SVENSKT NÄRINGSLIV

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

The Confederation of Swedish Enterprise (Svenskt Näringsliv) is representing 50 member-organisations and 60 000 member companies with over 1.6 million employees. In cooperation with members we have commented on the approach and proposals in the White Paper on Artificial Intelligence, AI, focusing on how to regulate AI.

Key messages

- The Commission should center its efforts on supporting research, innovation and robust digital infrastructure all over Europe
- A narrower AI-definition is needed to avoid over-regulation applied to a vast number of applications.
- To get better regulations, the most efficient approach would be to review and mapping the AI relevant frameworks. Clarifications to existing regulations should be done by guidelines.
- As technology continues to advance, there is a considerable advantage of self-regulation and sectorial codes of conduct over legal interventions
- Any new regulation on new technology should be principle-based and technology-neutral and thus futureproof.
- The definition of high risk must be narrow in order not to hamper innovation and the use of AI by legal uncertainty. A clear approach to risk assessment should identify all high-risk cases without the need to list high-risk sectors or areas.
- To foster greater trust, the operation and conclusions of the AI must be legally compliant. Europe should not close its door to the use of non-European data to power its AI and produce the highest quality AI outcomes.

Ecosystem of excellence

The Commission has rightly identified a need to focus on investment in and deployment of AI to ensure its benefits continue to grow, in particular in the context of the future economic recovery. The Commission should priorities its efforts on supporting the research and innovation community and ensuring the right skills are in place, so all are able to prosper from the AI benefits.

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

Europe needs top-class cyber-secure digital infrastructure to develop and run AI upon in order to foster our full capacities in this area, as well as a plan for harnessing 6G, to ensure Europe is better prepared for the next wave of digital infrastructure.

To test and verify AI is part of the production phase. But establishing testing facilities for AI could slow down AI-uptake and use in both public and private sector. The industry and sectors need to provide and develop testing facilities and references themselves to be at the forefront of innovation and competitiveness.

Permitting confidential testing and piloting of AI in the development stage, free of market access requirements, should be permitted in any future framework to support Europe's AI research community. This could be done by experimentation clauses and regulatory sandboxes at EU-level.

The use of sectorial codes of conduct are very important in this fast-moving field of tech. The most important mandatory requirement is in our view the information on the purpose and the nature of AI systems.

When it comes to voluntary labelling system it could be counterproductive challenging 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 to show adherence with Ethical guidelines for Trustworthy AI and we therefore do welcome a more advanced assessment list from the AI High level expert group, AI HLEG, to be released.

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 highly relevant issue for the society is that the operation and conclusions of the AI itself are legally compliant.

Europe's standardisation framework has a crucial role to play in fostering excellence in AI. Market-relevant technical standards can support interoperability, technology transfer and enable competitive levers to lead in AI applications. An international approach is favorable. Europe should only set its own standards when it comes to public sector data or when no international initiative has been taken.

Ecosystem of trust

For many industries and companies, the AI technology is a very important tool and asset. Traders, for example, have been using the technology for several years to improve their competitiveness, accessibility and customer experience. To mention a few examples, AI has been a contributing factor to improved customer service, more precise offerings to customers, identify fraud, enable more secure payments and perhaps most importantly, contribute to an increased sustainability in society.

Companies must earn trust by using data and new technologies responsibly. Through laws in areas such as product safety (GPSD), product liability (PLD), data protection (GDPR) and consumer laws the citizens and the environment are protected. In addition, people need to be able to understand how and what the new technology and

new systems can create. Of the demands placed on ethical AI, transparency is probably the most important to build and maintain trust. However, technological advances have now reached a level where it is increasingly difficult for many of us to understand the latest developments; at the same time, it is challenging for authorities to monitor and supervise. It is important with a risk-based and proportionate approach, which balancing potential harms with the social and economic benefits that will be created by AI.

Many organisations and companies have already established their own ethical codes. In Europe, ethical guidelines for trustworthy AI have been developed. In Sweden, IT and telecom companies have published an industry code to deliver responsible AI that contributes to a humane society, builds trust in the technology and delivers sustainability.

Regulating AI

In the name of better regulation, the most efficient approach would be to review and mapping the AI relevant frameworks, rather than creating a new AI-regulation. The most relevant thing for clarifications to existing regulations would be the use of guidelines.

AI applications encompass so many aspects that AI itself has been proved difficult to define. Because of the strong political will to make Europe more digitized and more competitive through the deployment of AI solutions and applications, it is important to divide its use according to different contexts and different users of services. There are considerable differences between applications for streamlining production methods and those for administration, or for customising treatments or training. Creating a horizontal approach that addresses all industries will not strengthen competitiveness; rather, it will create new regulatory burdens, with all that it entails in terms of uncertainty, time and costs.

The Commission notes that the existing EU legislation is fully applicable irrespective of the involvement of AI but stress the need to assess whether AI risks are adequately addressed. The Commission is of the opinion the legislative framework could be improved.

Today the General Product Safety Directive, GPSD, implies to products but not services. The difference between a service and a product can be very hard to tell in some cases but in general the legislation should not differ between AI and non-AI-based services. All and any services that impact safety should be covered regardless of the technology of choice. The GDPR, for example, do not distinguish personal data processed in a service from personal data processed in a product.

There is a need to regulate liability for third party suppliers that upgrade or change the product or service after its been placed on the market by the producer. Today this is done at national level.

Regarding the GDPR, AI would actually not change anything, it’s a system that process personal data like other systems. The potential issue lies with training and

evidence that the system is safe. Finding a suitable legal basis for such processing, data minimization and removal of data as well as informing individuals could be challenging.

The proposed mandatory requirements for high-risk AI applications could be in conflict with GDPR, for example when it comes to keeping of datasets and ensure datasets are sufficiently representative.

There is already consumer law 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 strive to be principle based and tech neutral as in GDPR, art 22, "automated individual decision-making, including profiling". Otherwise there is a huge risk ending up with obsolete regulations.

If regulating both the development and outcomes of AI systems, it is important to remain impartial towards the technology itself, and instead focus on principle-based rules that themselves are technology-neutral and thus futureproof. In addition, as technology continues to advance, there is a considerable advantage of self-regulation over legal interventions.

Definition of AI

AI is currently embedded into a huge variety of technical products and solutions and even from this point of view, AI is considered to be difficult to legally define. A clearly understood definition of AI will be critical to the effectiveness of any future regulatory framework. One of the existing definitions published in EU would be the AI HLEG definition from 2019.

In the White Paper, the main elements that compose AI are described as algorithms and data. Such a broad framing effectively puts all contemporary software in scope; a narrower definition is needed to focus on the subcategory of AI systems where issues could arise and to avoid over-regulation.

Levels of risk

The Commission's White Paper on AI proposes different rules depending on the sector 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 have 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 very concerned with the proposal that the use of AI for certain purposes would always be considered as high-risk such as AI applications for recruitment processes, AI-use in situations impacting workers' rights and the use of AI for the purposes of remote biometric identification.

The use of AI technology in the employment environment could raise concerns about bias, control or monitoring. However, AI solutions also offer significant benefits to employees, including reducing the effect of human biases, providing customised insights about potential jobs or careers, or personalised training. It is paramount to identify the specific risk foreseen from the use of AI in a particular context rather than risking the exclusion of the employment area from the potential benefits of AI.

The definition of high risk must be narrow in order not to hamper innovation and the use of AI. A clear approach to risk assessment should identify all high-risk cases without the need to list high-risk sectors or areas.

One suggestion for identifying high-risk AI would be to focus on learning rational AI systems (self-learning systems), with possible disproportionate impact on humans and/or the environment. Today most AI systems are rational AI systems[1], trained during development and then deployed in a non-learning mode. High risk AI should be limited to learning AI systems since those systems fall outside the scope of existing regulations like the product safety or product liability directives. As long as the AI is a rational AI system it should fall out of the high-risk definition and the scope of new compulsory requirements.
It is natural to assess this kind of the AI as any component in the product and the producer must take responsibility for the whole product.

It's proposed in the AI White Paper that high-risk AI should be tested by an independent body. The impact of compulsory testing must be evaluated on the better regulation-principle, not least because of the time, costs and competence aspects.

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 extremely complex systems that, although not AI based (it is reasonable to say), no one for sure can foresee all and any problems with, such as complex software for diagnosis or running of medical equipment. It is furthermore the approach taken for certifying human operators in potentially dangerous situations in manufacturing plants, as doctors or as drivers.

[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.

Safety and liability frameworks

Safety and liability frameworks must provide users of AI applications with sufficient protection, so if significant shortcomings are identified they must be addressed. However, the White Paper appears to conflate the notion of health and safety with concepts which fall outside the scope of product safety (e.g., cyber security, ethics, privacy and mental health). Any review of the GPSD should focus exclusively on areas where the unique properties of new technologies create a risk to the health and safety of consumers. To the largest extent possible this should be done 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. The PLD provides both legal certainty and compensation to consumers: Original Equipment Manufacturers (OEMs) are held liable because of a defective AI-based product and can later call upon their supplier.

It is proposed that there should be liability already during production of AI, i.e. before it is implemented on the market. In order to evade liability, AI must comply with ethical rules, be robust and in accordance with laws and regulations. Here we do believe that it would be most relevant that product liability applies when the product is placed on the market, but not before then. There should be a liability of the business that puts the product on the market regardless of whether it contains/is an AI or not. If a cleaning company sends a robot or a human for cleaning at 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. Burdening AI system developers with such legal exposure would significant hamper innovation and competition, and most likely disproportionately fall on European SMEs.

A third party that upgrade or make important changes of a product by introducing a new AI or software in the device or service after it has been placed on the market need to have strict liability of the product or service they change. The current PLD is solid and tech-neutral and should be kept that way.

Regarding legal liability for AI, we cannot see that the current regulations on product liability, indemnity liability, consumer liability, copyright liability etc. would need to be changed fundamentally due to AI. The principles of these legal areas have worked for many different technologies for a long time, but it is of course important investigate whether different types of liability rules and rules on ownership/use need to be adapted to AI.

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

An example is vehicle manufacturers who 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 used to develop it. Therefore, under no circumstances may other operators be allowed to install software (neither AI nor handwritten) in vehicles unless the vehicle manufacturer is no longer considered liable. It’s not reasonable that a third-party should be able to control the vehicle (ex. take control of its braking, steering, acceleration, signals, calling for the driver's attention). Especially for vehicles, the system using third-party approvals and manufacturer's product liability have worked well. The standpoint is that it is very important to keep the aspect of reasonable precautions based on known facts. If no adverse effects have been detected during a full set of tests, acknowledged both by authorities and de facto praxis, the supplier of such a system has taken reasonable precautions.

AI trained on non-European or on EU data

In terms of machine data, but also anonymized (personal) data in a variety of applications, it probably does not matter and is not obvious if the data was originally from the EU or elsewhere. Global players need to act on the global market, both in terms of development and products. If a company wants to operate globally, training data must be collected globally. This is very important if European industry is to continue being world leading. It would be inhibitory to limit the data on which AI can be trained. Companies buy components and AI from distributors in the US and elsewhere. At the technological forefront there is often only a few options of AI producers.

When discussing non-biased EU data, one should remember that some bias is commercially correct. Who determines which data and AI is bias and which AI or data used is bias intentionally to support different kind of customers? It's not gaining Europe or competitiveness to build protectionist walls. The time aspect is also very important – trained datasets are valuable and time efficient to buy. European data controlled by the authorities would be way too time-consuming to support businesses.

The EU companies are subject to European law in all their operations, regardless of which continent that performs them. Hence, they will and have to comply with e.g. the GDPR globally. This leads to a basic coherence in the collection, usage and impact of data. But at the same time differences in the environment, including those within the EU, produce different results. The manufacturer's development processes must take care of relevant cases the product meet, just as it is today. Therefore, we need to be able to use global data. This also has a bearing on the costs.

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 limiting access to non-European training data. On the contrary it is very important to facilitate that data can be transferred between countries around the world.

The value of the data will get lost if we do not dare or may not use it.