The Future of Artificial Intelligence

Victoria Hewson, Head of Regulatory Affairs, Institute of Economic Affairs

In February the Commission published the White Paper *On Artificial Intelligence – A European approach to excellence and trust*. It includes some interesting proposals on funding, attracting investment and skills, including prioritising the development of AI hubs across Europe. The most eye-catching proposals (and the focus of this briefing) relate to a future regulatory framework to support an ecosystem of trust and ensure that the use of AI in the EU is in accordance with "European values". But while the aspiration of supporting development and adoption of AI in Europe is welcome, it is based on some questionable assumptions and in places veers dangerously towards protectionism.

"Lack of Trust"

The White Paper recognises the importance of data and AI for economic growth and societal wellbeing but asserts that "lack of trust is a main factor holding back a broader uptake of AI". It notes that while a number of requirements identified in guidelines produced by the High Level Expert Group on AI are already covered in existing laws and regulations, those regarding transparency, traceability and human oversight are not specifically covered for many economic sectors. While the Commission accepts that legislation on data protection and privacy, non-discrimination, consumer protection and product safety all apply to AI applications, it notes that "some specific features of AI (e.g. opacity) can make the application and enforcement of this legislation more difficult." It therefore considers that a review of current legislation is necessary to establish if adaptation or new legislation is required. It also notes that some member states (such as Denmark, Malta and Germany) have launched their own measures, which it is feared point to "a real risk of fragmentation in the single market" which would "undermine the objectives of trust, legal certainty and market uptake". A "solid European regulatory framework for trustworthy AI is therefore thought to be necessary" to protect fundamental rights (such as privacy, freedom of expression and freedom from discrimination in employment) and address safety and liability-related issues.

According to CBInsights[1], only 15 European companies are in the top 100 global AI start-ups – and eight of them are in the UK and one in Switzerland. 65 are in the United States.

The Framework

The scope of the EU regulatory framework is based on a definition of AI composed of two "main elements" – data and algorithms. Machine learning is described as a subset of AI where algorithms are trained to infer patterns based on a set of data to determine the action needed to achieve a goal. The regulatory framework should be "effective to achieve its objectives while not being excessively prescriptive so that it could create a disproportionate burden, especially for SMEs". For this reason, the Commission favours a "risk based approach" where the new enhanced regulatory framework would apply to high risk applications. Lower risk applications could choose to adhere to the new framework as a form of assurance, but it would not be mandatory.

The (cumulative) criteria that would qualify an application as high risk are:

- Deployment in a sector where significant risks can be expected to occur, such sectors to be specifically and exhaustively listed. Examples include healthcare, transport energy and parts of the public sector.

- Use in the sector is such that "significant risks" are likely to arise – not every use of AI in a high risk sector will itself involve significant risks and the level of risk cold be based on impact on affected parties, for example whether it produces legal effects on individuals or risk of injury, death or material or non-material damage. Biometric identification usage would always be considered high risk, as would use in recruitment processes and situations affecting workers' rights.

The criteria are intended to ensure that the regulatory framework is targeted and provides legal certainty, though critics might point out that they are somewhat tautological. The proviso that there may also be exceptional circumstances where a particular use case is high risk in itself and irrespective of the sector in which it is deployed could be argued to undermine the legal certainty objective. The examples of high risk sectors accords with the examples of sectors where the Commission thinks the EU is strongest and could see most progress, like healthcare and transport so the Requirements risk holding back exactly the uses that the Commission is keenest to promote. The examples of high risk use cases include some, like content moderation, where use of AI is either mandated or encouraged by EU rules and guidance, like the Digital Copyright Directive and Code of Practice on Disinformation.

The Requirements being considered for the framework relate to listed "key features":

- training data;
- data and record keeping;
- information to be provided;
- robustness and accuracy;
- human oversight;
- specific requirements for certain particular AI applications, such as those used for purposes of remote biometric identification.

AI solutions in the high risk category will have to undergo conformity assessment and certification in respect of the requirements, in the same way that products like medical devices do, under goods regulations.

Excessively Prescriptive?

Most of the requirements seem to be desirable features that users of AI solutions would be incentivised to address with their suppliers or developers in any event. The White Paper seems to be lacking an analysis of how the market has failed to address these matters, or how they have been dealt with in member states and non-EU territories like the United States that have seen more success in the deployment of AI.

Some of the requirements risk undermining the viability of using AI at all (as has been noted in respect of an existing, similar requirement in Article 22 of the GDPR[2]). For example (under "record keeping") it would be necessary to ensure that "potentially problematic actions or decisions by AI systems [can be] traced back and verified" and (under "human oversight") the framework would require that all output must be reviewed and validated by a human before it is allowed to become effective. Some of the requirements also seem to be in tension with the objective of legal certainty – for example under human oversight it is noted that "the appropriate type and degree of human oversight may vary from one case to another" and the cited objectives of "trustworthy, ethical and human centric AI" that respect the EU's "values and rules" seem, well, subjective.

Responsibility for complying with the Requirements will be addressed to "the actor(s) who is (are) best placed to address any potential risks". Such actors could include the developer, the person who uses the AI equipped product or service or others such as importers, distributors service providers and private users. Presumably the eventual regulation will be more specific, if the objective of legal certainty is to be respected. It is noted that the obligation to comply with the new requirements will be different from the question of liability to end users or other parties under product liability law (as it may be developed pursuant to the accompanying report).

Technological Sovereignty

Importantly, the Commission is of the view that the requirements should apply to all operators providing AI applications in the EU, irrespective of where they are based geographically, otherwise the objectives of the legislation could not be achieved. This seems to run counter to the assertion that it is lack of trust that is holding back wider adoption of AI capabilities in the EU: if that were the case, users in the EU would surely choose products developed under the EU framework, and products from elsewhere that did not meet the requirements would not take hold in the market. There would therefore be no need to exclude solutions developed under the laws of other jurisdictions. In fact the extra territorial application seems more designed to pursue the goals also referenced in the paper of increasing "Europe's technological sovereignty in key enabling technologies and infrastructures for the data economy", creating "European data pools", and exporting Europe's values across the world, which arguably could all work against the broader objective of encouraging adoption of and investment in AI.

> The White Paper is accompanied by a detailed Report on product safety and liability legislation. It highlights issues such as accountability along the supply chain and issues from the ongoing development of applications which "may make it difficult for persons having suffered harm to obtain compensation under the current EU and national liability legislation".

As well as neglecting potential market solutions, the White Paper does not appear to consider that existing EU legislation may be contributing to the EU falling behind in AI uptake and investment, such as the copyright exemptions for text and data mining

[1] CBI Insights Research (2019). "*AI 100: The Artificial Intelligence Start-ups Redefining Industries*" https://www.cbinsights.com/research/artificial-intelligence-top-startups/

[2] Clarke, Osborne. Lexology (2020). "*European Commission's AI White Paper: A New Framework for Liability Issues"* https://www.lexology.com/library/detail.aspx?g=a24d4a2e-32be-438e-9abd-556aad2fac44

(vital to the development of AI) in the 2019 Copyright Directive[3]. The Commission does not countenance reviewing existing regulations for compatibility with AI. Quite the reverse, it emphasises that all AI applications "remain entirely subject to existing EU rules". Similarly, the reflexive instinct in favour of preventing fragmentation in the single market risks missing out on opportunities to learn from best practice as it evolves across competing jurisdictions. Research by McKinsey[4] found that different member states had varying strengths and weaknesses in key enablers for AI and that "The dispersion of strengths indicates that countries can borrow best practice from each other to create a more favourable and more enabling environment for AI."

In short, a regulatory framework intended to harmonise regulation of this complex area, with a view to its adoption around the world, needs to be rigorously justified. The cost of misjudging the needs for and effects of a (well intentioned) regulatory framework would be great, if it had the effect of slowing down innovation and adoption of AI, causing EU firms to fall further behind global competitors at a time when the global economy will be more than ever in need of innovation to power a recovery from the coronavirus pandemic.

In accordance with the Commission's Better Regulation guidance on achieving objectives "at minimum cost … while avoiding all unnecessary regulatory burdens", a fuller analysis of the laws, regulations, good practices and markets of countries (in Europe and beyond) that are most successful in AI should be considered, to validate the assertion that a specific regulatory framework of the kind envisaged in the White Paper is necessary to compete in AI.

A regulatory framework to support innovation in and uptake of AI should not duplicate existing obligations (for example, on record keeping, it is already a requirement of the GDPR that data processors must be able to demonstrate and provide evidence of their compliance with privacy and data protection laws), making AI less appealing than more basic technologies. Its main focus should be on transparency through explainability or interpretability, including addressing the problems caused by article 22 GDPR. This will rely as much on standards developed by industry, as on regulation, and could be further supported by the EU through investment in research into explainable machine learning models.

The interplay of a regulatory framework with the laws on liability for damage arising from defects in an AI solution is pivotal, and legislators should resist ex ante, prescriptive measures that pre-empt developers and users from reaching better outcomes, while ensuring that legal redress is available in the event of any loss or damage. Clarity and certainty on explainability/transparency and product liability should mean that the other Requirements will be met by the market without the need for specific regulation.

This briefing has been submitted to the European Commission's consultation on AI.

References

CBI Insights (2019) *AI 100: The Artificial Intelligence Start-ups Redefining Industries*

Lexology Library (2020) *European Commission's AI White Paper: A New Framework For Liability Issues*

Kluwer Copyright (2019) *The New Copyright Directive: Text and Data Mining (Articles 3 & 4)*

McKinsey Global Institute (2019) *Notes From The AI Frontier Tackling Europe's Gap in Digital and AI*

[3] Hugenholtz, Bernt. Kluwer Copyright Blog (2019). "*The New Copyright Directive: Text and Data Mining (Articles 3 and 4).*" http://copyrightblog.kluweriplaw.com/2019/07/24/the-new-copyright-directive-text-and-data-mining-articles-3-and-4/

[4] Bughin, Jacques. McKinsey Global Institute (2019). "*Notes From The AI Frontier Tackling Europe's Gap In Digital and AI*" https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Tackling%20Europes%20gap%20in%20digital%20and%20AI/MGI-Tackling-Europes-gap-in-digital-and-AI-Feb-2019-vF.asshx