



DOT Europe position paper

DOT Europe Position on the Artificial Intelligence 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 presents a real **opportunity to create a clear and future-proof framework** which provides the legal certainty necessary to encourage innovation in the Digital Single Market and which can become model legislation for the rest of the world. In particular, considering the widespread use of AI applications, rules need to be considered in a global context. Therefore, the EU institutions should drive an effort in cooperation with bodies such as the G7, G20 and the OECD, to agree on global regulatory principles and standards for the deployment of AI.

While the Commission’s proposal presents a good starting point for discussions, there are some issues that policy-makers need to address to guarantee the success of the legislation.

Scope

One of the biggest priorities in creating an effective and workable AI Act is to appropriately establish the scope of the legislation. Article 3(1) defines “AI system” as any software developed using specified techniques that “generate[s] outputs [...] influencing the environments they interact with”. The vagueness of this definition could lead to an overly broad interpretation as **virtually all software generates some form of output and whether it influences the environment it interacts with depends on how it is used**. Specifically, Annex I, points (b) and (c) include any software that uses “inductive (logic) programming” “statistical approaches” or “search and optimization methods” in the scope of the legislation which are most often not connected to AI.

Keeping the scope of the legislation as broad as it currently is would risk creating new administrative burdens in areas not directly connected to AI and whose risks are already managed through existing regulations and frameworks, such as the GDPR. This could hinder innovation and create legal uncertainty going forward.

Recommendations

We would recommend a definition of AI that is in keeping with the view of the High-Level Expert Group on Artificial Intelligence, namely that it entails at least three main capabilities: perception, reasoning/decision making and actuation that differentiate it from simple algorithm-driven decision making systems. In order to ensure a clear focus of the legislation on AI, we suggest to preclude source code or pre-trained models from the definition of “AI system” in Article 3, and search and optimisation methods from Annex I. Further, it should be clarified that in order to be considered an AI system a





program must be designed, or have as an intended purpose, to influence the environments they interact with.

Prohibited AI practices

DOT Europe supports the Commission's approach to clearly identify a number of AI applications which will be prohibited outright under the AI Act. However, the current language remains vague, raising important questions as to which applications are covered. For example, the draft regulation prohibits applications which deploy "subliminal techniques beyond a person's consciousness" to distort behaviour or cause harm, but in this context **the word 'subliminal' is undefined**.

On the subject of remote biometric identification, more clarity is needed on how such a prohibition would work in practice and whether it would cover all types of facial recognition technology and one-to-one user authentication (e.g., unlocking a device with voice or facial scan), noting that, without further context or clarification, any form of identification using technologies such as a smart device could potentially be argued to be "remote" or "at a distance".

Recommendations

DOT Europe recommends that **prohibited forms of AI be clearly and narrowly defined so that the regulation does not prohibit a variety of other, less risky uses of AI**. For example we recommend defining "subliminal techniques" to clarify whether such techniques are intended to refer primarily in a traditional sense to subliminal audio/visual stimuli and to refine the definition of "remote biometric identification system" to clarify that requisite comparison to a "reference database" entails so-called "one-to-many", rather than "one-to-one" matching. The co-legislators should also elaborate on the notion of "psychological harm" and provide a clear definition, as well providing references or criteria on how to assess whether an AI system is likely to cause psychological harm.

High-risk AI

DOT Europe supports the Commission's approach to make the AI Act future-proof by creating a definition of high-risk AI applications which can adapt over time and respond to technological developments. However, some concerns remain about Article 7, which foresees that the definition of high-risk AI applications can be amended through delegated acts. While this approach seems to be aimed at allowing the regulation to keep up with technological developments, these provisions would potentially allow the Commission to expand the definition of high-risk AI beyond what was originally foreseen under Article 6 of the proposal.

Recommendations

DOT Europe recommends that **clarity is provided regarding how and when Annex III will be updated**, including whether all or only certain of the listed criteria must be considered and how they should be weighed, and the role industry will play therein.





Data & Datasets

DOT Europe commends the Commission for appreciating the importance of datasets for the successful development of AI. DOT Europe members in particular have put a lot of effort into creating appropriate data validation procedures in order to address the risks which can arise from shortcomings of datasets. That said, Article 10 of the Commission's proposal puts in place **requirements which are practically impossible to meet**. Requiring that datasets be "free of errors", "free of bias" and "complete" is a virtually impossible standard to meet for datasets of any size as the collection and labelling of data is a human effort with an inevitable risk of error (and in some cases, relies on end user input which a provider may not be in a position to verify). Moreover, **"completeness" is an unclear and often subjective or inapplicable metric** in reference to data sets.

Recommendations

While DOT Europe members remain fully committed to using high-quality data sets, we suggest to lower the requirements for datasets that are used in the training of algorithms to make this provision realistically achievable, for example focusing such requirements on taking reasonable and appropriate measures designed to ensure the quality of such datasets, rather than setting an unattainable standard of perfection of the datasets themselves. We furthermore encourage a multistakeholder process tasked with developing consensus standards around issues like data quality, fairness, accuracy, and robustness.

Information obligations

Article 52 of the Commission's proposal requires providers to ensure that AI systems which interact with natural persons are designed to inform the user of this fact. DOT Europe supports the Commission's aim of giving more clarity to consumers, however, **the terms "informed" and "interacting" need to be clarified** in order to provide more certainty about which cases would fall under the scope of these requirements. An overly broad interpretation of "interacting" for instance could apply to features that are a mere output of an AI system, for instance a home page module or personalised search results, rather than just to an interaction in which a natural person would otherwise believe they are interacting with another natural person.

Furthermore, Article 52 imposes certain obligations with respect to emotion recognition systems, defined as "AI system(s) for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data". While DOT Europe supports measures to address risks posed by systems used for such sensitive matters as real-time emotion detection or determination of association with social categories, identifying "intent" is much broader, and could arguably capture basic aspects of such widespread and fundamental technologies as natural language processing which do not present such risks.

Recommendations

We encourage the co-legislators to better clarify these provisions. Terms of Service and automated communication (e.g. automatic reply emails from service provider's support system) should be considered as informing the user. DOT Europe further recommends removing "intents" from the definition of "emotion recognition system" in order to avoid an overbroad definition which, for





example, inadvertently encompasses a wide range of basic natural language processing and similar systems.

DOT Europe also recommends to **impose disclosure obligations only in cases where it is not obvious from the circumstances and the context of use that content is generated through AI systems**, extending the caveat foreseen under 52.1 to provisions contained in arts. 52.2 and 52.3. The AI Act should further clarify that art. 52.1 is intended to apply to AI systems that are designed to make users believe they are interacting with another human and that the information obligation requirements should not come at the expense of the quality of service or user's experience.

Balance of responsibilities between AI providers, deployers and users

The draft regulation does not fully reflect the complexities of the AI ecosystem when it comes to allocating responsibilities for compliance between actors in the value chain. As written, the main burden for complying with the high-risk requirements rests on “providers” while in practice many AI applications may involve different AI systems developed, modified and used by different entities over time.

This is particularly challenging for companies providing general purpose APIs and/or open source AI models that are not specifically intended for high risk AI systems, but are nevertheless subsequently used by third parties in a manner that could be considered high risk and in scope for compliance (e.g. open deep fake detection API that is used by law enforcement, traffic routing model used by municipalities to dispatch first responders). This is to some extent addressed by Article 28, which states that any third party that modifies “the intended purpose of a high-risk AI system already placed on the market or put into service” or makes “a substantial modification to the high-risk AI system” should be considered the provider. However, in the case of open source/API systems where the intended purpose is unclear or open source, using the applications in a different, high-risk operational context would not necessarily modify their intended purpose. In this case, the original developer would remain in the provider role despite having no knowledge of the changes, nor means to fulfil the obligations in the proposal.

Recommendations

DOT Europe suggests clarifying the scope of Article 28 to account for general purpose or open source AI systems which can be used for a broad range of purposes, specifying that in such cases responsibility for compliance, conformity assessment and post-market monitoring lies with the distributor, importer, user or other third-party.

Enforcement

With regards to the enforcement of the AI Act, DOT Europe has a number of concerns relating to the Commission's proposal. We fear that the enforcement structure of the AI Act **will create a complicated regulatory environment that will directly contravene the legal basis for the AI Act**, with a proliferation of national supervisory authorities each with differing interpretation and legal standards and without a sufficiently broad degree of expertise. This would prevent the harmonisation of national laws across Europe and frustrate the goals of the Digital Single Market. Many DOT Europe





members are particularly concerned that this will pose significant burdens on SMEs across Europe, limiting their ability to develop innovative new AI systems in Europe.

In articles 65 and 67, the Commission's text appears to permit market surveillance authorities in any Member State to order the withdrawal from the market of a high-risk AI system even if the system complies with the provisions of the Regulation. Among the potential reasons stated for such an order of withdrawal is that the system presents a risk "to the compliance with obligations under Union or national law intended to protect fundamental rights or to other aspects of public interest protection". DOT Europe is concerned that **such far-reaching capabilities could lead to a fragmentation of the Regulation's Single Market objectives.**

DOT Europe is also concerned by the fact that Article 64 foresees that national market surveillance authorities which conduct checks and inspections have the right to request access to datasets, Application Programming Interfaces (APIs) and even the source codes of AI systems. These requirements should be aligned with the EU Trade Secrets Directive.

Recommendations

DOT Europe recommends that providers can legally challenge data sharing requests to limit their scope to what it is strictly necessary and proportionate to the objectives at hand. Additionally, DOT Europe recommends that the AI Act build on and extend the model of the AI Board proposed in the Act, in order to vest supervisory authority in an entity that can draw upon diverse expertise and better balance tradeoffs between risks and opportunities. Finally, we recommend that the Commission clarify the conditions under which market surveillance authorities can exclude products from the market, e.g. precluding removal for minor or technical violations.

