DOT Europe position paper

Harmonised Rules on Artificial Intelligence: Questions and Recommendations on the AI Act

Introduction

With the Artificial Intelligence Act, the European Commission has proposed the first legal framework for Artificial Intelligence (AI) in Europe. The proposal aims to allow Europe to profit from the wide range of economic and societal benefits of AI while addressing potential associated risks. DOT Europe – the voice of leading digital, online and tech companies in Europe – welcomes this approach. The AI Act has the potential to provide the legal certainty necessary to encourage innovation in the Digital Single Market and serve as model legislation for the rest of the world.

One of the key challenges that the AI Act faces is to find a balance between protecting consumers and their fundamental rights and enabling innovation in Europe. The AI Act aims to ensure that consumers are not subjected to AI systems that pose a great risk of undermining their rights and freedoms, especially in sensible contexts such as health and justice, while enabling innovation and ensuring European consumers experience the benefits that new technologies can bring.

To this end, below we put forward some initial questions, examples, and recommendations on the AI Act and the related discussions. We believe these questions will need to be considered by policymakers when reviewing and refining the proposed text, in order to deliver a balanced and proportionate framework.

Conformity assessment of high-risk AI systems

There is a consensus that, before being placed on the market, high-risk AI systems must undergo a conformity assessment procedure to demonstrate that they are in conformity with the requirements laid down in the legislation. It will be important to agree what constitutes 'high-risk' AI and ensure that Annex III is clearly and narrowly defined, based on a risked-based approach. In addition, there is an ongoing disagreement about who should be in charge of conducting the assessment. While some argue that the assessment should be conducted by an objective third party, there are strong arguments to suggest that the assessment is best placed with the provider to frequently justify this position, given the in-depth knowledge and understanding that they have of their own work.

DOT Europe Questions:

- The goal of the AI Act is to enable innovation while providing safeguards where significant risks to users could exist and specific safeguards are needed. How can it be ensured that the list of high risk AI in Annex III is developed on a **risk-based approach** and not overly broad as to include activities which are not AI or for which there is no objective assessment that risks to consumers are high?
- While in the grand scheme of things, high-risk AI systems constitute a small share of AI systems, nonetheless if these providers were required to seek a third party assessment it would mean a significant increase in demand. As a result of this, it is likely that prices for

third-party assessments would steeply increase and the associated cost would serve as a disincentive for innovation in Europe. **How can it be ensured that the costs linked to third-party assessment requirements do not hamper innovation in Europe?**

- Whereas increased costs can serve as a disincentive to innovation for bigger players, they can be even more detrimental to smaller players such as SMEs and start-ups who may not be able to meet the financial requirements associated to a third party assessment. **How are SMEs and start-ups expected to be able to afford third-party conformity assessments?**

DOT Europe Recommendations:

- Ex-ante conformity assessments for high-risk AI applications play an important role in ensuring that the legislation is adhered to. Given their knowledge of the technical details and their expertise in the field and relative context that an AI may be used in, the assessment should be conducted by the provider of the AI.

Transparency of AI systems

At present, algorithmic transparency is dealt with across a number of different legislative acts, including the GDPR, P2B Regulation, UCPD, PID and most recently the DSA. However, there remain calls for more thoroughgoing algorithmic transparency for AI systems, either vis-à-vis general users or market surveillance authorities (auditing). With a balanced approach, the AI Act can enhance the existing transparency framework by providing clarity for consumers and market surveillance authorities without going so far as to open the door to actors who would abuse this information.

DOT Europe Questions:

- One of the key concerns when it comes to the transparency of AI systems is proportionality. When it comes to access to sensitive data such as training and validation datasets or the code of an algorithm, appropriate safeguards must be put in place to ensure that the information is handled with a due level of confidentiality. **What measures must be put in place to ensure that transparency obligations remain proportionate?**

- Many AI systems used by online platforms contain sections which are aimed to limit the spread of dangerous content such as child sexual abuse material or terrorist content. Providing access to training datasets used for this purpose or the code of the algorithm itself would provide deep insights into the workings of these protective measures which could be used by bad faith actors to circumvent these mechanisms. **How can transparency obligations provide meaningful insights while protecting information the potential misuse of which could negatively affect or even endanger users?**

- Datasets and in particular the codes of algorithms contain very complex information and require a high level of knowledge in fields like computer science and statistics in order to be understood. As such, the information relating to AI systems is not intelligible to the vast majority of its users, who would not gain any understanding of it by reading it. **How can users be provided with insights into the algorithms they interact with that are intelligible and complete at the same time?**

DOT Europe Recommendations:

- When information is made available to users of an AI, the focus should be on providing the relevant information in a way that is accessible and intelligible to laypeople. This could be achieved through algorithmic explainability where users are provided with a description of what an AI is doing, decisions that were made during the development and information on how specific parameters are weighted in order to educate them about the AI they interact with.
- For information that is requested by market surveillance authorities, providers and deployers of AI should work hand in hand with authorities and assist them in their assessment by providing relevant information as well as the necessary facilities to carry out robust testing, consistent with appropriate safeguards.
- A separate DOT Europe position paper on algorithmic transparency and explainability is publicly available on our website.

Nonmaterial aspects – democracy, environment, rule of law

AI systems interact with the environment in complex and multivariate ways. Some concerns have been raised as to the impact on nonmaterial public goods such as democracy and the environment, with ensuing calls for providers to assess that impact ex-ante. These concerns are understandable, but seldom go into detail regarding how a developer can make such assessments, as this is inevitably linked to how the system is deployed, on what scale, and how to assess the impact.

At the outset, AI systems must be understood as tools which can be used for informing decisions, some of which may adversely impact e.g. the environment. Where to allocate responsibility for such decisions (i.e. with the entity taking the decision or the AI system which is used to inform it) is an important question.

DOT Europe Questions:

- **How can policymakers protect important public goods without unduly burdening providers whose AI tools can serve a number of purposes, even those against the public interest?**
- **How to create a proportionate burden of regulation given the impossibility of knowing the range of applications that AI systems can be used for?**

DOT Europe Recommendations:

- DOT Europe recommends addressing these issues through sectoral legislation (e.g. climate/energy policy, specific initiatives on rule of law)

Expansion of scope – linkage with other digital legislation

The EU’s digital agenda is a multipronged strategy covering issues dealing with competition, content moderation, cybersecurity, data protection, pluralism and more. We believe that these issues are best dealt with in specific horizontal legislation which also applies to systems using AI technology. In this context, including them in the AI Act could lead to duplication of responsibilities.

For example,it has been suggested that digital advertising should be added to Annex III and subject to the additional conformity assessment, but the processing of data for digital advertising is already subject to stringent GDPR rules, including user content which can be withdrawn at any time.

Similarly, platforms designated as VLOPs under the DSA which use AI technology fall within the scope of both the AI Act and the DSA. Under the DSA, these platforms are required to provide for transparency regarding recommender systems. If platforms are designated as high-risk AI, VLOPs will have to follow two parallel procedures tending towards the same objective including transparency reports, technical documentation and putting in place risk management systems all of which tending towards the same objective.

DOT Europe Questions:

- **How to avoid duplication of regulation where AI systems are already regulated in content, data protection or privacy legislation?**

DOT Europe Recommendations:

- DOT Europe recommends maintaining the focus on AI technology and avoiding duplication by way of overlaps with DSA or other forms of content moderation, in particular by defining social media and other platforms as high-risk.
- DOT Europe recommends against including advertising under Annex III as stringent regulation already applies in this area under GDPR.

Protection of vulnerable groups

AI systems can have an impact on the decision-making of users that interact with them. The degree to which users are affected varies widely and is linked to circumstances and context of the use. As part of the discussions surrounding the AI Act, some have called for specific measures aimed at limiting the impact that AI may have on specific groups of users that may be in a vulnerable position, such as children.

DOT Europe Questions:

- Vulnerability is a broad and vague concept which could lead to legal uncertainty and drastically widen the scope of the proposal if no clear and specific definition is provided. **How can vulnerability be defined in a way that achieves enhanced protection for specific groups without creating legislative uncertainty and confusion?**
- In most use-cases for AI systems, the AI system may not have access to the information that would be required to make a reasonable assessment towards the level of vulnerability of a user. This would either make it impossible for a provider to comply with the requirements in the AI Act or it would force the system to collect much more data about its recipients in order to better be able to make an assessment. **How is the provider of an AI system supposed to know that the system is interacting with a vulnerable user?**

DOT Europe Recommendations:

- DOT Europe acknowledges that children are particularly susceptible to AI. In order to address the concerns that AI systems may have a negative impact on children, AI systems that are intended to be used by children and which are intended to have a significant impact on their personal development could adhere to more stringent requirements.

General-purpose artificial intelligence

General-purpose AI systems are a crucial part of the online ecosystem. They are developed for a range of purposes rather than for a specific use-case and constitute the basis for different applications. An example is traffic routing model used by municipalities to dispatch first responders.

In the discussions surrounding the scope of the AI Act there is disagreement on the appropriate level of regulation that general-purpose AI developers should comply with given their place in the value chain.

DOT Europe Questions:

- General-purpose AI systems are purpose-neutral as they are designed to be deployed in a variety of settings. As a result these models do not have a clearly determined risk profile. One of the key elements of the AI Act is the focus on the application of an AI system to determine its risk level. **How could an inclusion of general purpose AI in the scope of the AI Act be reconciled with the legislation's focus on the risk of application?**
- Oftentimes general-purpose AI systems are modified by a third party in order to fit their specific use case without informing the original provider of the AI system of the changes and the context of use. **Given the possibility that any general-purpose AI may be used in a high-risk context, would these systems automatically be assumed to be high-risk?**

DOT Europe Recommendations:

- The AI Act should clarify that when other actors in the value chain modify a general-purpose system in a way that makes it high-risk, they should assume the responsibilities of a provider as they are best equipped to identify the risks associated with their specific use case. Furthermore, given the purpose-neutral nature of general-purpose AI systems, they should be clearly excluded from the scope of the proposal so as not to undermine AI Act's approach of being application oriented.