05/08/2021

EU ARTIFICIAL INTELLIGENCE ACT – SPLUNK POSITION

The development of artificial intelligence has major potential to improve business processes and services for citizens, but there are a number of complex issues associated with its adoption. Splunk supports a flexible policy framework that builds confidence and trust in AI systems, encourages investment in research and development, strengthens cybersecurity and privacy protections, and takes into account different types of AI and machine learning to avoid hampering innovation unnecessarily.

With its strong risk-based approach, the EU's proposal for an AI Act is largely in line with these principles. We welcome the focus on regulating high-risk AI systems and the proposal's approach to conformity assessments (done through internal checks for all high-risk AI except remote biometric identification). We do however have some concerns about the sharing of responsibilities between AI providers and AI users and about the exact nature of requirements introduced for high-risk AI systems.

1. A risk-based approach to regulating Artificial Intelligence is the right way forward

The EU proposal aims to regulate *uses of AI*, rather than AI itself as a technology. On this basis, the proposal rightly aims for a risk-based approach to regulation. Some limited AI uses will be prohibited due to the unacceptable risk they present; some high-risk uses will be subject to compliance requirements before their placing on the market; other low-risk AI systems will only face some transparency obligations. This tiered structure of the Regulation is welcome and should appropriately address the most pressing concerns around AI, for example the safety of human beings or the protection of their fundamental rights. We think that such a risk-based approach will be able to generate trust in the technology amongst citizens and stimulate AI innovation and the development of new AI use cases.

Definition of AI

Whilst the overall approach is correct, we do however have some questions about the definition of Artificial Intelligence in the proposal. The Regulation's definition of AI is very broad, and so is the list of techniques listed under Annex I.

We understand the EU's desire to provide a future-proof definition, but we are concerned that this broad definition could cover techniques that are not *always* AI. For example, under point (c), we would argue that there are lots of "statistical approaches" and "search and optimization methods" that are not AI.

To avoid overregulating non-AI techniques, Annex I could be tightened to focus only on Machine Learning approaches covered under (a). Other public authorities in the world have opted for such a targeted definition, such as the ICO in the UK[1], focusing on supervised, unsupervised, and reinforcement learning.

[1] AI definitions, Information Commissioner's Office (ICO)

Definition of high-risk AI systems

Annex III on high-risk areas also looks quite broad and could be more granular. For example, under 'employment', AI used for task allocation is considered high-risk, which may not be the case (for example in the case of predictive behavioural routing of phone calls). To assess the level of risk, the intensity of harm should be the guiding criterion (which is precisely highlighted under Article 7(2)), and high-risk AI systems should also present a demonstrable impact on fundamental rights or the health and safety of persons. Obligations described in the proposal should only apply to high-risk systems listed in Annex III that meet these criteria.

The list of high-risk AI systems will be updated regularly through the adoption of delegated acts to keep up with technological progress. This is likely to generate legal uncertainty for providers and users of AI. It will be a challenge for companies to determine at any point in time if an AI system is high-risk or not.

2. More balanced responsibilities for AI providers and users

The European Commission's proposal includes a series of obligations to be met by AI providers before placing AI systems on the market (Article 16). After determining that the AI system is classified as high-risk, the provider shall undertake a conformity assessment procedure and ensure that the high-risk AI system complies with all requirements listed in the proposal (transparency, data governance, etc). The AI user is subject to a shorter list of obligations, for example operating the system following instructions of use and ensuring human oversight.

Aiming for the right balance of responsibilities

This split in responsibilities between AI providers and users does not look adequate, especially considering the realities of the market roll-out of AI solutions. Splunk is a provider of AI-powered solutions for specific use cases, for example to look for insights and enhance our security, IT Operations and observability solutions. We provide tooling and frameworks that customers can use to build their own AI solutions. Software providers supplying customers with Machine Learning tools cannot always control how their customers use these tools and deploy their own models.

One key element for the evaluation of AI systems is around the datasets used for their training. Very often, software providers have no control of or access to their customers' datasets. For this reason, they are not able to meet the obligations laid out in Article 10 around data governance.

Article 28, which aims to shift the AI provider's responsibility onto AI users in some circumstances (for example if the user places on the market a high-risk AI system under its name or trademark) does not address these concerns.

Clear and proportionate obligations for all actors involved

The sharing of responsibilities between AI providers and users should more adequately reflect the realities of market deployment of AI solutions. We would recommend three major changes to develop a more proportionate framework.

First, in light of the above-mentioned considerations, we think the entity that determines the purposes and means *by which an underlying model is trained and used* should bear greatest responsibility for ensuring compliance with the AI Act.

Second, we would recommend adding a definition that distinguishes more clearly between *users as deployers* (which is often the case in a B2B context) and *users as individual end users*, which would be a fundamental step in ensuring that all entities involved in the AI deployment phase receive clear and proportionate obligations.

Finally, we would suggest adding an additional category in Article 28 to address instances in which an AI user or another third party uses or modifies an AI system in a manner that would render it a high-risk AI system. In such circumstances, the user or the other third-party should be considered the AI provider under the Act.

Responsibilities of AI providers

AI providers are however aware of their own responsibilities. They are best placed to explain how the AI tool works and how it was developed (e.g. which part of the solution uses AI; which AI technique listed under Annex I was used), so that the users can assess if it is appropriate for them and use it responsibly in the workplace.

AI providers can also make AI systems as transparent as possible for users and explain their intended outcome. We agree with the formulation of Article 13(1) ("sufficiently transparent to enable users to interpret the system's output and use it appropriately") but believe any attempts to open up AI algorithms would provide little transparency to users.

3. Requirements for high-risk AI should be principle-based and achievable

Requirements should be principle-based and easily applicable for developers and/or users of AI solutions. Compliance with some of the requirements proposed for high-risk AI looks very difficult to achieve, especially **Article 10 on Data and Data Governance** and **Article 14 on Human Oversight.**

Data Governance

Article 10(3) provides that "Training, validation and testing data sets shall be relevant, representative, free of errors and complete." Aiming for "free of errors" and "complete" datasets is difficult to achieve, so we would propose a more practical formulation ("whenever possible" or "deploy reasonable efforts to…").

It will also be difficult to guarantee "representative" datasets without a precise definition of what this means in concrete terms. A possible definition could be datasets "that represent real-world distribution".

The wording of Article 10(3) is also probably too simplistic, and we would treat training/validation and testing separately. For testing, we believe it is important to use actual, real-world datasets, e.g. incomplete datasets (even with errors). This is a way to assess how decisions can be biased by the use of imperfect datasets.

On a final note, AI providers have no access to or control over the datasets used by their customers to train AI models, and would not be in a position to meet the requirements laid out in Article 10.

Human oversight

Article 14 provides that "High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use." Natural persons will be asked to "fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible".

It may be very challenging to comply with parts of this requirement for some categories of Machine Learning techniques, especially unsupervised learning. Requiring human oversight would represent a challenge for AI users and would likely limit their ability to take advantage of future ML opportunities. Specifically, "fully understanding" capacities and limitations of AI systems would be very difficult to achieve. However, we agree that humans should have a role in detecting issues and providing feedback on high-risk AI models when anomalies occur.

4. Final remarks

Access to source code is not technically justified

The proposal provides that "Where necessary to assess the conformity of the high-risk AI system with the requirements [of the Regulation] and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system." (Article 64)

This provision is not justified, as we do not think that access to source code will help market surveillance authorities check compliance with the proposal's requirements.

This provision could deter innovation in Europe. If AI providers are asked to provide access to source code, their intellectual property rights could be at risk in the absence of sufficient protection by market surveillance authorities.

Working towards global AI standards

Regulating AI should be done in a way that prevents unnecessary barriers to transatlantic trade and investments. The EU and the US should maintain a dialogue to align AI regulation, with an eye towards developing de facto global standards for AI governance, based on common democratic values. The EU should particularly monitor the work undertaken by the National Institute of Standards and Technology (NIST) to develop a risk-based framework for managing AI bias.[2]

Splunk welcomes the establishment of a Transatlantic Trade and Technology Council (TTC) and, within it, the set-up of a working group on AI. Any AI standards developed within the TTC should be discussed and promoted with like-minded international partners (UK, APAC countries, etc).

About Splunk

Splunk is an advanced operational data platform with use cases in cybersecurity, IT Operations and Observability (DevOps). Splunk technology is designed to investigate, monitor, analyse and act on data at any scale, from any source and over any time period. Splunk allows customers to ask any

[2] A Proposal for Identifying and Managing Bias in Artificial Intelligence, NIST, June 2021

questions of their data, from the optimisation of industrial processes to the early detection of cyber threats.

Splunk played an important role in a WEF project on "Unlocking Public Sector Artificial Intelligence" that provides guidelines to help governments to procure AI responsibly.

www.splunk.com

EU Public Affairs Contact:

Clara Lemaire, European Government Affairs Manager | clemaire@splunk.com | +32492613659

EU Transparency Register: 676974536971-63