +39 051 5076666
Capitale sociale i.v. Euro 3.365.292.408,03 - Registro delle Imprese di Bologna, C.F. 00284160371 - P. IVA 03740811207 - R.E.A. 160304
Capogruppo del Gruppo Assicurativo Unipol iscritto all'Albo delle società capogruppo al n. 046
www.unipol.it

up EUR 400.000 which could cause profits to decline by 40%" (see Center for Data Innovation – How Much Will the Artificial Intelligence Cost Europe?).

Leaving aside the costs quantification, there is broad consensus among stakeholders that the AIA risks to cause severe damage to the development of EU digital economy. In this respect, it is worth considering that:

- (i) the wide scope of the high-risk AI systems will impact most firms employing even basic software in their value chains, obliging to undertake costly conformity assessment and to implement even costlier risk management frameworks;
- (ii) the exorbitant implementing costs will force many firms (especially SMEs) to avoid the development and use of AI systems deemed at high-risk;
- (iii) the disincentive towards the development of high-risk AI systems will hamper the competitiveness of EU firms putting them at disadvantage against those established out-side EU and could also drive away from Europe skilled workforce and innovators as well as new businesses;
- (iv) EU firms could be forced to import even more technological solution that in the current situation, provided that it would be easier to develop AI systems outside EU;
- (v) ultimately, EU consumers and businesses could have later or no access to innovative AI systems, especially those developed by smaller firms that do not possess as much financial resources and risk management capabilities as bigger firms.

Although we appreciate the ambitious objectives of the AIA, we believe that, at this stage, the proposal is too prescriptive and punitive towards digital innovation and risks to put European firms at a disadvantage in the global competition.

Therefore, at this stage, we advocate for more gradual set up, narrowing the scope of the Regulation and amending the disproportionate requirements. Indeed, it is worth considering that there are already in place comprehensive

legislative frameworks addressing similar issues on the perspective of product safety (General Product Safety Directive), product liability (Product Liability Directive), data protection (GDPR) and consumer protection (Consumer Rights Directive, Unfair Commercial Practices Directive, Anti-Discrimination Directive), not to mention the specific legislations and supervisory frameworks for financial entities (CRD/CRR, Solvency II and IDD).

Definition of Artificial Intelligence

AIA defines “artificial intelligence 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”*.

In our view, AI systems should only be regulated by legislative provisions as long as they pose risks and threats that need to be addressed, as it could be the case with the security of autonomous driving vehicles and of smart grids, where a mistake can lead to catastrophic consequences and, thus, there is need for *ex ante* regulation. Instead, we see that the AIA has adopted an opposite approach, starting from a very broad definition of AI, especially considering *“the techniques and approaches listed in Annex I”*, i.e.:

- (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;*
- (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;*
- (c) Statistical approaches, Bayesian estimation, search and optimization methods.*

The items under (b) and (c) should be dismissed, if they do not have the ability

to self-learn from experience. Otherwise, the definition would include in its scope basically any software, even if it uses simple logic and statistical approach. Even using simple “filters” on certain data pool could be deemed as “AI” and, thus, subject to the Regulation, which would be inappropriate and overly burdening.

In our view, also machine learning approaches should be excluded from the AI’s definition, considering that in most cases they just refer to faster and more efficient versions of the techniques listed under (b) and (c). On the contrary, the only AI systems that could be worth regulating are only those that are able to learn at scale from unstructured data, deal with uncertainty and incompleteness, and interact naturally with humans.

Alternatively, suggestion is, at least, excluding from AIA’s scope the systems generating only predictions and recommendations that are reviewed and assessed by a human being in a later stage. In these cases, which represents the majority, AI only works as a supporting tool with the aim of reducing bias and errors in certain processes that would otherwise involve repetitive tasks of little added value for human beings, as it is the case with the analysis of large data pools. In this context, the use of AI is simply aimed at enhancing the productivity and, thus, should not be at least not discouraged with unnecessary requirements.

Regulating only AI systems that are used for decision-making and that may have material impacts would also be coherent with Article 22 of GDPR, which provides that *“The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her”*.

Thus, suggestion is keeping out of scope the AI systems generating mere predictions and recommendations, considering that those systems are only meant to support decisions taken by humans in a later stage.

Prohibited AI Systems

We agree with the Commission's choice to ban AI systems posing unacceptable threats to fundamental rights and values. In particular, the use of social scoring techniques by public authorities could be contrary to basic premises of the rule of law (as the related sanctions are applicable with no need for an independent enforcement authority) and risks violating fundamental human rights and core EU democratic values.

That being said, we believe that products and services employing subliminal psychological manipulation and/or exploiting the weaknesses of certain vulnerable groups should be banned *per se* and not only in relation to AI Systems. In this respect, we believe that the ban of these practices should be introduced in more general terms in the context of the reviews of the Consumer Rights' Directive and of the Unfair Commercial Practices Directive.

Furthermore, we note that the provisions on prohibited AI Systems are somewhat vague and imprecise, leading to interpretative uncertainties. In particular, clarification is needed with reference to the legal meaning of "subliminal techniques". In this respect, suggestion is focusing more on the outcome (*e.g.*, on the possibility to generate material harm following the manipulation) instead of the technique employed.

Definition of High-Risk AI Systems

We agree with the need to provide certain rules for the development and use of high-risk AI systems. However, the scope of high-risk AI systems set forth by the AIA is overly broad and the related definitions are somewhat vague and imprecise.

As to "*the AI system intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II*" we want to highlight that the AI systems implemented only as a supporting tool to provide additional features without the ability to power the core functions should not be deemed at "high-risk", even more so considering

the broad definition of AI systems, which includes basically any software using basic logic and statistical approaches.

As to the sectors listed in Annex III, whereas we agree in principle that certain areas of application of AI systems may pose higher risks, we note that:

- some of the areas of application set forth in Annex III do not pose high-risk;
- urgent clarification is needed on the scope of certain provisions that are vague and not well defined.

First, in our view it is inappropriate deeming “high-risk” any “AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests”. In this respect, it is worth noting that in most cases AI systems are only implemented to streamline certain internal processes and to support human decisions taken at a later stage. Indeed, the ultimate decisions on hiring, promotions and more in general on the contractual relationships are taken by human beings. In this context, the implementation of AI systems can provide valuable data and evidences to support certain decisions, which could be otherwise biased or more subject to errors.

Also, we do not agree with labelling “screening applications” as “high-risk”. Given that big firms receive thousands of applications for a single vacancy, it is important to filter those that are plainly inconsistent with the advertised job requirements. In this context, AI systems allow HR to spend more time in assessing worthy candidates.

More in general, we do not agree with the fact that even simple software using logic and statistical approaches fall within the definition of AI, also because in certain scenarios the analysis of huge data pool is more subject to biases and errors if performed by a human being.

That being said, we believe that more appropriate criteria for determining the risk level should include the likelihood of a harm to the users and the organisations as well as the severity of the impact and the possibility to

implement remedies.

As to the activities listed in Annex III, we understand that insurance activities are not expressly qualified as “high-risk” and we support that choice. Indeed, the risk management systems implemented by insurance undertakings and the related tools are already subject to thorough scrutiny by the competent authorities. Thus, whereas we appreciated the guidance provided by EIOPA on AI governance principles, we remark that further legislative and regulatory provisions for the insurance sector would be inappropriate and unnecessary, also considering that Solvency II, IDD and GDPR already provide effective requirements to ensure adequate governance, risk management, data quality and the duty to act honestly, fairly and in accordance with the best interest of the customers.

However, even though insurance activities are not mentioned in the AIA, its broad provisions may raise doubts with reference to the “access to and enjoyment of essential private services and public service and benefits”. Indeed, adopting an extensive interpretation, the use of AI systems within certain insurance activities (such as underwriting and claims management) could in theory fall within the “high-risk” category, arguing that some coverages are mandatory to access basic goods such as motor vehicles and housing (in some jurisdictions) and to exercise certain professional activities. In particular, our concern is that some judicial court could rule that *“AI systems intended to be used to evaluate the creditworthiness of a natural persons”* should also apply to the systems used in the underwriting process and in particular for the pricing of insurance policies. As argued above, such outcome would not be appropriate considering that those systems are already subject to extensive controls by supervisory authorities. Such approach would also be coherent with EIOPA’s report on AI governance principles, which expressly states that insurance activities are not deemed at high-risk according to the AIA.

In light of the above, and provided that the assessment of creditworthiness is already subject to extensive regulation and supervision by the competent authorities and that there is no evidence on the need of new specific rules, we

advocate for excluding such cases from the list of “high-risk” AI applications, also in order to avoid legislative overlapping and coordination issues between different authorities.

Another provision of Annex III raising interpretative uncertainties is that related to *“AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid”*. In our view, such provision could be reasonable if referred to public emergency numbers and, more in general, to services of this kind provided by public entities. On the contrary, similar services offered by private entities that do not replace the public ones should be kept out of scope. This is the case, for example, of certain black-boxes capable of calling without any human input the single emergency numbers when their sensors recognize a serious crash of the vehicle where they are mounted. In those cases, it is clear that the service offered by the black-box is an additional service that does not preclude in any way the injured person or other bystanders to call the publicly available emergency number to receive support. Indeed, given the positive social externalities of this kind of services, we think that any regulation discouraging their development and marketing should be avoided.

Thus, suggestion is amending the provisions as follows: *“AI systems intended to be used by public authorities or on behalf of public authorities to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid”*

Requirements for High-Risk AI Systems

We agree that High-Risk AI Systems should be subject to specific requirements and that, in this context, a risk management framework and human oversight represent the most effective instrument to mitigate the risks stemming from such AI system.

However, we see that the AIA adopts a *“paper compliance”* approach, heavily reliant on requirements, procedures and disclosure instead of providing new rights for the individuals and groups and the adequate means to exercise them.

In particular, we would have at least expected the right to challenge an automated decisions materially and negatively affecting the users, which is not expressly provided by the AIA. The suggested approach, focusing on the outcome instead on the technical means to achieve on a certain objective, would have been better suited for a level-1 framework and less punitive towards business and innovation.

In this respect, we also note that many requirements are either unrealistic or unfeasible as they are provided in absolute terms demanding a technical perfection. As argued above, such prescriptive provisions could damage the global competitiveness of EU firms, hamper the development of EU digital economy and will most burden on SMEs, which cannot rely on conspicuous financial resources to bear the cost of the massive compliance requirements introduced by the AIA and do not possess the required risk management capabilities.

In particular, suggestion is amending the following provisions:

(i) **Data quality** (Art. 10.3) – Requiring “*training, validation and testing datasets*” to be “*free of errors and complete*” is technically unfeasible as it demands perfection; whereas we agree on the importance of data quality, the provision should be amended according to a risk-based approach. It also worth considering that a thorough validation of datasets may be impossible for providers using datasets elaborated by third parties, whose sources could be protected by license or other contractual agreements. In those cases, providers should be allowed to rely on the independent assessment produced by account of the providers without being required to re-assess the whole data-sets from scratches, which could be legally and practically impossible in certain circumstances. In our view, such assessment could follow the ordinary outsourcing rules provided for financial entities;

(ii) **Transparency** (Art. 13) – We agree that transparency towards end-users is a necessary mean for increasing the trust around the use of AI, especially where AI systems interact with human beings. We also

welcome the fact that transparency obligations “*shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence*” (Art. 52), which is the case of AML due diligence. However, we would like to point out that the detailed information that AIA requires to disclose seems inappropriate as it is not balanced against confidentiality of trade secrets. Indeed, providing all the information listed under Art. 13.3 and especially related to “*the characteristics, capabilities and limitations of performance of the high-risk AI system*” may reveal confidential information and thus further discourage investments and research for the development of new AI systems. Also, the amount of information to be provided to end users is disproportionate as it leads to a disorienting information overload. Thus, we think that it would be best relying on a reasonable level of “explainability” instead on a list of detailed information of little value for the end user. Alternatively, we suggest at least deleting the detailed information pointed out in the sub-paragraphs of Art.13(3)(b).

(iii) **Human oversight** (Art. 14) – We agree with the provision according to which the human oversight operator shall “*fully understand the capacities and limitations of the high-risk AI system*”. Indeed, effective human oversight and explainability are key to avoid unpredictable outcomes. However, we suggest replacing “fully understand” with “have a comprehensive understanding”. In the suggested terms, the provision would be more proportionate as it would not rely on absolute concepts like “full understanding”, which could prove challenging especially for the most sophisticated AI systems. Also, it is worth remarking that full understanding of the high-risk AI system should not cover the explainability of the machine reasoning behind each single intermediate step of the assessment performed by the AI systems, which is not always possible, especially for sophisticated AI systems such as non-symbolic AI.

(iv) **Quality management systems** (Art. 17) – The provisions on the data quality management systems are overly prescriptive because their

implementation demands huge implementing costs (especially with reference to the conformity assessment procedures) that could discourage EU firms and especially SMEs from developing AI systems deemed at high-risk. The ability to comply with the numerous provisions on the quality management systems is further hindered in the situations where, according to Art. 28.1, any distributor, importer, user or other third-party qualifies as a “provider” because either: *“(a) they place on the market or put into service a high-risk AI system under their name or trademark; (b) they modify the intended purpose of a high-risk AI system already placed on the market or put into service; (c) they make a substantial modification to the high-risk AI system”*. Indeed, setting up full and sound quality management systems over AI applications developed by third-parties becomes prohibitive especially for SMEs lacking compliance/risk management skills and financial resources and, thus, are not able for effectively verify whether the AI system is fully compliant with the numerous requirements provided by the AIA. Therefore, we recommend amending the provision according to a more proportionate and risk-based approach.

(v) **Automatically generated logs** (Art. 20) – The provision on the conservation of automatically generated logs is vague in its scope as it may suggest that *every* log that is automatically generated by high-risk AI systems shall be kept by the providers. In these terms, the provision is overly broad, also considering that most of this data may be of little relevance and that its conservation comes at a cost in terms of storage and energy consumption, notwithstanding the fact that not every data can be stored, also for legal reasons related to privacy. Furthermore, the coordination clauses with GDPR rights to data deletion/minimisation are not convincing. Therefore, suggestion is restricting the scope of the provision only to important logs, i.e., the logs explaining the rationale behind certain decisions or recommendation that may have material impact on the end user or the firm.

Overlapping legislations

We welcome the coordination mechanisms provided for financial entities by recital 80, according to which: *“To further enhance the consistency between this Regulation and the rules applicable to credit institutions regulated under Directive 2013/36/EU of the European Parliament and of the Council, it is also appropriate to integrate the conformity assessment procedure and some of the providers’ procedural obligations in relation to risk management, post marketing monitoring and documentation into the existing obligations and procedures under Directive 2013/36/EU. In order to avoid overlaps, limited derogations should also be envisaged in relation to the quality management system of providers and the monitoring obligation placed on users of high-risk AI systems to the extent that these apply to credit institutions regulated by Directive 2013/36/EU”*.

However, we would like to point out that further regulating the use of AI for financial entities is unnecessary and inappropriate considering that any material uses of AI systems within the core processes of banks (and insurance undertakings, which are not mentioned in the recital) is already subject to extensive requirements and thorough assessment by the competent authorities and that there is no evidence on the need of further specific rules. In particular, reference is to the use of AI in the banks’ rating models and in the insurance companies’ risk management framework and underwriting processes. As it is also pointed out by a recent paper published by the BIS, *“existing banking and insurance international regulatory standards can be applied in the context of addressing reliability/soundness of AI models”* and *“existing laws, standards or regulatory guidance sufficiently cover data privacy, third-party dependency and operational resilience, and may be applied in the context of AI”* (see BIS – *Humans keeping AI in check – emerging regulatory expectations in the financial sector*).

Furthermore, the provisions on the Member States’ duty to design a national competent authority for the enforcement of AIA would create institutional obstacles for the activity of the financial supervisory authorities, which are already well established and expert in assessing operational and ICT risks of

financial entities.

Thus, in order to avoid duplicating requirements and imposing further unnecessary compliance costs, we would advocate to not include the assessment of the creditworthiness within the high-risk AI application.

Should the co-legislator decide not to follow such recommendation – notwithstanding the above reasoning – we deem that clarification is at least needed on:

- (i) the practical interactions between CRD and AIA, especially with reference to the Supervisory Review and Evaluation Process (SREP), also considering that the implementation of rating systems for assessing the creditworthiness is already subject to extensive and thorough scrutiny and requirements under CRR (173-179 and 186) and, thus, any further requirement on this matter would be ultroneous and inappropriate;
- (ii) the precise extent of the “limited derogations” foreseen by recital 80.

Regulatory Sandboxes

We welcome the fact that AIA provides for the establishment of regulatory sandboxes by Member States. Indeed, in the financial sectors the Member States have moved at different paces and with heterogeneous rules, leading to significant regulatory arbitrages (many companies moved to other jurisdictions offering more lenient conditions for the experimentations).

That being said, to avoid more regulatory arbitrages and to make regulatory sandboxes more effective in fostering innovation, we would have expected at least the requirement on Member States to ensure transparency not only about the eligibility criteria but also about the metrics used to assess the application to join the experimentation, not to mention the requirement to ensure transparent and fair access for the firms interested in take part in the sandbox.

Also, in accordance with the international best practices, it would be advisable

that the authorities responsible for the regulatory sandboxes would publish on an annual basis the results and achievements of the experimentation as well as any relevant finding that could help business outside the sandbox building effective and compliant AI systems.

Transition period

We note that, according to Articles 7.1 and 73.5, the delegated acts amending the lists of high-risk AI systems listed in Annex III would enter into force “within a period of three months of notification of that act to the European Parliament and the Council”. In our view, it would be more appropriate to grant at least 12 months to the firms for complying with potential amendments to Annex III adding new AI systems to the list of high-risk applications.

Concluding remarks

We commend the Commission for its human-centric approach to regulation and for the ambition to lead on standards setting at international level, with the aim of fostering the trust on the use of AI and of promoting the development of AI and EU digital economy.

However, even though the adopted approach is agreeable (*i.e.*: banning the use of AI incompatible with fundamental rights; setting requirements on the high-risk AI systems and providing simple transparency requirements for AI systems interacting with humans), we see the urgent need of amending:

- a) The AIA’s scope, which is too broad as it qualifies as “high-risks” applications that do not in fact pose such risk;
- b) The requirements on “high-risk AI system” by adopting a truly proportionate and risk-based approach, whereas the proposed provisions demand technical perfection and huge implementing costs.

On a general note, we think that more consideration should be given to the rights of individuals and groups - providing the means to effectively exercise

them - and to the EU global competitiveness and strategic autonomy. In this respect, it is worth remarking that Europe is a net importer of technology, struggling to keep pace with other geographical areas in the run for innovation.

Whereas we agree that providing some rules on high-risk AI application can help fostering the trust and use of AI, the proposed Regulation goes too far, risking to seriously hinder the development of EU digital economy.

Instead, we believe that the AIA should be reviewed according to a more pragmatic and innovation-friendly approach, and that to foster the development of AI it is first and foremost necessary to improve the availability of early-stage private capital and the public investments in the development of strategic technologies.

* * *

UNIPOL GRUPPO S.p.A.

Luca Giordano

Head of Regulatory Affairs

A handwritten signature in blue ink, appearing to read "Luca Giordano".