GIGAEurope calls for greater clarity on definition of high-risk AI

October 2022

As private operators active in investing, building and operating Gigabit infrastructure and 5G networks across Europe, GIGAEurope's members welcome the European Commission's 2021 Proposal for a Regulation laying down harmonised rules on artificial intelligence ("the proposed AI Act"). GIGAEurope commends this initiative to establish a proportionate risk-based legal framework, according to which EU citizens can have confidence in the AI they are using, whilst simultaneously harnessing its true socioeconomic potential.

At the outset, the Commission emphasised the need for a clear definition of "high-risk AI", and that this was intended to cover only a limited number of AI systems. The Commission recognised the acute need for legal certainty and sought to avoid abstract risk definitions by proposing (under Annex III, point 2(a)) an exhaustive list of scenarios where AI applications relating to critical infrastructure may be deemed "high risk". This was complemented by future-proof mechanisms (contained in Articles 6 and 7 of the proposed AI Act) for evaluating potential risks of emergent AI applications in a dynamic context. GIGAEurope believes that the Commission's proposal strikes an appropriate balance between the twin objectives of promoting the uptake of AI and of addressing the risks associated with certain uses of such technology.

The Gigabit connections that our members deploy provide the capacity and functionality needed to support a wealth of advanced analytics and AI applications for European businesses and consumers, in support of the green and digital transition. The use of AI and machine learning in the connectivity sector is predominantly related to such beneficial use cases as network optimisation and maintenance, innovation towards software-defined network functions and optimisation of customer service (e.g. machine-learning chatbots). AI plays a pivotal role in the evolution of current Gigabit networks towards software-defined networking, whereby next generation networks are made more programmable, in turn rendering them more flexible, scalable, and reliable. This facilitates agile service deployment and reduces the carbon footprint by supporting intelligent energy savings in operational networks and data centres, and allowing for greater innovation and investment to the benefit of Europe's end users.

Mindful of the balance between optimising the potential of AI, while protecting EU citizens against legitimate risks to health, safety and fundamental rights, GIGAEurope has been closely following the evolving classification of high-risk AI systems in Annex III of the proposed AI Act. Given the onerous administrative requirements that flow from this classification, it is imperative that there is clarity on the types of AI applications falling within its scope. Overly-broad definitions may inadvertently create a disproportionate burden for valuable AI solutions and for the connectivity providers supporting such applications.

In this regard, GIGAEurope notes the fourth compromise text recently circulated by the Czech Council Presidency in point 2(a) of Annex III of the proposed AI Act, which refers to "*AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic and the supply of water, gas, heating and electricity*". GIGAEurope recalls that the Commission's original proposal, which was supported by a full impact assessment, did not include a reference to digital infrastructure in Annex III, reserving this list only for AI systems where there is a justified cause for concern or where such concern can be reasonably anticipated in the near future. GIGAEurope agrees with the Commission that emerging uses and applications of AI are more appropriately screened via the dynamic procedures in Articles 6 and 7 of the proposed AI Act, enabling it to evolve organically and proportionately as new technologies materialise. However, GIGAEurope believes that, compared to earlier versions of the Council's texts, the wording in the latest Czech Council Presidency text moves in the direction of offering a greater degree of clarity to network operators that deploy AI for the purposes of network security, and is closer to reflecting the limited scope of this Annex as intended by the Commission. We believe that Council's position is broadly in line with Parliament's amendment 287 to Annex III (1.2a) that also focuses on the safety and security components of critical infrastructure, including the "*internet*". However, GIGAEurope recommends the Council's wording in this regard, as, instead of the "*internet*" (which is not legally defined), it refers to "*digital infrastructure*", which is an existing, legally-defined term under EU legislation.

As the Act aims to balance risk prevention and legal certainty with a pro-innovation environment for AI deployment, it is important that any classification of high-risk AI remains proportionate by being evidence-based and reflecting uses of AI that constitute actual potential risks at the present time. Proportionality also implies avoiding overlapping legal requirements. In this respect, GIGAEurope recalls that providers of electronic communications networks and services are already subject to an extensive set of regulatory instruments and obligations. For example, the European Electronic Communications Code ("EECC") already includes robust requirements for consumer protection and security in electronic communications. Article 40 of the EECC contains detailed security requirements for electronic communication providers and Article 41 empowers the competent authority with respect to the implementation and enforcement of these requirements.

Against this background, and whilst acknowledging the more finely-balanced language in the latest Czech Council Presidency text, GIGAEurope underlines its view that, as a general principle, premature classification of AI systems as "high-risk" should be avoided by following the evaluation procedures described in Articles 6 and 7 of the proposed AI Act. GIGAEurope therefore cautions against including AI systems in Annex III beyond the Commission's initial proposal and suggests deferring instead to the due diligence mechanisms in Articles 6 and 7. However, to the extent that any high-risk definitions pertaining to electronic communications are included upfront in Annex III, it is important that these are: a) clearly specified, including by way of a precise classification of use cases (that are not covered by existing legal obligations); and b) aligned with existing legal definitions under relevant EU law. Clear and precise definitions, that are properly understood by all actors within the complex AI ecosystem in Europe, are indispensable to avoid inadvertently chilling the development of valuable AI initiatives in support of Europe's twin green and digital transition.

To conclude, GIGAEurope calls for restraint regarding possible extension of the rules beyond the Commission's original proposal on high-risk AI. However, in recognition of the evolution of the proposal through the legislative procedure, GIGAEurope supports the wording in the latest Czech Council Presidency text, while recommending adding a clearer and more precise classification of use cases that fall within the identified risk area for critical digital infrastructure in Annex III.