10 SEPTEMBER 2020

DIGITALEUROPE input to Commission Inception Impact Assessment on AI

DIGITALEUROPE supports the Commission in its ambition to stimulate the development and uptake of AI and new technologies, while ensuring that any potentially linked risks are adequately addressed. In this paper, we provide our comments to the public consultation on the published Inception Impact Assessment[1].

General considerations

As highlighted in this Inception Impact Assessment (IIA), existing EU regulation on the protection of fundamental rights, consumer protection as well as regarding product safety and liability remains relevant and applicable. This robust regulatory framework is and should remain technology neutral.

DIGITALEUROPE also agrees with the Commission's reasoning that there could be some room to evaluate the existing framework and ensure it remains fit for purpose, not in the least to avoid a situation of increased regulatory fragmentation, with diverging or even conflicting rules between Member States.

Any new legislation or measures should, within that same reasoning, also be mindful of the global nature of the development of new technologies and not lead to unwarranted divergence between the EU and other countries or needlessly complicate the development or deployment of AI products and services from companies and organisations operating beyond the EU, or wishing to scale up to non-EU markets. This type of regulatory divergence may also not allow the EU to benefit from AI products and services developed in other markets.

Further, the overall aim of the EU's approach should not lead to overly burdensome obligations on organisations developing, deploying or using AI technologies, where more light-touch or industry-driven measures would suffice. Otherwise, the launch of certain new and cutting edge AI-powered products and services in the internal market could be delayed or even not take place at all.

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Requirements-for-Artificial-Intelligence

Analysis of the various options

In the IIA, the Commission outlines four scenarios, in addition to the baseline or status quo, ranging from a purely soft-law approach to legal requirements on any and all types of AI applications. When it comes to regulatory tools, the IIA, just as in the Commission White Paper, identifies potential ex-ante and ex-post mechanisms for compliance and enforcement. The IIA also recognizes that some of these tools may not always be equally effective for various types of AI applications, as well as entailing potentially significant costs or complications for organisations, both for developing or deploying AI.

Given the nascent and diverse nature of AI applications and technologies, DIGITALEUROPE therefore recommends the Commission to take a risk-based and focused approach. Such an approach should be based on clear definitions and well-identified regulatory gaps. It should take into account the risk posed by the deployment of an AI system, the area of application, type of deployer (including whether it's private or public sector) and nature of the risks.

In line with these views, DIGITALEUROPE therefore considers a mix of the various options provided in the IIA. A fully soft-law approach as proposed in Option 1 would be a good starting point, but we recognize that it may not be sufficient to provide enough legal certainty and clarity. It may also still lead to regulatory fragmentation or divergence.

A voluntary label, as suggested in Option 2, may have value if well designed, recognised and sufficiently specific, but seems premature at this phase. It would in any case require further reflection on how such a framework could accommodate the myriad of AI use cases and application areas. Its usefulness would very much depend on the scope of the products considered, their applications and end-user, and the availability of common standards.

A general voluntary label could further have limited or even a negative impact on consumer trust, through label fatigue and overuse. Given also that the use of label would likely require extensive assessments and market surveillance, it could be a disproportionate measure compared to the envisaged effect. Voluntary labels should therefore ultimately be considered in specific contexts, focusing on areas where it could ameliorate user trust and reduce such deterrents to adoption.

Option 3 has several sub-options, introducing mandatory requirements to either very specific applications, to 'high-risk' applications, or to all applications.

Option 4 then adds in a tiered model with types of risk.

As acknowledged in the IIA, Option 3 and 4 could be an adequate model to take forward, but are completely dependent on yet to be defined elements, including what would be considered as 'high-risk', how and when to asses an application or use case, and the aforementioned lack of definition of 'AI systems'.

Further, the requirements themselves, how these can be set and measured, how they are enforced (i.e. ex-ante or ex-post) are intrinsically linked to the scope. Some requirements (e.g. on ways to provide transparency) are sensible in a business-to-consumer context and can be seen as requiring a more case-by-case approach. Other requirements (e.g. on accuracy thresholds) may be more common in a business-to-business context and could possibly be assessed in advance of deployment.

DIGITALEUROPE therefore advises against any proposal that would mandate specific requirements on all AI applications (i.e. Option 3, sub-option c). or similarly, we strongly advise against expanding the scope of the definition to encompass all of 'automated decision making'. This would simply not be proportionate or effective towards the Commission's intended goal as well as going against the initial and thoughtful direction of the AI White Paper. Most AI applications do not pose any risks to fundamental rights or safety (for example industrial applications such as optimizing production or logistic chains, or optimizing consumer device performance) and therefore should not be subject to new regulation in this area. It should also be acknowledged that not every use of AI in a given sector (e.g. healthcare) necessarily involves significant risks.

Regarding enforcement, we find that the ex-post approach for when problems arise as the appropriate and proportionate mechanism, as in many times it will only be on a case-by-case basis that the nature of the AI deployment and the ways to mitigate or prevent potential harms will become clear. As we further detail below, the types of risk can vary greatly and only in some situations can they be fully foreseen or assessed.

For those areas then where policy-makers do consider ex-ante enforcement, we recommend that this should take the form of self-assessment procedures based on clear 'due diligence' guidance from the regulators. A practical approach would be for regulators to set principle requirements to be met by (global where possible) industry-led voluntary standards, or in their absence to provide templates and guidance on how to carry out and document the risk assessment, but delegate responsibility to those using and most familiar with the AI system to conduct an accurate and timely assessment.

Any such ex-ante assessment should in any case be limited, and be aligned with existing procedures where possible. The use of conformity assessments should therefore only be considered in very specific cases, where the nature of the risk (including type of damage and likelihood of occurrence) lends itself to an ex-ante assessment and mitigation strategy. This could specifically be the case with the use of AI systems in applications where faulty behaviour can cause physical harm (though even here this varies with the eventual intended use). We find that many such scenarios may fall in already regulated sectors, in which case any measures should as much as possible be coordinated and part of the established conformity assessment procedures already present in many sectors (for example the Medical Devices Regulation in the healthcare sector, or the Type-Approval process for vehicles).

In areas where the potential risk is however more of a nature to damage or restrict fundamental rights (e.g. privacy, discrimination) an approach combining principle-based internal governance processes, industry best practices (including standardisation where possible), and ex-post monitoring. This is because those risks are far more dependent on the context and specificities of the use case given the existing and technology neutral EU acquis, it will often also be much more a matter of interpretation and application of existing legislation.

For example, a case of discriminatory bias may entail many different factors to take into consideration: the training data set, how the algorithm was tested, how the deployer chose to implement and use the AI system to assist its decision-making and, potentially, which parameters the deployer adjusted or finetuned. Those factors cannot be easily made subject to ex-ante requirements, thresholds or technology standards. Rather, these types of harm are better mitigated and prevented through information and communication between developer and deployer, best practices for testing and upkeep of the AI system, and appropriate transparency towards users and regulators.

Conclusion

Consequently, following our comments above and within the proposals made in the IIA, we would suggest the way forward for the Commission to lie in a combination of industry-led measures (Option 1) with targeted obligations for specific categories of high-risk applications (Option 3a/b). It will be imperative for the terms AI and risk to be clearly defined, and that any requirements should be operational in practice. Where possible, classifying and assessing the risk of the AI applications should be part of respective existing sector-specific regulatory frameworks.

DIGITALEUROPE further refers to our response to the AI White Paper consultation (read here) where we elaborate on many of these aspects and considerations in more detail.

FOR MORE INFORMATION, PLEASE CONTACT:

Jochen Mistiaen

Senior Policy Manager

jochen.mistiaen@digitaleurope.org / +32 496 20 54 11

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world’s largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world’s best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK