Axel Voss
Member of the European Parliament

Response to the AI-White Paper

I. General remarks: comparable with the development of engines or the use of electricity, technologies based on Artificial Intelligence (AI) represent a revolutionary innovation that is already reshaping the world. While other regions have acted promptly to foster the development of AI, being fully aware of the historical opportunities, most EU Member States remained indifferent and barely cooperated among each other. Solely domestic, half-hearted initiatives and investments by the EU Member States, an industry that barely uses AI technologies, and a public discourse that too often concentrates on hypothetical threats paint a clear and unflattering picture of Europe's current level of ambition when it comes to AI.

While the European Commission's White Paper is a long-awaited wake-up call for a harmonised and more ambitious European AI strategy, and while it proposes several strategies that will indeed help to protect Europe's digital sovereignty, it unfortunately lacks the radical but necessary change of direction. It also fails to supply a thorough strategic analysis evaluating Europe's strengths and deficiencies and an in-depth assessment of the existing legislation that already covers AI technologies. Perhaps counterproductively, in several passages the White Paper focuses heavily on the potential risks of AI and thus, aligns itself with the pessimistic tone that has coloured much of the public discourse on this topic.

If the European Union does not wish the revolutionary innovation of our time to be shaped outside Europe, we need to act as one, move forward courageously and fully embrace the manifold chances that AI technologies offer humankind. We have a simple choice to make: either we develop AI ourselves based on EU values or we become an ordinary consumer of non-European AI-products, missing out on an expected 14% increase in the global GDP (equivalent to $15.7 Trillion). Based on a comprehensive preliminary analysis (much more advanced and detailed than the White Paper), we should therefore bravely progress with a combination of both, doing more and doing less: more investments in research, innovation and education - less red tape and overlapping legislation.

II. 'Ecosystem of excellence': the European Council's agreement on the EU Recovery Fund and the long-term budget would drastically reduce the funds for research, trainings and digital infrastructure. In particular, the cuts to the Digital Europe Programme and to Horizon Europe will hamper European innovation in AI. Although the proposals in the AI White paper to establish an 'ecosystem of excellence' are in general very welcome, they will be worthless if they are not backed up with massive investments. At least 20% of the European and national budgets should be reserved for digital transformation, of which a significant part should go into AI.

- *Digital infrastructure*: to develop and deploy AI-technologies, Europe needs a top-class cyber-secure digital infrastructure as well as a higher quality and better access to data. This means that the new standard for cellular networks has to be implemented more rapidly and broadly based on the 5G toolbox as well as a binding timetable. Furthermore, industry driven guidelines and best practices should be promoted to raise Europe's cybersecurity awareness and abilities. Finally, greater voluntary data sharing and access should be incentivised while creating AI data centres and an open and transparent European cloud infrastructure (e.g. Gaia-X) based on the principles of portability, interoperability and encryption.

- *Digital networks*: Europe has excellent AI-research but lacks coordination and knowledge transfer to the business sector required to fully exploit its potential. New lighthouse projects across the EU that are based on existing structures of excellence (e.g. CLAIRE, ELLIS), a fully working European cloud network, the further strengthening of public-private partnerships (including the new AI & Robotics PPP) and a focus on sectors, where Europe has the potential to become a global champion seem to be good steps forward. Digital hubs and AI testing sites (both financed by InvestEU and the Digital Europe Program) could also help to better coordinate between schools, researchers, start-ups and larger companies and improve the access to finance, expertise and talent among them.

- *Digital skills*: developing, operating or offering trainings to other persons in AI-technologies requires certain digital skills. The newly updated Digital Education Plan as well as the new Skills Agenda seem well equipped to promote STEM-education and to provide employees with digital training programs. Better cooperation between the education sector and businesses can also help to improve public knowledge in AI. The EU should also boost the role of flexible upskilling and reskilling programmes in training and education funding initiatives. AI competences and qualifications should be easily identified, validated and recognized.

- *Common standards*: better coordination with and between European businesses is necessary to develop market-relevant technical standards that promote interoperability and technological transfer while enabling competitive levers. European standardisation organisations should act as first-movers and identify gaps in international standards, having in mind that AI-technologies are not developed and deployed in regional silos.

- *Top tier talent*: whilst some European companies have impressive AI research teams, the most prolific researchers are working in the US and China. Together with the business sector, the EU as well as the Member States should establish an environment that convince those talent to stay here or to come to Europe (e.g. stock option schemes; tax breaks to businesses for doing research; EU-Visa scheme; reliable 5G internet connections; better access to computer capacities and datasets).

- *Market conditions*: Better protect European AI start-ups and AI knowledge from being sold off by foreign state funds or foreign state-supported cooperation. Therefore, create the right conditions for more European cooperation to enable our AI-companies and joint ventures to reach the necessary scale and compete worldwide while staying in Europe.

III. 'Ecosystem of trust': even though existing legislation already covers today’s AI-technologies, many Member States are working on new AI regulations. A principle- and risk-based as well as future-oriented AI framework at the EU level combined with sector-specific rules therefore seems necessary to avoid a fragmented Digital Single Market, something that would be highly hostile to digital innovation. However, the White Paper does not follow the Better Regulation principle to regulate only where necessary. The White Paper also concentrates too much on the potential risks of AI technologies and thereby ignores the lessons learned from the EU’s experience with the GDPR. As happened before with the privacy paradox, a minor time advantage or a slightly cheaper price could convince European consumers and businesses again to choose non-European AI products that clash with our principles and values. Overall, the new framework needs to strike a much better balance between privacy, security and innovation if the EU wants to become a global leader in AI.

- *Legal certainty*: the biggest flaw of the White Paper is the missing analysis of the existing horizontal and sector-specific legislation at the European and national level. Excessive regulation or overlapping with other rules (e.g. GDPR, PLD, GPSD, anti-discrimination directives, medical device regulation, payment services directive) should be avoided. The new AI regulation(s) should be narrow lex specialis, accompanied by regulatory sandboxes and innovation incentives. Anyone, regardless of whether they are developing the technology or operating it, must always have a clear understanding of which rules are applicable to the AI technology at hand. Strong property rights can further help encourage innovation and create more legal certainty.

- *AI-definition:* emphasizing the human origin behind any AI system, the definition of AI should be very precise and differentiate between the various AI technologies. The new framework should only cover systems that learn from data and experience, including machine- and deep-learning, as the traditional software and central systems that function according to predictable rules are already covered by law. Such a definition should also aim to be aligned with international concepts and terminology, for instance with the ones developed by the OECD and international standardisation bodies like ISO.

- *Risk-based approach*: the new provisions should only regulate high-risk AI systems while giving businesses the flexibility to choose measures that deliver the best outcomes for low-risk technologies. The classification of 'high-risk' should be based on the concrete use and the context, the complexity and autonomy of the AI-system, the probability and likelihood of the worst-case scenario and the severity of the harm as well as its irreversibility. Since applications, products and services in one AI-sector have very different risk levels, sectors should be taken into account but should not be a defining criteria for determining high-risk technologies. The classification should however take into account that AI-technologies reduce the risks during an operation significantly as they exclude the human error. Eventually, the framework should not include clauses for 'exceptionally instances' as this would lead to legal uncertainty.

- *B2B exclusion*: the requirements that AI-systems should fulfil differ significantly in a B2B compared to a B2C environment. While for instance consumer rights need to be protected by special laws, companies can solve liability and other legal challenges more quickly and more cheaper by contractual means, directly with their business partners. In particular, SMEs and start-ups investing in AI-technologies could be supported with a B2B exclusion as they are disproportionately affected by new legal obligations, harming also their ability to attract investments.

- *Ethical standards*: based on the interdependence between the EU and other like-minded democratic countries as well as their shared values, the new AI framework should follow the OECD AI principles, adopted in May 2019. The new ethical standards should however not set stricter rules for AI activities than those already existing for human or automated actions. One should also have in mind that those principles reflect idealistic goals, and go far beyond concrete legal obligations for individuals or businesses. Therefore, transparent AI systems should be understandable (operator knows how AI broadly works and which personal data is being used) as well as interpretable (experts understand the rationality behind AI-decisions). In any given use case, it should always be clear whether AI technologies are being used, which functions are AI-enabled, if there is human oversight and who is responsible for the decision-making. It is crucial that the new principles should only be established if they are made necessary by specific characteristics of AI technologies, and only if they have not already been established in another context (e.g. anti-discrimination directives, GDPR).

- *Biases in AI systems*: the GDPR and the anti-discrimination legislation seem in principle sufficient to guarantee that AI-based decisions do not entail unintentional or hidden negative biases (e.g. refusal of loans or promotions based on gender- or country-biased discrimination). Currently, most biases in AI-systems are due to a lack of diverse training data (minorities not sufficiently covered in the data set) or due to the limited volume of training data (overly strict data protection provisions). Moreover, some biases are also intentionally created in order to improve the AI's learning performance for certain circumstances (e.g. detect a cancer type that often occurs in 50-year-old white men). Since completely unbiased data sets are either unwanted or impossible to create, the new provisions should instead focus more on testing the outcomes of AI systems before they are deployed.

- *Data protection*: there is no need for additional data protection rules given the existence of the GDPR and the law enforcement directive. However, since the distinction between personal and non-personal data is in reality often very difficult to achieve and since mixed datasets are crucial for many AI technologies, new exceptions within both laws should be considered. The legislative updates should also incorporate new approaches such as deep learning into the laws, as some of the current concepts (e.g. information obligations, informed consent or purpose limitation) are no longer applicable. Due to the importance of data for AI, the principle of data minimization should be replaced by the principle of data sovereignty. Last but not least, the problem of the fragmentation with different interpretations by national and regional Data Protection Authorities needs to be addressed urgently.

- *European data*: forcing European companies to retrain their AI systems with European data - as it was discussed in unpublished versions of the White Paper - would have been self-defeating, discriminatory and unrealistic. Instead of closing its door to global data sets, the EU should apply existing standards (e.g. ISO/IEC 25024 or 25012) and focus its activities on whether the operation of an AI system is compliant with EU law.

- *Face recognition and biometric data*: although the application of AI in this area is in many situations highly appropriate and beneficial for the general public (e.g. to search suspect databases and identify victims of human trafficking or child sexual exploitation and abuse), several ethical and legal questions raised by new technologic opportunities remain open and need to be addressed. Since the EU Charter and the GDPR already apply to these technologies, more testing, specified training and better oversight by competent public bodies should be employed to strike the right balance between risk and chances, public security and fundamental rights.

- *AI-enabled mass scale normative scoring of individuals:* whilst AI offers many advantages, any form of normative citizen scoring on a large scale by public authorities, in particular within the field of law enforcement and the judiciary, leads to the loss of autonomy and is not in line with European values.

- *European coordination*: build up an adequately resourced mechanism to supervise the uniform, EU-wide enforcement of the new AI framework. Instead of creating an expensive new EU-Agency for AI, the Commission and the national authorities should closely cooperate with each other, using a similar approach to the European Competition Network (ECN). This mechanism should also assist public authorities and businesses in assessing the effects of automated decision-making. In sectors like healthcare or finance, which already feature regulatory agencies, the new mechanism would only have a supportive and coordinating role.

- *Product safety:* forcing businesses to guarantee outcome reproducibility or to predict ex-ante the entire potential of an AI life cycle (especially with deep learning and AI's ability to learn from the end-user) is not feasible. Obligatory ex-ante risk self-assessments – comparable with CE markings or data protection impact assessments – combined with administrative surveillance based on clear standards and complemented with ex-post enforcement for high-risk AI systems, seem to be a more fitting approach. However, new safety assessments should only be mandatory when there is an important security-relevant change in the specification of the AI system. The obligation to keep the operational records from high-risk AI might be another useful measure but one would need to take the additional costs as well as security deficits (e.g. third party auditing, trade secrets, GDPR, Copyright, IPR, cybersecurity) into account. Voluntary labelling schemes for all low-risk AI-systems should only be introduced in specific areas and with a bottom-up-approach, where minimum criteria are identified by all actors participating in the same ecosystem in order to prevent dominant businesses from defining labels for all market players.

- *Product Liability Directive*: despite the legal challenges that are being caused by AI-systems, there is no need for a complete revision of the existing liability framework. The PLD can remain the centrepiece for all harm caused by defective products. Some changes to the definition of 'product' (including integrated software applications/digital services) and 'producer' (including backend operator/service provider/data supplier) are nevertheless required to ensure that compensation is available for harm caused by emerging technologies. However, an overly broad approach to the 'product' definition should be avoided, as this may make it difficult to differentiate between AI and less complex algorithms. The possibility of contractual liability clauses in B2B relations should be maintained.

- *Additional liability rules:* Since the frontend operator is not liable under the PLD but exercises significant control over the risk posed by the AI system, an additional liability regime seems necessary to guarantee that third parties without any contractual relations to the frontend operator receive adequate compensation for their harm caused by an AI system. While exceptional high-risk AI systems should fall under strict liability combined with mandatory insurance cover, victims of low-risk AI-systems should benefit from a presumption of fault against the frontend operator. Neither the PLD nor the new liability regime against the frontend operator should cover damages for non-pecuniary loss since our legal traditions only offer strict liability when actual and quantifiable material harm is suffered. The dual-use of AI technologies as well as the compensation mechanism of immaterial harm already offered by existing laws (e.g. GDPR, anti-discrimination directives or tort law) would also increase the legal uncertainty and make it hard for SMEs and start-ups to calculate.