Position Paper on the European Commission's White Paper on Artificial intelligence

The Confederation of Swedish Enterprise (Svenskt Näringsliv) represents 50 member organisations and 60,000 member companies with over 1.6 million employees. In cooperation with our members, we offer our comments on the approach and proposals in the White Paper on Artificial Intelligence (AI), focusing on the regulatory aspects.

Key messages

- The European Commission should concentrate its efforts on supporting research, innovation, skills and providing a robust digital infrastructure throughout Europe.
- AI needs a narrower definition, otherwise it risks facing over-regulation in a vast number of applications.
- The most efficient approach to designing better regulation is to review and map the AI-relevant frameworks. Existing regulations should be clarified through guidelines.
- As the technology continues to advance, self-regulation and sectorial codes of conduct offer considerable advantages over a legal intervention approach.
- Any new regulation on regulation should be principle-based and technology neutral; this will ensure it is futureproofed.
- The concept of 'high risk' must be defined narrowly to avoid legal uncertainty acting as a constraint on innovation and AI use. A clear approach to risk assessment should identify all high-risk cases without a requirement to list high-risk sectors or areas.
- Europe should not close its door to the use of non-European data to power its AI and produce the highest quality AI outcomes. The relevant issue for the society is that the operations and conclusions of the AI itself are legally compliant.

Ecosystem of excellence

The Commission has rightly identified the need to focus on investing in and deploying AI to help maximise its benefits. This is increasingly important given the need to stimulate a future economic recovery. The Commission should prioritise support for the research and innovation community and ensure that the required skills are in place to allow all to prosper from the benefits offered by AI-solutions.

Svenskt Näringsliv Confederation of Swedish Enterprise
Postadress/Address: SE-114 82 Stockholm Besök/Visitors: Storgatan 19 Telefon/Phone: +46 (0)8 553 430 00
www.svensktnaringsliv.se Org. Nr: 802000-1858

If Europe is to realise its full capacity in this field, it will need world-class, cyber-secure digital infrastructure to develop and run AI. It also requires a plan for harnessing 6G, in order to position Europe appropriately for the next wave of digital infrastructure.

Testing and verifying AI is part of the production phase. The industry needs to develop and provide their own testing facilities and references to place themselves at the forefront of innovation and competitiveness.

To support Europe's AI research community, confidential development, innovation and piloting of AI should be permitted in any future framework, free of market access requirements. This could be achieved using experimentation clauses and regulatory sandboxes at EU level.

Sectorial codes of conduct are particularly important in this rapidly evolving field. In our view, the most important mandatory requirement is the information on the purpose and the nature of AI systems.

A voluntary labelling system for AI could challenge the level playing field for businesses. A labelling system risks placing a significant burden on SMEs. This would favor large players who can afford to meet the requirements whilst delivering minimal benefit to consumers. Self-regulation and self-assessment are preferable for demonstrating adherence with the Ethical guidelines for Trustworthy AI and we will therefore welcome the release of a more advanced assessment list from the High Level Expert Group on AI (AI HLEG).

Europe should not close its door to the use of non-European data to power its AI and produce the highest-quality AI outcomes. The most pressing issue for society is that the operation and conclusions of the AI itself are legally compliant.

Europe's standardisation framework is vital in fostering excellence in AI. Market-relevant technical standards can support interoperability, technology transfer and create competitive levers to provide a lead in AI applications. An international approach is preferable; Europe should only set its own standards for public sector data and AI-applications when there has been no international initiative taken.

Ecosystem of trust

For many sectors, AI technology is an important tool and asset. Traders, for example, have been using this technology for a number of years to improve their competitiveness, accessibility and to provide a better customer experience. For example, AI has enhanced customer service by creating more-precisely tailored offerings to customers, has helped identify fraud, enabled more secure payments and increased sustainability by improving logistics and less waste of fabrics.

Companies must earn public trust by using data and new technologies responsibly. Citizens and the environment are protected through laws for product safety (GPSD), product liability (PLD), data protection (GDPR) as well as consumer laws. In addition, the public need to be able to understand how and what these new

technologies are creating. Of the all the demands placed on ethical AI, transparency is probably the most important in building and maintaining trust. Many organisations and companies have already established their own ethical codes in this area. In Europe, Ethical guidelines for trustworthy AI have been developed. In Sweden, IT and telecoms companies have published an industry code for delivering responsible AI that will contribute to a humane society, builds trust in the technology and delivers sustainability.

Regulating AI

The Commission notes that the existing EU legislation remains in principal fully applicable, irrespective of the involvement of AI, but it stresses the need to assess whether AI risks are adequately addressed. The Commission believes that the legislative framework has room for improvement.

The most efficient approach to better regulation would be to review and map AI-relevant frameworks, rather than creating a specific new AI regulation. The most useful way of clarifying existing regulations would be to rely on guidelines.

AI applications encompass so many areas that the technology itself has proved challenging to define. Given the strong political will behind making Europe more digitised and more competitive by deploying AI solutions and applications, it is important to segment its use according to specific contexts and specific service users. Clearly, there are considerable differences between, for example, those applications for streamlining production methods, those for simplifying administration and those for customising treatments or training. A horizontal approach that addresses all industries will not strengthen competitiveness; on the contrary, it will create fresh regulatory burdens, with all that it entails in terms of uncertainty, time and costs.

Currently, the General Product Safety Directive, GPSD, applies only to products, not services. Differentiating between the two can be difficult in certain cases. The GDPR, for example, does not distinguish between personal data processed in a service from that processed in a product.

The legislation should not differ between AI and non-AI-based products. All and any product that impact safety should be covered, regardless of the technology deployed.

There is a need to regulate liability for third party suppliers that upgrade or change any product or service after it has been placed on the market by the producer. Currently, this is undertaken at national level.

AI would not actually change anything concerning the GDPR, it is a system that processes personal data, like any other system. But the proposed mandatory requirements for high-risk AI applications could create conflict with GDPR, for example when it comes to keeping datasets (the principle of data minimisation) and ensuring that datasets are sufficiently representative (use of sensitive personal data).

There is already consumer legislation in place, and for B2B there should still be freedom of contract.

Legislation should aim to regulate the outcome and effects from a service or product (i.e. product safety or product liability) and should strive to be principle-based and technology neutral, as stated in Article 22 of the GDPR; “automated individual decision-making, including profiling”. Otherwise, there is a substantial risk that it will render regulations obsolete.

As technology continues to advance, self-regulation offers considerable advantages over legal interventions.

Definition of AI

AI is currently embedded into a huge variety of technical products and solutions, yet it remains difficult to define legally. A widely understood and accepted definition of AI will be vital for ensuring the effectiveness of any future regulatory framework.

The White Paper describes the main elements of AI as algorithms and data. Such a broad framing effectively puts all contemporary software within its scope. Clearly, a narrower definition, focused on the subcategory of AI systems, is needed to help avoid subsequent over-regulation.

Levels of risk

The Commission’s White Paper on AI proposes different rules depending on the sectors and the types of risk associated with AI use. By focusing on precision regulation - applying different rules for different levels of risk - Europe can ensure its businesses and consumers can trust in technology.

A clear approach to risk assessment should identify all high-risk cases without the need to list high-risk sectors or areas.

Definition of high-risk

The Confederation of Swedish Enterprise is concerned with the proposal that the use of AI for certain purposes would always be considered as high-risk, these include AI applications for recruitment processes, in situations impacting workers’ rights and for remote biometric identification purposes.

The use of AI technology in employment scenarios could raise concerns over bias, control or monitoring. However, AI solutions also offer significant benefits to employees, including minimising the effect of human bias, providing customised insights into potential jobs or careers or personalised training. It is paramount to identify the specific risk foreseen from AI use in a specific context, rather than preventing the employment area from potentially benefiting from AI.

It is important that definition of high risk is narrow, in order not to hinder innovation and the uptake of AI. A clear approach to risk assessment should identify all high-risk cases without the requirement to list high-risk sectors or purposes.

One suggestion for identifying high-risk AI would be to focus on those rational learning AI systems (also known as self-learning systems) with a potentially disproportionate impact on humans and/or the environment. Currently, most AI systems are rational AI systems[1], trained during development and then deployed in non-learning mode. High risk AI should be restricted to learning AI systems, as these currently fall outside the scope of existing regulations such as the product safety or product liability Directives. As long as the AI in question is a rational system, it should drop out of the high-risk definition and the scope of any new compulsory requirements. It is normal to assess this kind of AI in the same way as any other component in the product, and the producer must take responsibility for the whole product.

It has been proposed in the AI White Paper that high-risk AI applications should be tested by an independent body. However, the impact of any compulsory testing must be evaluated on the better regulation principle, not least because of the time, costs and competence implications.

The traditional theory of risk should be applied; the triplet of 'potential threat – probability – effect of outcome if the threat is actuated'. This has already been done for highly complex systems where - although not AI based -no one can clearly foresee all and any problems with, such as complex software for diagnosis or running medical equipment. Furthermore, this is the approach taken for certifying human operators in potentially dangerous situations in manufacturing plants, such as doctors or as drivers.

Safety and liability frameworks

Safety and liability frameworks must provide users of AI applications with adequate protection; thus, where significant shortcomings are identified, they must be addressed. However, the White Paper appears to conflate the concept of health and safety with notions that fall outside the normal scope of product safety (for example cybersecurity, ethics, privacy and mental health). Any review of the GPSD should focus exclusively on those areas where the unique properties of new technologies create a potential threat to the health and safety of consumers. To as great an extent as possible, this should be undertaken at the level of special safety regulation (e.g. Regulation (EU) 2019/2144 on type-approval requirements for motor vehicles).

The current PLD remains fit for purpose, being both effective and technology neutral. It provides both legal certainty and compensation for consumers; original equipment manufacturers (OEMs) are held liable for a defective AI-based product and can later call upon their supplier.

[1] High level expert group on AI, Definition of AI, 2019: Rational AI systems are a very basic version of AI systems. They modify the environment, but they do not adapt their behavior over time to better achieve their goal. A learning rational system is a rational system that, after taking an action, evaluates the new state of the environment (through perception) to determine how successful its action was, and then adapts its reasoning rules and decision-making methods.

It has been proposed that there should already be liability during the production of AI, i.e. before it reaches the market. In order to avoid liability, AI must comply with ethical rules, be robust and in accordance with laws and regulations. Here, we believe that it would be most appropriate for product liability to apply from the point when the item is placed on the market, not before. There should be a liability on the business that places the product on the market, regardless of whether it contains or relies on AI. Thus, if a domestic services company sends a robot or a human to clean a customer's house and something goes wrong, the company is equally responsible for both the cleaner and the robot; there shouldn't be any difference. Overburdening AI system developers with such legal exposure would significantly constrain innovation and competition and is likely to place a disproportionate burden on Europe’s SMEs.

At the same time, a third party that upgrades or make important changes to a product by introducing new AI or software in the device or service after it has been placed on the market needs to have strict liability for the product or service they amend.

Regarding legal liability, we cannot see any reason why the current regulations on product liability, indemnity liability, consumer liability, copyright liability etc. would have to change fundamentally to accommodate AI. The principles applying to these legal areas have been effective in a wide range of technologies for a long time; however, it is important investigate whether different types of liability rules, as well as rules on ownership/use, need to be adapted for AI.

The White Paper suggests considering the entire lifecycle of AI, and that each actor should be responsible for their respective area. Developers would then be responsible during the development phase, and distributors and users for risks during the use phase. Here, it’s important to aim at better regulation with correspondence between different frameworks. According to the PSD, the producer is responsible for defective products.

A good example is vehicle manufacturers. They are, and will continue to be, responsible for the safety of the vehicle even when certain AI is included in the vehicle's software or has been used to develop it. Therefore, under no circumstances may other operators be allowed to install software in vehicles, unless the original manufacturer is no longer considered liable. It is not reasonable that a third-party should be able to operate aspects of the vehicle (for example the brakes, steering, acceleration, signals) or call for the driver's attention. For vehicles in particular, the system relying on third-party approvals and manufacturers’ product liability has already proved effective. The argument is that it is important to retain the perspective of reasonable precautions based on known fact. If no adverse effects have been detected during a full set of tests, acknowledged both by authorities and in practice, the supplier of such a system can be deemed to have taken reasonable precautions.

AI trained on non-European or on EU data

In terms of machine data - but also anonymised (personal) data - in a variety of applications, it is probably irrelevant whether the data originated in the EU or

elsewhere. Global players need to deal with the demands of a global market, both in terms of development and products. Therefore, if a company wants to operate globally, training data must be collected globally. This is essential if European industry is to maintain its position as world leaders. It would act as a constraint to limit the data on which AI can be trained. Companies buy components and AI from distributors in the US and elsewhere. At the forefront of technology, there are often only few AI producers to choose from.

When discussing non-biased EU data, one should remember that some bias could be commercially correct. Who determines which data and AI is biased and which AI or data used is biased intentionally to support different kind of customers? European data controlled by the authorities would be way too time-consuming to support businesses. Timing is an important consideration; trained datasets are valuable and time efficient to buy.

EU companies are subject to European law in all their operations. Hence, they will comply with, for example, the GDPR globally. This leads to a basic consistency in the collection, usage and impact of data. However, at the same time differences in the environment - including those within the EU - produce different results. The manufacturer's development processes must take account of the relevant cases the product may meet, just as is the case today. This makes it essential to be able to use global data.

To foster greater trust, it is crucial that AI in Europe is trained in accordance with quality standards and that the outcomes of the AI are legally compliant. However, we do not believe in restricting access to non-European training data. On the contrary, it is essential to help ensure that data can be transferred between countries around the world.

If we do not dare or may not use it, then the value of the data will be lost. It doesn’t benefit Europe or competitiveness to build protectionist walls.

***