Position Paper

1 February 2022

ECOMMERCE EUROPE

Position Paper on the Artificial Intelligence Act

Introduction

On 21 April 2021, the European Commission published a proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) together with a Coordinated Plan for the Member States. Artificial Intelligence (AI) is increasingly being integrated in the retail landscape. From customising offers in real time, innovating the way consumers can digitally try on fashion items, to optimising inventory management, AI can help e-commerce companies better meet changing consumer demands.

Ecommerce Europe welcomes the European Commission's initiative to establish harmonised rules on Artificial Intelligence. It is important to stress that online retailers are mainly users of AI systems in their everyday business models to tailor their services to customers' needs and improve internal efficiency. At the same time, e-commerce businesses increasingly start to develop their own artificial intelligence solutions. In both cases, e-commerce companies look at the opportunities AI systems offer benefiting consumers, businesses, and society as well as promoting sustainability and innovation. Generally, AI solutions mainly used or developed by retailers carry no or very low risks to individuals. Ecommerce Europe appreciates that the European Commission has also recognised the retail sector as a safe sector in its AI White Paper.

In this paper, Ecommerce Europe addresses its main concerns with regards to the Draft AI Act. While we generally support the Commission's ambition to establish an EU-level legislative framework on AI, we would like to share some comments and recommendations to ensure the final text is workable, future-proof and allows for sufficient space for innovation.

Key Recommendations

1. **Review the current definition of AI so that it is adapted to regulatory purposes.**
2. **Review the categories and definitions of "high risk AI systems" to ensure legal precision and focus on AI-specific risk.**
3. **Review the requirements for high-risk AI so that they consider AI-specific characteristics, technical feasibility, and existing legislation and international standards.**
4. **Review prohibited AI use cases to ensure they are specific and do not lead to broad interpretation.**

1. Definition of AI

As the main objective of the AI Act is to regulate AI systems, their definition is essential to provide companies with the necessary legal certainty. Ecommerce Europe believes that the proposed definition goes beyond what is commonly considered to be AI. While Annex I (a) covers traditionally defined AI systems, namely AI techniques and approaches (e.g., machine learning), Annex I (b) and (c) also include other applications such as *logic-based systems, statistical approaches, Bayesian estimation and search and optimisation.* Such software applications should not be included in the scope. The currently drafted definition of AI system creates a risk of unintentionally regulating many traditional technologies, not just AI, and may result in significant barriers to growth and innovation. Subjecting such technology to the Act's requirements, including the high-risk requirements, could also create substantial barriers to access and use of technology in the EU. Additionally, this could lead to overlap with other sector-specific and horizontal legislation and thus add complexity to the legislative framework and compliance process. To ensure legal certainty at this stage, but also towards any future development of other software applications, Ecommerce Europe calls on policymakers to narrow down the definition of AI.

Additionally, the definition of AI systems should be modified to clarify that (i) general-purpose "building block" or "development" AI tools which serve as components or precursors of AI systems are not covered; and (ii) only software that genuinely uses AI technology fits in the definition. This is because AI tools (as distinct from AI systems) often have no broader purpose beyond serving as building blocks for various user-designed applications, which in turn serve more specific user-generated intended purpose. Consistent with Recital 60, we do not think it is the Commission's intention to cover software, tools and models which are not in and of themselves AI systems.

The proposal allows the Commission, on the basis of Article 4 in conjunction with Article 73, to amend definitions, including the AI definition, by delegated act. In addition, the list of high-risk AI uses of annex III can also be amended by delegated act every two years. While we recognise the importance of flexibility in the rapidly changing digital environment, we would like to stress the importance of following a transparent regulatory process with the involvement of relevant stakeholders and representatives of the industry. That is why we believe that such update should be done on a yearly basis in consultation with stakeholders, rather than the Commission relying solely on Delegated Acts in accordance with Article 73. Stakeholders can provide EU Institutions with the expertise and industrial experience necessary to build a balanced and future-proof framework for Trustworthy AI to the benefit of consumers and businesses alike.

2. Risk-based approach

Ecommerce Europe welcomes the risk-based approach that the Commission has adopted in its proposal for the AI Act. In the proposal, the Commission distinguishes between four different categories: (1) prohibited practices, (2) high-risk AI systems, (3) systems requiring increased transparency measures due to a risk of deception, and (4) all other systems. While we support the idea behind this risk-based, multi-layered approach, we believe further improvements can be made to the current categorisation.

High-risk AI

With regards to high-risk AI systems, we believe that Article 6 dedicated to classification rules for high-risk AI systems and annex III are a good first step but require further legal clarification. To ensure that the boundaries between the different categories are clear and easy to implement, we recommend basing the classification of "high-risk" AI on concrete use cases and examples of the techniques that fall under the scope. As drafted, the AI Act suggests that any AI system used in connection with certain high-risk products or industries (e.g., AI systems used in recruitment), regardless of how that AI system is specifically used and whether that use creates a material risk of harm, is a high-risk system. This results in many AI systems inadvertently being classified as high risk and subject to the onerous high-risk requirements in a way that is likely to hinder innovation and limit use of technology in the EU.

Currently, some proposed high-risk AI systems seem to insufficiently capture the context in which they are used. We propose that in order to be considered high risk, an AI system must also make final decisions that create a material adverse risk to a person's fundamental rights, health or safety. This clarification is important because AI may play a low-risk role in a high-risk category. For example, while it is understandable that AI systems used to evaluate credit score or creditworthiness of people are considered high-risk, machine-learning can also be used by retailers to offer a better consumer experience in the payment process and to prevent fraudulent orders or account take-overs. For e-commerce companies, we do not consider there to be a risk for the customer to lose access to "essential" private services or suffer any other significant harm if they are not offered their preferred payment method. To create legal certainty about whether such systems used by retailers would fall in the high-risk category, it would be important to define what an "essential private service" (Annex III.5) is.

Additionally, the use of AI systems in employment does not automatically qualify an application as high risk. We recommend amending Annex III, section 4 to differentiate between applications according to the risk they pose to one's individual rights. Our concern is that the classification of all HR applications as high-risk does not recognise the need to differentiate between applications in the area of HR according to actual risk, and that such a broad categorisation will stifle innovation in the near future and pose as a barrier to transforming HR processes to the benefit of workers and employers alike.

To ensure a link between the AI system as such and the context in which it used, we would suggest reintroducing the cumulative criteria put forward by the Commission in its AI White Paper. This would mean that an AI system is classified as high risk when both the sector and the specific intended use involve significant high risk allowing for a more nuanced and realistic risk-based approach. This will provide more legal clarity on what really constitutes high-risk and avoid diverging implementation.

Biometric Identification

Annex II includes as a high-risk AI system those intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons. We believe that EU rules for remote biometric identification systems should balance concerns such as on discrimination or privacy with opportunities to improve consumer experiences in a transparent way. It is therefore important that only passive mass identification is covered and not the active identification of individuals. In e-commerce, biometric identification can be very safely used for authentication purposes. Important innovations have been developed in the last years by use of fingerprints, facial patterns, or voice in areas such as payments and fraud prevention. It is therefore also important that the distinction between "biometric remote identification" and "biometric categorisation system" (Art. 52.2) is unambiguous.

Prohibited AI

The AI Act includes a list of prohibited AI whose use is considered unacceptable as contravening Union values, for instance by violating fundamental rights. The prohibitions cover practices that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness or exploit vulnerabilities of specific vulnerable groups such as children or persons with disabilities in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm. Naturally, Ecommerce Europe supports the introduction of this category of prohibited practices to avoid the use of AI systems that are incompatible with fundamental rights. However, considering the importance of correct application of these rules, we deem it crucial that no uncertainty exists on which AI uses fall within this category. As a ban on using technology in certain contexts is a quite far-reaching remedy, when prohibiting AI use cases, policymakers must be very targeted to capture the specific uses of AI technology that they view as contrary to EU principles and not inadvertently include other use cases. Ecommerce Europe is concerned that subsections (1)(a) and (1)(b) of the current draft could be misread to apply to some forms of personalised advertising or personalisation. Such broad application would not serve the goal to introduce proportionate and effective rules that are tailored to the intensity and scope of the risks. Policymakers should clarify that the legally not defined term "beyond a person's consciousness" only include hidden.

Article 5.1 a prohibits AI systems that deploy subliminal techniques *"beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or likely to cause physical or* *psychological harm."* The legally non-specified term of subliminal techniques needs to be clarified in a way that this should not be understood as a prohibition on the use and development of marketing, personalisation, and search recommendations AI systems, which are commonly used techniques in e-commerce. These systems do not cause material, physical or psychological harm, and should therefore not fall within the scope. Additionally, the example provided by the European Commission on their website, namely that of "*toys with a voice assistant that encourage minors to engage in dangerous behaviour*", does not provide additional certainty. Instead, a question rises on what constitutes "dangerous behaviour", as this does not necessarily have to lead to "physical or psychological harm". Another example that could benefit from further clarification is the use of chatbots. Chatbots are generally classified as minimal risk, meaning they would only be subject to the transparency requirements under Article 52. However, they could also be considered a prohibited use of AI if they potentially cause "physical or psychological harm", which they normally do not. Generally, we foresee potential enforcement issues with regards to the legal assessment on the basis of terms such as "consciousness", "subliminal" and "psychological harm". We would therefore recommend including materiality qualifiers to help clarify the scope of these prohibitions to ensure sufficient legal certainty and avoid a fragmented interpretation, in particular considering the high fines proposed by the Commission and the diverging national legal frameworks with regards to tort law.

3. Allocation of responsibilities

E-commerce businesses are mainly users of third-party AI systems. However, they are also increasingly developing their own artificial intelligence solutions. The ability to comply with the various obligations of the AI Act is strongly dependent on a business' role in the supply chain. It is therefore crucial that these responsibilities are clearly allocated. The proposal includes obligations for providers to put a quality management system in place, and for importers and distributors to ensure that the systems are compliant. Any distributor, importer, user or other third-party that places an own-branded system on the market, significantly modifies the intended purpose of the system or makes a substantial modification takes over the responsibilities of the provider. It should be clarified what the concepts of 'substantial modification' (Articles 3, 12, 28, 43) and 'significant change' (Article 8) entail. Furthermore, the term "user" can be further specified taking into account the respective context (e.g., B2B/B2C). With regards to joint responsibilities between different actors in the supply chain, we ask policymakers to carefully consider past experiences with for instance the joint controllership under the GDPR.

Ecommerce Europe would also like ask for a clarification on the possible vertical market application of Article 2.1 in the case of third-party or vendor relationships. The article states that the Regulation applies to (a) providers placing into service AI systems in the European Union, irrespective of whether those providers are established within the Union or in a third country; (b) users of AI systems within the European Union; (c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the European Union. Moreover, the compromise of the Slovenian Presidency of the Council also includes in the scope *d) importers and distributors of AI systems; (e) product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark; (f) authorized representatives of providers, which are established in the Union.* The Regulation, however, does not specify the case when a vendor or third-party platform is using an AI system on behalf of a "client", for example, if a vendor uses an AI system to provide a service (e.g., background/resume review). To ensure legal certainty, we ask the Commission to clarify if in such instances the AI Act applies only to the vendor, or if the client that commissions the service would also be in the scope.

4. Feasibility of obligations

While we recognise the ambition of the Commission to create a legislative framework that is innovation-friendly and intended to intervene only where this is strictly needed, we believe some of the proposed requirements are highly prescriptive and difficult, or sometimes even impossible, for economic operators to comply with. For the legislative framework to deliver on its projected objectives, we stress that feasibility should always be a key consideration, in the interest of businesses, enforcers and consumers.

For instance, we foresee difficulties with the legal obligation that “training, validation and testing data sets shall be relevant, representative, free of errors and complete”. While businesses aim to minimise the risk of errors when gathering and training data, ensuring that training data is “complete”, “representative” and “free of any errors” is an unrealistic standard. In our view, this should be rephrased as ensuring “best efforts” or abiding by “industry standards” to leave enough flexibility to businesses to determine how best to achieve those outcomes. For instance, Article 10 (3) could instead have the following rewording: “Training, validation and testing data sets shall be relevant, representative, and appropriately vetted for errors and completeness in accordance with industry standards”. Similarly, as Article 15(3) remarks that high risk AI systems “shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates”, we suggest that this should be reworded as “high risk AI systems shall make reasonable attempts to be resilient as regards errors, faults or inconsistencies [...]”. Furthermore, the notion that AI systems must be developed in a way that ensures their operation is sufficiently transparent to *“enable users to interpret the system’s output and use it appropriately”* can be interpreted in various ways.

Finally, the proposal lays down rules for the placing on the market, putting into service and the use of AI systems within the EU. The training of AI data sets is covered in Article 2 and requires the use of AI output from third countries to adhere to EU rules when operating in Europe. Ecommerce Europe urges policymakers to consider how it can be best ensured that datasets trained outside the EU, but used inside the EU, are fully compliant with EU rules.

Considering the technical nature of many obligations, Ecommerce Europe would advise policymakers to consult industry experts on the feasibility of the proposed obligations. In addition, any future amendments would also benefit from a careful review of industry experts as well as during any kind of future planned amendments of the list of high-risk systems.

Overall, Ecommerce Europe recommends in the revision of high-risk requirements that:

1) Requirements should be high level, with details being driven by industry-specific regulators (e.g., medical device regulatory bodies should be responsible for establishing AI medical device requirements), or by broader standards bodies.
2) Requirements should seek to avoid regulating input or development of systems, which will significantly hamper companies’ abilities to innovate, and instead focus on output, such as managing how the output is used to make decisions.
3) Requirements should be objective driven and specifically address the risk of the use-case.

5. Enforcement

Ecommerce Europe would like to stress the importance of effective enforcement to ensure a level playing field across the EU. As the e-commerce sector is highly cross-border by nature, it is particularly important to reduce regulatory fragmentation. The Commission’s proposal in its current form, seems to strongly rely on the competencies of national authorities. From experience with existing legislation, Ecommerce Europe is cautious about a lack of coordination between national authorities. As the proposal does not include a one-stop-shop mechanism, but instead requires national legislators to design the proposed regulatory mechanisms at a domestic level, we fear businesses will face a fragmented enforcement landscape across the EU. In addition to the envisaged coordination by a European Artificial Intelligence Body, we strongly recommend legislators to support national regulators with detailed implementation guidance, and to identify existing legislative overlap between the EU AI Act, international and harmonised standards, and other ongoing legislative initiatives at EU level.

Regarding the entry into force and application of the AI Act, we believe a timeline greater than 24 months will be required to hire and train the necessary workforce in the relevant notified bodies, and to ensure harmonised standards are available. We therefore recommend modifying Article’s 85(2) writing and change the 24-month reference to 36 months instead.