AmCham EU

SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Artificial Intelligence Act

Priorities for trilogues

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3.7 trillion in 2022, directly supports more than 4.9 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

Executive summary

As informal interinstitutional (trilogue) negotiations between the co-legislators are taking place with a view to reach a first reading agreement on the Artificial Intelligence Act (AI Act) proposal, we encourage EU decision-makers to:

- support the Parliament's definition of AI;
- ensure a tight high-risk designation of the use cases included in Annex III and refrain from adding new sections to Annex III;
- refrain from adding new categories to prohibited uses in article 5, notably the broad banning of biometric identification and emotion inference;
- tighten the high-risk designation in article 6 along the lines suggested by Parliament;
- ensure that the language for high-risk AI systems ensures flexible and adaptive requirements,
- ensure a balanced approach to the AI value chain, ensuring clear responsibilities for providers and deployers;
- further clarify definitions and concepts on general purpose AI/foundation models/generative AI;
- refrain from adding duplicative and unnecessary new obligations on deployers of AI systems (ie FRIA and employee consultations)
- ensure that requirements on providers of general purpose AI and foundation models are targeted, realistic and flexible;
- distinguish between artificially generated content for public dissemination and for use in closed groups;
- avoid overlap between the AI Act and other pieces of legislation;
- ensure harmonised and predictable enforcement; and
- ensure a flexible and clear approach to standardisation.

Introduction

The Commission appropriately aims to create an ecosystem of trust and excellence and to ensure that the EU becomes a vibrant hub for research, development and innovation in trustworthy artificial intelligence applications through the proposed AI Act. In the current context characterised by ongoing technological developments and divergent institutional views, AmCham EU would like to give concrete recommendations to the co-legislators as they progress interinstitutional negotiations in the coming months to achieve a first reading agreement on the AI Act proposal. These proposals are intended to contribute to realising the objectives of the AI Act: to create safeguards for trustworthy AI systems, and foster development and use of AI in the EU.

Definition

A targeted and focused definition of AI that is in line with internationally accepted ones would set the stage for multilateral coordination and harmonisation of AI policy. Both Council and Parliament have addressed this issue, and they have taken steps to align the AI Act definition of AI with that adopted by the Organisation for Economic Co-operation and Development (OECD).

While the Council's amendments to the proposed definition of AI systems were a step in the right direction, it still retained overly broad elements, such as the reference to logic and knowledge-based approaches, which could risk capturing predominantly traditional software rather that provide the much-needed delineation between such software and AI systems. The Parliament's definition of an AI system more closely aligns with international best practice such as OECD and National Institute of Standards and Technology (NIST) frameworks, an approach more suitable to development of international standards. Moreover, the Parliament and Council deleted the list of AI techniques and approaches in Annex I, as these are overly broad and would risk capturing a broad array of software programs already on the market for many years (eg productivity applications).

We recommend further aligning the definition of AI with the OECD definition and encourage more refinement. We support deletion of Annex I as proposed by both Council and Parliament and support the clarifications provided by the added recitals 6a and 6b.

High-risk designation

The risk-based approach is a fundamental building block of proportionate and effective AI regulation. AI systems are and will be used in a wide variety of scenarios and, thus, regulation must be designed to reflect this diversity in risk profiles. The European Commission's original text would be too broad and vague in its description of use cases in Annex III. It is therefore appropriate that the Parliament and Council have adopted amendments that aim to narrow the scope of the high-risk designation.

The Parliament has proposed amendments to art. 6.2 so that AI systems encompassed by the categories set out in Annex III should be considered high risk 'if they pose a significant risk of harm to the health, safety or fundamental rights of natural persons'. This concept, properly defined, could add clarification to the Council's proposal to limit the high-risk designation to AI systems whose output is 'not purely accessory' to the action or decision in question.

The Parliament also appropriately suggested that AI providers should notify supervisory authorities if they plan to launch AI systems that are covered in Annex III but which the provider does not consider high-risk. Authorities would have three months to respond – if they find that the AI system does present significant risks. It is yet to be defined how this process would work in practice and whether supervisory authorities would be able to deal with notifications in a timely and thorough manner. Both the Parliament and Council texts call for additional guidance on the delineation of high-risk categories. Additional guidance is needed in the form of legislative or non-legislative instruments (eg Communication, Implementing Acts) which should be outlined by widely consulting with industry and other stakeholders. With reference to art. 6.1, an AI system should be considered as high-risk only when it is used as an 'essential' or the 'only' safety component in a system.

Annex III has been subject to a number of amendments, both by the Council and the Parliament. In line with our overall position, we support amendments that attempt to make the language clearer and more targeted, such as in Section 4 (employment/workers management). Nevertheless, this section should be further clarified to exclude non-personal monitoring/evaluation of performance. Another helpful clarification is the EP's proposal to exempt AI for fraud detection in credit evaluation. Additionally, we discourage expanding Annex III further, as well as including use cases that are covered by other laws. In this case, for example, other amendments establish new categories, and also include some AI use scenarios that are already covered in existing legislation, such as the Digital Services Act.

Requirements for high-risk AI

The requirements set out in Chapter III are consistent with the High-Level Expert Group on sustainable finance (HLEG) recommendations and reflect to a large extent the practices already being undertaken by responsible AI providers. However, these requirements should be flexible enough to reflect the wide variety of AI systems that must meet them, be designed to manage the risks they are meant to be mitigated and be realistic as well as outcome-oriented.

The detailed technical standards that will form the basis of providers' compliance with the AI Act have not yet been developed. Thus, articles 9-16 should not be made too detailed and prescriptive. The absence of standards will also be a challenge in implementing the AI Pact proposed recently by Commissioner Breton.

The EP and the Council have proposed amendments that would appropriately specify the risks that the requirements should deal with: those involving health, safety and fundamental rights. However, in art. 9, the EP text includes broad fundamental concepts (eg 'rule of law, democracy, and the environment') that could lead to confusion among AI providers and developers seeking to design compliant risk management systems. The EP text in art. 12 also requires AI providers to include monitoring and calculation of energy consumption and impact on the environment. The AI Act is not the right instrument for these purposes. By regulating the energy consumption of computer servers through commission regulation (EU) 617/2013[1], this issue is already dealt with.

Overall, we support amendments to include wording such as 'technically feasible', 'reasonable', 'to the best extent possible'. This language helps setting out requirements that reflect the fact that technical standards to implement the requirements do not yet exist, and that best practices are constantly evolving.

Foundation models/Generative AI and General Purpose AI (GPAI)

The concepts of general purpose AI, generative AI and foundation models were not included in the initial proposal for the AI Act, in line with the risk-based approach. The Council's text created provisions on general purpose AI, and the European Parliament introduced provisions on foundation models, including generative AI. While regulating AI tools that have no specified or intended purpose is inconsistent with the risk-based approach, it is clear that the final text will need to develop an approach to these concepts. In this context, we outline below some recommendations.

Firstly, there is a need for clarity of definitions and concepts to ensure that the regulatory requirements and enforcement are focused on the right models. For example, companies use general purpose tools and application programming interfaces (APIs) to design, train and deploy AI systems in a variety of industries. These tools, as well as APIs, are not AI systems *per se*, but users develop them into AI systems by defining their intended use.

[1] Commission Regulation (EU) No 617/2013 of 26 June 2013 Implementing Directive 2009/125/EC of the European Parliament and of the Council with regard to ecodesign requirements for computers and computer servers

Consistent with the AI Act risk-based approach and emphasis on intended purpose, a provider's duties should be assigned to the party that determines an AI system's intended purpose. In this way, the AI Act should give flexibility to allocate responsibilities contractually in the value chain. Including obligations for General Purpose AI (GPAI), foundation models and generative systems would compel AI providers to comply with the AI Act regardless of whether the AI in question poses a high risk or not. This is fundamentally at odds with the risk-based approach the AI Act is based on. As mentioned above, the AI Act should mitigate actual, tangible risks to health, safety and fundamental rights. It should not include concepts such as speculative, systemic risks to democracy and the rule of law. This would lead to impossible compliance obligations, raise cost and complexity for AI developers, and hamper innovation in these models.

We generally welcome Parliament's more focused approach through its introduction of the concept of foundation models, compared to Council's broad and less precise approach to general-purpose AI systems. (An improvement could be exemption of GPAI where the provider has specified in the instruction of use that the GPAI is not to be used in high-risk scenarios). Nonetheless, this definition of foundation model would benefit from further calibration. This would help to better address highly capable foundation models at the frontier of existing capabilities (eg GPT-4), which are intended to be adapted and integrated into a wide range of different downstream applications, and not deployed directly to end-users.

Requirements placed on foundation model providers should take into account relevant existing legislation as well as the technological realities of the AI value chain. They should be practicable and only extend to what foundation model providers can reasonably address during design and development, rather than all potential risks that downstream applications may present. From this perspective, several of the proposed requirements introduced by the Parliament in article 28b are either not feasible in practice or overly burdensome on model providers, as set out further below:

- **Risks are often context and use-case specific.** While developers should make significant efforts to mitigate known and identified risks during design and development stage, they will not be able to reasonably foresee many of the specific use-cases and related risks, which can only be done by the deployer. Therefore, in article 28b(2)(a) 'reasonably foreseeable risks' should be replaced with 'identified risks'. Moreover, 'non-mitigable risks' should be replaced by 'known risks'.

- **No guidance on democracy and rule of law risks.** Delegating to the private sector the obligation to establish what constitutes risks to the rule of law and democracy is not appropriate in the absence of clear guidelines on how foundation model providers could reasonably comply with this requirement. Therefore, this requirement should either be deleted or accompanied by guidelines demonstrating what would constitute (reasonably foreseeable) risks to democracy and the rule of law that it is possible to address at the model layer, and how these could be identified, reduced and mitigated.

- **Mandatory involvement of third parties in the development phase.** A strict requirement to involve independent experts in the development phase of all foundation models would be unfeasible due to the lack of expertise on the market. Moreover, given that this requirement is not even applicable to high-risk AI systems, it is not clear why foundation models would face this requirement, or how this requirement would address specific challenges related to foundation models. Therefore, the requirement to involve independent experts should be removed.

- **Calibrate environmental impact requirements to ensure feasibility.** The environmental requirements – in particular where they relate to the impact that deployment and use of the systems have over their entire lifecycle – are not feasible in practice in light of the complexities of the AI value chain.

New obligations on deployers/users

The European Parliament's text imposes new and potentially significant obligations on deployers of AI systems. In particular, they would need to complete a new fundamental rights impact assessment prior to launch. This impact assessment would be necessary even though the AI system in question already meets all the requirements set out in the AI Act. No other New Legislative Framework (NLF) legislation includes such a provision. Such a requirement seems duplicative and unnecessary given existing requirements for Data Protection Impact Assessments in the General Data Protection Regulation (GDPR). It would create additional compliance costs and complexity to be shouldered by companies across all sectors, big or small, who will face a disincentive to adopt these new technologies. In addition, the Parliament text proposes that deployers should consult with employees representatives before deploying a high-risk AI system in the workplace. Again, such an approach is in conflict with the NLF model of legislation and creates barriers to deployment of these technologies. Hence, these ideas should not be reflected in the final text of the AI Act, for the reasons set out above.

Transparency obligations for artificially generated content

There is benefit in requiring AI generated image and audiovisual content to be labeled in important scenarios so that the public 'knows the content' it is receiving. Thoughtful measures to deter the misuse of new technology to deceive or defraud the public will benefit the health of democracy and future of civic discourse. However, the transparency requirement in article 52(3) would benefit from distinguishing between generative AI services disseminated to the general public and those provided in a (closed) enterprise environment or in the context of (business or private use of) productivity software. Moreover, the addition of text-based content as added by the Parliament does not appear to be appropriate in the context of the requirement.

Overlaps with existing, dedicated regulation

The Parliament intention to label AI systems intended to be used by Very Large Online Platforms as high-risk AI systems under Annex III overlaps with the provisions laid down in the DSA, which have only entered into application last month. Moreover, this provision significantly deviates from the AI Act's risk-based approach, as it is unclear which specific risks it concerns and how it relates to the type and size of the entity deploying such systems.

The Parliament's added requirements in art 12, art 41(1c) and Annex IV relating to energy consumption and environmental impact of high-risk AI systems, do not take into account the significant number of existing and upcoming legislation in this area, such as ecodesign regulations, IT efficiency indicators in the context of the Energy Efficiency Directive, the Corporate Sustainability Reporting Directive and the EU Taxonomy Regulation. Moreover, the level of detail does not take into account the technical feasibility of logging capabilities along the AI value chain, nor does a system's designation as being high-risk have any bearing on its energy consumption, compared to low-risk systems.

Harmonised enforcement

The Parliament's approach to enforcement, whereby Member States would designate a single national supervisory authority (article 59) should be prioritised over the Council and the Commission's proposals whereby each Member State could designate multiple national competent authorities. The Parliament's proposal to partially centralise some enforcement authorities under an AI Office within the Commission (article 66a) is also beneficial, as it would take on especially serious cases of AI risk in addition to providing support services through a secretariat.

The Parliament proposes that in cases where multiple national supervisory authorities are involved, the lead NSA will be where the infringement took place (article 59a[2]). It remains unclear how the lead NSA would be determined in the case of simultaneous cross-border alleged infringements. Thus, a supervisory authority of a company's main establishment should be the only competent authority for decision-making, including imposing fines. A one-stop-shop mechanism is particularly crucial for companies with separate legal entities and different business lines operating in several Member States, as they need legal certainty as to the one 'lead' regulator being their single point of contact. The one-stop-shop also provides clarity to consumers as to the competent regulator and by ensuring a consistent and more efficient application of the AI Act across Europe.

Clarity and flexibility around standards

The Council requests the Commission to issue common specifications for high-risk systems requirements and general-purpose AI systems. This request is also supported by Parliament's position, which proposes an additional layer of consultation with the AI Office and AI Advisory Forum before the issuance of common specifications. However, the Commission should only develop common specifications in narrow, exceptional circumstances where conventional standards are clearly not be appropriate. The international standard-making process should remain the principal process as it is effective at gathering a broad range of input, helping ensure standards are effective and durable. This process should be utilised rather than promoting the development of bespoke specifications from the Commission through a less inclusive and consultative process.

Conclusion

The Artificial Intelligence Act can create a prosperous market for reliable and ethical AI systems. Nevertheless, for artificial intelligence to continue flourishing, it should be monitored and regulated appropriately. As the policymaking process accelerates, we call on EU policymakers to create safeguards for trustworthy AI systems and foster the safe development and use of AI across the EU.