June 2020

# European Commission's White Paper on Artificial Intelligence - A European approach to excellence and trust

ETNO position paper

ETNO welcomes the publication of the European Commission's White Paper on "Artificial Intelligence – A European approach to excellence and trust" (the "White Paper"), a key pillar of the Commission's digital strategy for the next five years.

The European telecommunications industry will be a key enabler of the future AI ecosystems. 5G and fibre connectivity will accelerate the digitisation of services and industrial processes, enabling the rapid expansion of the Internet of Things (IoT). The massive amounts of data generated by IoT connections and devices will open up new growth opportunities for data analytics and AI services in Europe. High-class, secure connectivity will then drive IoT, and IoT will in turn fuel European AI. Together, they can form a truly powerful virtuous circle that our industry is committed to nurturing. Digital network providers themselves increasingly deploy AI solutions in various areas, typically to improve efficiency in network operations (e.g., network security and predictive maintenance), to enhance customer experience, and for better product and service development.

We welcome the two-fold approach described in the White Paper, which aims at fostering the uptake of AI technologies and products in Europe as part of an "ecosystem of excellence", while ensuring their compliance with European ethical norms, legal requirements and fundamental rights that together form an ''ecosystem of trust''[1]. These two elements are mutually supportive, as long as new requirements to build a culture of trustworthy AI are proportionate to the objective of establishing European excellence.

The overarching goal of the European AI strategy should be to pursue a coordinated approach to AI across the EU, bolstering the Union's capacity to keep pace and remain competitive with other regions of the world in the development and deployment of AI applications. Divergent national requirements that raise barriers to the development and the uptake of AI technology across the single market should be avoided. When defining new rules, it is equally important to consider the whole AI value chain in order to target in the first place those segments that are most suitable to bear responsibility in line with the "polluter pays principle".

Whereas we largely commend the overarching vision outlined in the White Paper, we would like to offer our recommendations to further strengthen the promotion of a trustworthy AI as a competitive advantage and investment incentives in Europe.

[1] ETNO's contribution to the "Ethics Guidelines for Trustworthy Artificial Intelligence'' is available at https://www.etno.eu/library/389-etno-response-to-the-stakeholders-consultation-on-draft-ai-ethics-guidelines.html.

## 1. An Ecosystem of Excellence

We welcome the emphasis on the objective of enabling an "ecosystem of excellence" for AI; however, we also believe that in fact the White Paper focuses too much on the regulatory aspects related to trustworthy AI. The document lacks bold and actionable measures to mobilise resources that can achieve the excellence ecosystem along the whole value chain. Furthermore, the paper does not sufficiently expand on the details of actions that would enable the uptake and scalability of AI technology and products across Europe to drive EU competitiveness on the global scene.

The world is witnessing an intensifying race for global dominance in AI between Asia and the United States, which have both been outspending Europe in research funding, patent applications and technological development (see Fig. 1 and Fig. 2). The strong leadership role of the US and some Asian countries in AI technology undermines Europe's goal to become a strategically autonomous global power. European technology companies suffer from insufficient dynamism and scale compared to their Asian and US counterparts, not least because of the historical fragmentation of the European market.

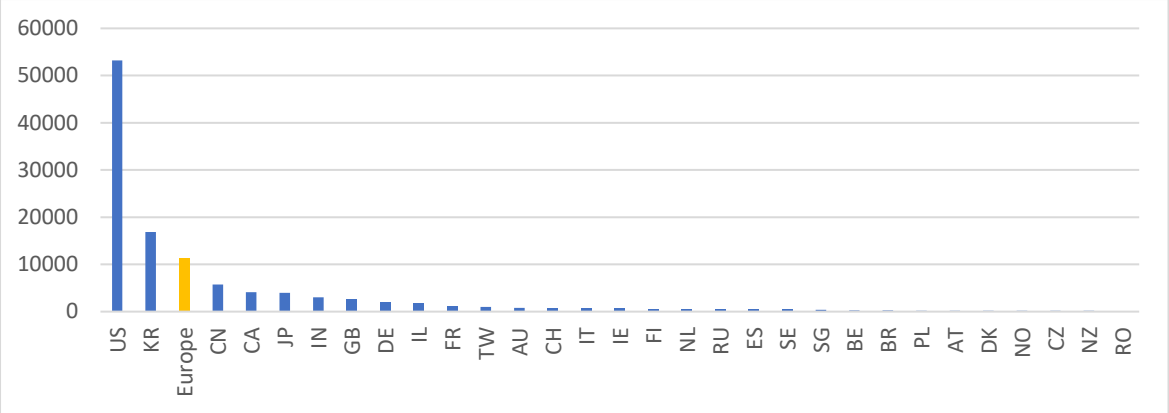


Fig 1. A.I. Patents granted by inventor's country (2010-2020). Source: Analysys Mason, 2020.

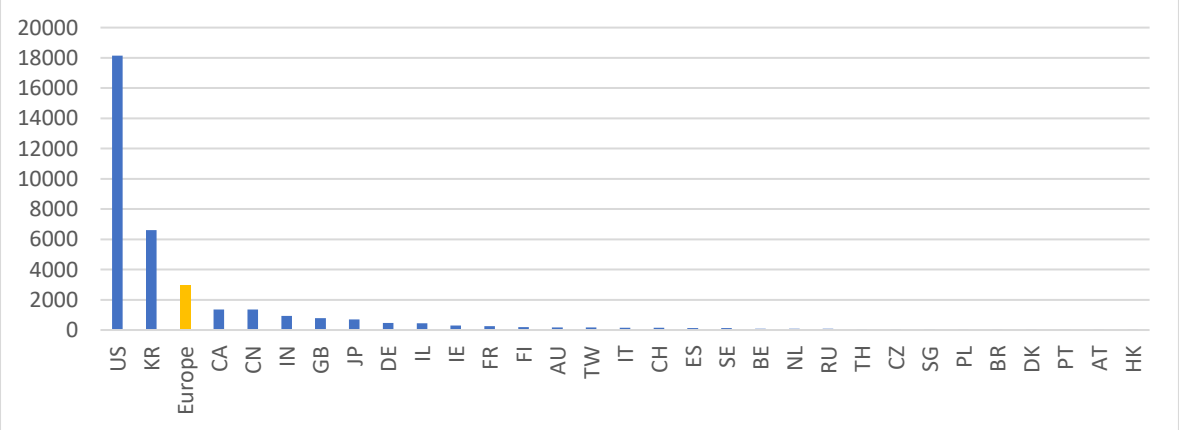


Fig.2 AI inventors in Telecom by country (2010-2020). Source: Analysys Mason, 2020.

Nonetheless, although Europe is lagging behind in the race for technological leadership in AI, it remains a large and attractive market for AI technologies. There certainly is a window of opportunity for the EU to act.

To seize the trustworthy AI opportunity, Europe needs to attract a larger pool of public and private investments in AI technology development and to overcome fragmentation in the access to and retention of talents. Cross-national efforts and collaboration between public and private partners must be reinforced.

More importantly, a European approach should foster the creation of technology ecosystems around AI applications in the strategic industry sectors where Europe has been traditionally strong, such as manufacturing.

Even though public spending accounts for nearly half of the EU's GDP, a reference to the crucial lever of public procurement is missing in the White Paper. Similarly, the paper fails to expand on EU-funded national and transnational lighthouse projects that would establish a pathway for further development and implementation of AI.

## 2. An Ecosystem of Trust: Regulatory Framework For AI

### Definition of AI

The White Paper gives a broad definition of AI that exacerbates, rather than minimise, legal uncertainty. According to the document, *"AI is a collection of technologies that combine data, algorithms and computing power"* pointing to the *"the main elements that compose AI"* being *"data"* and *"algorithms"*. This definition is too broad, and it is unclear whether it refers to AI, machine learning or automated decision making. It could potentially apply to any given piece of software, going much beyond the scope of the White Paper.

Furthermore, the proposed definition does not correspond to the one given by the Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG) in its Ethics Guidelines for Trustworthy Artificial Intelligence, which was widely endorsed by industry, civil society, and academia. Inconsistent definitions at EU level may create confusion and uncertainty, in view of the planned next steps that will need to build on a shared understanding of AI.

We recommend to carefully review the definition of AI and carefully delineate its perimeter, drawing from the definition rendered by the HLEG guidelines. An accurate definition of an AI system is the key to a proper problem assessment.

### Existing regulatory framework and AI

Today, no specific legal framework to regulate AI exists in Europe. The development, deployment and use of AI systems are subject to a range of horizontal laws and principles such as rules on personal data protection and privacy, consumer protection, product safety and liability.

We support the proposed approach to first examine the existing regulatory framework and assess whether adjustments are necessary to address the emerging risks potentially posed by AI systems, before designing additional legislation. A profound review of current regulation is also crucial to ensure consistency of any AI-specific rules with the broader EU legal framework. We appreciate that legislative review is a time-consuming and sensitive exercise that must be undertaken with caution, involving a relevant corpus of competencies across various domains, and engaging with stakeholders through a transparent public consultation process.

**Risk-based approach**

ETNO supports the proposed risk-based approach to AI regulation, including a conformity assessment requirement exclusively targeted to "high-risk" applications of AI. However, for the sake of greater legal certainty, further adjustments and clarifications are needed.

The cumulative criteria of (1) high-risk sectors and (2) high-risk applications of AI in those sectors are very sensible. However, while the former criterion provides regulatory certainty on specific sectors, the latter criterion requires further specification.

It should be very clear why certain sectors and applications specifically pose a direct risk of damage, death or significant physical or non-physical harm to people. The principles that identify a sector or application as high-risk should then be clearly defined, e.g. by specifying the "significant" impact on affected parties or other "exceptional instances". The White Paper considers significant risks from a very broad viewpoint of safety protection, consumer rights and fundamental rights.

The Commission's intention to periodically review the list of high-risk sectors could bring legal uncertainty to all sectors that currently are not placed this category, which could eventually have negative effects on their investment plans. Therefore, the review periods should be appropriate.

Furthermore, it should not be forgotten that AI technologies are an integral part of larger value chains, where different players play different roles. Those players (and sectors at large) may be exposed to different levels of risk, across the value chains, for which more clarity is warranted. How the responsibility for complying with the mandatory requirements suggested in the paper would be shared among the different actors in the chain remains an outstanding issue. For instance, AI technology can be developed by a research institution, integrated as part of a service by a commercial player, and deployed and/or sold to end-users by a government agency in a high-risk application. How would responsibility for complying with the mandatory requirements be shared between these different actors? The research institution or commercial player may not know at development stage that the AI system will end up in high-risk application.

More specifically, it is not clear whether the providers of AI-enabled business-to-business (B2B) solutions (and services to consumer markets) belong to the non-exhaustive list of sectors at p. 17 of the White Paper. Would, for example, telecom operators providing AI-enabled 'smart connectivity' solutions that guarantee quality of the service to hospitals fall under the high-risk sector definition of the White Paper, hence be subject to ex-ante conformity requirements? This could be clarified if the definition of high risk specified that the risk of damage, death or harm should be directly posed by the system itself. This would avoid that a single AI-based subsystem be considered high-risk depending on where it is deployed. If indirect risks were also factored in, legal uncertainly for all providers and the complexity of *ex-ante* conformity assessment would increase exponentially.

Finally, it remains unclear whether this definition of high-risk AI application will be consistent with the high-risk definition in the scope of the proposed liability provisions for AI systems[2].

**Requirements for High-Risk AI Applications**

The White Paper proposes new measures to remedy *"specific features of AI (e.g. opacity) [that] can make the application and enforcement of this legislation more difficult."* Those requirements relate to training datasets, record-keeping, provision of information on AI applications, robustness and accuracy, human oversight, and specific requirements for facial recognition.

- **Training data.** If it becomes mandatory to check the adherence of trained datasets to EU values and rules, the suppliers of such datasets should have an obligation to certify that their data lives up to the standards. Nonetheless, it could often be challenging and impractical to prove the absence of bias in the datasets: checking for absence of bias against sensitive information requires that this information is available in the dataset[3]. Due to data minimisation requirements provided by the General Data Protection Regulation (GDPR) and the possible risk of unwanted access to or disclosure of data, organisations may actively decide not to store such sensitive information. It is even more challenging to prove the absence of bias that violates "EU's values and rules" based on the requirements set out by the White Paper, since they would compel a great level of granularity of datasets involving the processing of special categories of data. The importance of distinguishing the responsibilities of the dataset owner and of the user who applies the dataset must also be made clearer. It should be on the AI engineer to validate and explain the training data used. The dataset owner should describe and disclose how the dataset was created.

- **Keeping of records and data.** The keeping of records could be a reasonable means to help users prove mistakes and harm in the context of liability claims. This requirement should be in accordance with the GDPR's documentation obligations. As such, the requirement to keep the datasets themselves in certain justified cases should be strictly defined. Additionally, this approach should be consistent with the broader liability framework.

- **Information provision.** We welcome the acknowledgment that the information to be provided should be tailored to the particular context. We believe that it is proportionate for competent authorities to impose reasonable requirements and demand access to results and decisions of the AI systems. Such interventions should respect intellectual property rights and business secrets, to not cause harm to competition and innovation. On the contrary, it would be disproportionate to grant competent authorities' access to and review of algorithms and data models, unless this is justified by a risk to public health or national security posed by the AI application at hand. Additionally, requesting that the data used to train and periodically retrain algorithms be stored for an undefined amount of time would be disproportionate as the amount of data may be enormous.

[2] The report of DG JUST's Expert Group on Liability and New Technologies is available here: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608

[3] https://business.blogthinkbig.com/is-your-ai-system-discriminating-without-knowing-it-the-paradox-between-fairness-and-privacy/?_thumbnail_id=5164

- **Robustness and accuracy**. Alongside the *ex-ante* conformity assessment requirement, specific conditions to ensure resilience to attacks and security (e.g. security-by-design), general safety, accuracy and reliability should be considered. Appropriate technical standards could be approved, possibly based on the certification mechanisms provided by the Cyber Security Act. However, this must not lead to constraining innovation and growth and preventing EU undertakings from developing and applying the AI technology across high-risk applications and sectors, such as public health, cybersecurity or critical transport infrastructure.
- **Human oversight.** We generally support such obligation, which should remain limited to high-risk applications. The degree of oversight, human in the loop (HITL) or human on the loop (HOTL) could vary from one application to another, for the sake of proportionality depending on the risks involved. Further details are needed on when HITL or HOTL should be adopted.
- **Biometric identification in the public sphere.** We consider such practices as highly problematic, especially against the objective of creating an ecosystem of trust. If biometric identification in public spaces were to be permitted in principle, it should always be considered as a "high risk" application. Additional rules should restrain its application, considering its severe impact on individuals and society.

**Ex-ante Conformity Assessment**

We agree that AI systems should reflect European values and rules, and conformity assessments for high-risk AI applications would help confirm that this expectation is met. Nonetheless, greater legal certainty around the concrete mechanisms for the *ex-ante* conformity assessment is needed, ensuring that Europe does not create red tape for AI industrialization and growth. *Ex-ante* conformity should remain limited to high-risk AI and be carefully designed to avoid inhibiting the development of AI applications in Europe versus other regions of the world. If the *ex-ante* conformity assessment process implied the intervention of external entities (e.g., regulatory authorities or assessment bodies) during the development process, the time to market of AI developed in Europe would be severely slowed down. Finally, *ex-ante* conformity should also apply to AI systems developed in third countries before they are deployed in the EU's single market.

**Safety and Liability**

The emerging AI technologies are set to challenge the current legal framework for product safety and product liability. At the same time, digital products and services typically include different and interlinked technologies, with little user awareness. We believe that consumers should be able to rely on consistent and easy-to-understand safety and liability rules. As a general principle, ETNO recommends that decisionmakers refrain from creating AI-specific regulation and that they focus on guaranteeing consistency by applying horizontal rules in a technology-agnostic way. This would also allow to apply the EU's innovation-friendly approach to liability to other crucial technologies, such as the IoT.

To address potential issues around liability, undertakings along the value chain should ensure clarity within their contractual arrangements as to which party is responsible for any physical or non-physical harm caused by an AI-enabled product or service to individuals. Yet, anticipating the outcomes of fully autonomous AI systems and attributing liability for their damages will become inherently more difficult.

Beyond the Product Liability Directive, liability in business-to-consumer (B2C) relations regarding defective products or services is also based on contractually agreed terms, according for instance to the Sales of Goods Directive and the Digital Content Directive. Sector-specific laws, such as the European Electronic Communication Code and the Telecom Single Market Regulation, lay down liability provisions concerning connectivity services. Therefore, consumers can increasingly rely on EU rules that influence their contractual rights and that should be considered when assessing potential gaps in the Product Liability Directive or Product Safety Directive.

If liability rules are tightened, the last link in the value chain such as the deployer or trader must not be left alone. A better and fairer distribution of liability throughout the value chain, with a focus on AI technology developers like hardware manufacturers and software developers, would enable the downstream value chain to fulfil their obligations, preventing unfair burdens on them, and guaranteeing security safeguards for consumers. In line with the "polluter pays principle", obligations to mitigate the risks should target the actors that are best suited to held responsibility.

Reforms to improve consumer safety should rather focus on "*ex-ante*" mechanisms based on the Product Safety Directive, which would set higher safety requirements for getting access to the EU market. This will also directly address those parts of the value chain that should be responsible for the safety of their products in the first place.

For high-risk AI systems, the framework of *ex-ante* safeguards via a conformity test before a product is placed onto the market is a reasonable complement to applicable *ex-post* safeguards that apply after placement in the market, according to liability rules. As already noted, applying the conformity test to AI applications that are developed in third countries before they are offered in the EU market or to EU citizens could be a value-add.

The review of the Product Safety Directive should take into account the whole cycle of development, deployment and use of emerging AI technology. The introduction of mandatory security updates supply should be an important area of intervention. This needs to go hand in hand with updated liability rules. For low-risk AI applications, users should be obliged to install the software updates made available to them, in order to preserve their safety and security and to not lose redress claims in case of damage. For high-risk applications, an obligation for the producer to provide and install such updates should be considered.

**Privacy related matters**

The GDPR is a principles-based law designed to be future-proof and adaptable to emerging technologies, such as AI. In addition, the GDPR embeds a risk–based approach that allows for the consideration of risks and harms to individuals and to calibrate compliance accordingly. Therefore, as far as personal data is concerned, the risk-based and technology-neutral approach of the GDPR provides a level of data protection that is adequate to the risk of the respective processing also with regards to AI development, deployment and use.

Still, as already observed, several of the GDPR's provisions (e.g., compatible use, data minimisation, automated decision-making) may lead to tensions with AI applications. New EU guidelines that clarify how the existing data protection and privacy framework applies in the AI context would be more suitable than additional AI-centred privacy legislation.

Although the White Paper seems to call for both high-quality training data and strict restrictions on personal data, in practice the two might be in contradiction and need to be balanced. The calibration between accuracy, sufficiency, representativeness, and personal data protection should be carefully considered because limitations to personal data processing may undermine the quality of training data. Training AI systems by processing personal data cannot solely rely on the use of anonymous or non-personal data. Furthermore, the application of consent requirements for the use personal data for AI training often results in insufficient training datasets in practice.

Under the current data protection legislation, AI training on personal data usually falls under the "legitimate interests" legal ground for processing, or can sometimes be considered as compatible further processing. These options should not be further limited. However, the sectors subject more specific privacy laws in addition to the GDPR (such as telecoms with the e-Privacy Directive, but also healthcare, finance etc.) often are subject to stricter legal grounds and conditions for processing certain types of personal data, which seriously undercuts their possibility to use personal data for AI training. To ensure high quality of AI training data, it would be important to have clear and consistent legal grounds for using personal data in AI training, which could also apply to data subject to sector-specific regulation.

**Voluntary labelling**

A voluntary labelling framework aimed at sustaining the uptake of trustworthy AI in Europe is a reasonable option. However, it is necessary to clearly define labels and their assignment mechanism. Criteria underpinning the labels could relate to e.g. transparency, robustness, and human oversight. The role and the authority of testing centres shall be further defined.

The voluntary nature of this labelling system should not become a *de facto* legal requirement for market access. Criteria to comply with such labels must be meaningful to users, while avoiding excessive burdens on businesses to not discourage them from adopting these labels.

**Governance**

Several governance and enforcement aspects of the AI framework need to be resolved, as the White Paper does not provide strong guidance. For example, it is not clear who decides whether an AI application falls under the high-risk regime – whether the EU or national institutions, or rather dedicated watchdogs for AI. Also, regulatory "forum shopping", whereby a non-EU actor could pick the national regulator of its own choice to gain access to the internal market, should be avoided.

A flexible and open EU-level governance structure, which delegate enforcement responsibilities to Member States, could be a pragmatic way forward. Such structures must be sufficiently funded and powerful enough for their monitoring and enforcement authority to be effective and consistent across borders.

**Policy contacts:**

Paolo Grassia, Director of Public Policy

grassia@etno.eu

Sara Ghazanfari, Regulation & Economics Manager

ghazanfari@etno.eu