Brussels, 10 October 2022

AIOTI views on the Artificial Intelligence Act

AIOTI welcomes the proposed regulatory framework on Artificial Intelligence (AI) by the European Commission as well as the efforts made by the European Parliament Committees to strengthen the regulation.

Our members appreciate the European institutions commitment towards a human-centred, sustainable, safe, ethical and trustworthy artificial intelligence.

With regards to the objectives set by the AI Act, we would like to express our views on the following aspects of the regulation:

General purpose of AI & definitions

General purpose tools are not AI systems per se but are developed into AI systems by their users. Importantly, General purpose tools do not have an intended purpose, and their provider is generally not aware of the exact future intended use of these tools, the AI model which will be used or the data which will be used to train the model. Think of an AI-based speech recognition service which allows to transform speech into written text. Depending on the application area in which the speech recognition service is used, its risk assessment will be completely different.

1. If the service is used in the field of radiology (healthcare) to process radiology reports dictated by the radiologist to generate inputs for medical diagnosis, human health could be at risk.

2. If the service is used by a private person to control e.g. Alexa or Bixby, the person might be frustrated but not experience serious harm.

In both cases, the potential harms can only be analysed in the context of the concrete AI application (and intended purpose) with concrete AI model(s).

We do not see the need for the AI Act to have a specific section on General Purpose AI (GPAI). The original text of the Commission should stand, in order to maintain the risk-based approach. AI systems which can be used in high-risk scenarios are already covered in the Act. GPAI having no defined purpose, it would contradict the risk-based approach to have them explicitly covered or explicitly excluded and would make the assumption that they're all used for high risk applications.

According to the Commission's own analysis, if users need information from GPAI providers to ensure compliance, these providers have a commercial interest in helping these users/clients with all requested information to become compliant. This idea that the market will take care of the cooperation is indicated in Recital 60.

As proposed by MEP Tudorache in the draft IMCO-LIBE report, we suggest to fine tune the allocation of responsibilities and clarify that the entity which decides over the intended purpose of an AI system or gives an intended purpose to a system becomes the provider. The provider then use of the training data and development information received from the provider of the GPAI in the following risk assessment process. Importantly, this allocation should be modifiable through contracts.

Definition of AI System

AIOTI believes that the current definition of "AI system" is too wide (Article 3(1)). The AI-techniques listed under Annex I that classify a software as AI include "statistical approaches, Bayesian estimation, search and optimization methods," (Annex I, part b and c) all of which are widespread and largely accepted techniques in numerous industrial domains, including but not limited to logistics and manufacturing. Although these methods can be deployed in automated decision-making processes for critical applications, there is a fundamental issue of measurability and thresholds to identify at what point the use of such techniques can effectively qualify as AI.

The AI-techniques deployed by manufacturers are almost exclusively limited to Narrow or Weak Artificial Intelligence ("Narrow AI"), a form of AI that implements specific tasks requiring only a limited form of intelligence, subject to a narrow set of constraints and limitations that are assigned from the outset by humans – Typically designers, computer specialists and plant engineers, among others. In fact, narrow AI has been safely and effectively deployed in the manufacturing sector for many years to improve the reliability of components, implement predictive monitoring and maintenance, increase the lifespan of machinery, optimise energy efficiency, and adapt production to customer demand.

For this reason, AIOTI proposes a revision of this definition to ensure that 1) it includes a necessary element of "autonomy" and "intelligence behaviour" in decision-making, and 2) that it does not include widely used statistics and optimization methods, while on the other hand 3) the definition should be future-proof and allow for the inclusion of technological approaches that cover more powerful forms of AI in the future. In particular, we recommend using the definition proposed by the High-Level Expert Group on AI, focusing on AI-techniques that display intelligent behaviour and take actions with some degree of autonomy (Annex I, part a). The definition of AI systems should also include a reference to "human defined intended purpose" rather than "human defined objectives", in order to ensure consistency with the rest of the AI Act.

High Risk Products

In AIOTI's view, obligations for providers and users of high-risk AI could result in being costly and excessive, with the consequence that innovation, development and investment are all chilled, or certain market actors fail to fully comply, both of which would be detrimental to the stated aims of the legislative intervention, in particular the requirement to keep technical documentation for over 10 years, including pictures, the definition of residual risks in terms of risk management, and the record keeping of logs.

According to Article 6, an AI system can be classified as high-risk on the basis that it is *1) "used as a safety component of a product, or is itself a product covered by the Union legislation listed in Annex II"* and that *2) "the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment pursuant to the Union legislation listed in Annex II,"* thereby extending the classification beyond safety components and safety-relevant software products. Although this risk-based approach may seem purposeful and pragmatic, it creates significant ambiguities in the interplay between the AI Act and the legal acts listed under Annex II, which already provide for comprehensive safety requirements covering most industrial applications of AI. The current classification rules in Article 6 would force EU manufacturers to abide by overlapping classification and obligations from both the AI Act and their respective sectoral legislation.

According to AIOTI, the proposed classification rules for High-risk AI should be redefined to ensure consistency with sectoral legislation in Annex II, thus regulating only high-risk AI applications in areas where a clear regulatory gap has been demonstrated, without extending beyond safety components and safety-relevant software products. Furthermore, the provisions of Article 6 should not hold the third-party conformity assessment as a criterion for all high-risk classified systems, given that this would undermine the development of innovative and beneficial AI-techniques that grant EU manufacturers a competitive edge, particularly in our sector where highly customized solutions are often commercialized. We invite to not include all household appliances to be considered as high risk but only those which use personal data.

We are also aware that both the Parliament and Council are considering to extend Annex III of the regulation (high risk AI systems) to include management of the Internet and/or control of digital infrastructure. We would ask co-legislators to urgently reconsider their approach, as it is evident that necessary threshold to be considered as High-Risk is not met in all cases. This is largely on account of the fact that the AI systems deployed within communications networks do not interact with or give rise to decisions that affect individual EU citizens, but instead relate exclusively to the routing of traffic across the network, something which is already subject to a sectoral regulatory regime under the European Electronic Communications Code[1]. As such, direct impact on the fundamental rights that are addressed under the AI Act (for example: the right to privacy, the fundamental right to life and physical integrity, the prohibition of discrimination) are minimal.

Electronic communications service providers continue to bear significant regulatory obligations to guarantee the security and resilience of their networks (both sectoral and horizontal) in the form of the Code, the NIS Directive, GDPR, Cyber Resilience Act and ePrivacy Regulation. Given this existing regulatory framework and bearing in mind the legal basis for the AI Act we do not think it appropriate that the AI Act should duplicate existing legal obligations pertaining to security and privacy of the network itself, but instead focus on upholding and promoting the fundamental rights of natural persons.

We therefore underline the fact that mere control of digital infrastructure should not be considered a High-Risk activity and should therefore not be included within Annex III of this regulation.

Harmonised Standards vs. Common Specifications

Under Article 41 of the draft AI Act, the Commission would be given the possibility to develop common specifications via implementing acts in cases where harmonised standards do not exist or where the Commission considers that the relevant harmonised standards are insufficient or that there is a need to address specific safety or fundamental rights' concerns.

This provision risks undermining the inclusiveness and technical quality of standard-setting processes and disincentivising the participation of companies, particularly manufacturing SMEs, and thereby weakening the legal and technical status of standards. Standard-setting processes are and must remain inclusive and market-driven processes drawing on the expertise of a wide range of stakeholders including users, market surveillance authorities, notified bodies, Conformity Assessment Bodies, academia, and industry.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1547633333762&uri=CELEX%3A32018L1972

From AIOTI's perspective, the implementation of common specifications should be seen as a time-limited "fall-back" option in the absence of harmonized standards rather than a replacement, whose use should only be permitted under the strict, finite and clear conditions outlined below:

- No reference to harmonised standards published in the Official Journal of the European Union (OJEU) according to Regulation (EU) No 1025/2012
- Submitted request by the Commission to one or more Standardisation Bodies to draft a harmonised standard subject to undue delays or to rejection
- Repeal of common specifications when references of a harmonised standard are published in the Official Journal of the European Union (OJEU).

On these grounds, AIOTI strongly recommends that harmonised standards should be formulated with the active participation of industry, particularly SMEs, to ensure market relevance, technical quality and to avoid a "one-size-fits-all" approach. Ultimately, the powers of the European Commission to introduce common specifications via implementing acts should be on the basis of strict and unambiguous conditionality.

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT Innovation in Europe, bringing together small and large companies, start-ups and scale-ups, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share and promote best practices in the IoT ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT Innovation in society.

AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies. We also put them in practice in vertical application domains with societal and economic relevance.