Svenska
Bankföreningen
Swedish Bankers' Association

12 June 2020

The Swedish Bankers' Association response to the European Commission's AI White Paper

Key positions

- The Swedish Bankers' Association welcomes the European Commission's White Paper on "Artificial Intelligence - A European Approach to Excellence and Trust" and appreciates the opportunity to contribute. This paper complements our response to the European Commission survey on the AI White Paper.

- The suggested risk-based approach is a sound principle but needs to enhance a degree of flexibility. An approach centered on prescriptive, wider regulation could hamper the adoption of this enabling technology and harm Europe's competitiveness globally.

- The human-in-the-loop approach should always be ensured, so that the results of a system can always be overruled by a human. There should always be a clear responsibility for the implementation of an AI system.

- We welcome the White Paper's focus on applications rather than on the technology itself and would recommend the adoption of a technology neutral principle. Legal requirements should not apply to the underlying technology but to the use to which it is put.

- Although anonymization of data in general is good it can also limit the use of AI-technology. In cases such as Know Your Customer (KYC) or financial crime prevention where the AI system must be able to learn from meaningful data and determination of false positives in order to accurately detecting true anomalies, applying anonymisation to the training data could decrease the accuracy of the application.

Section 1 - An Ecosystem of Excellence

We welcome the initiative and proactivity shown by the European Commission with its work on a common European AI-strategy and we appreciate the opportunity to contribute. AI has the potential to contribute with significant benefits in a variety of areas through increased economic growth, and solutions to environmental and social challenges. Artificial intelligence is developing rapidly and by international standards, Sweden is in the vanguard. Banks in Sweden contribute decidedly to this leading role.

The first wave of using AI technologies is already happening in the banks: rule-based AIs boost productivity in internal processes in areas such as compliance. The second wave of AI is now being rolled out: chat bots in customer service, dealing with routine customer queries and integrated sophisticated machine learning techniques are growing in significance within its general operations such as risk-assessments and most importantly, detecting financial crime and fraud targeted at customers.

We support the view that further cross collaboration between SMEs, larger corporates and public sector can be very beneficial as many of the needs are common – such as education, climate and reskilling of the workforce, improving movements between academia, public and private sector.

Creating a clearer data regulation would facilitate the sharing of important data sets between the private and the public sector. The current legislative landscape makes sharing of data cumbersome. Some guidelines around data sharing would enable larger collaborations between these important players in the acceleration of AI application and research. However, regulation needs to be both narrow to avoid overregulation and based on current legislation (these perspectives are developed in section 2 and 3).

Although a shared European strategy and a level playing field for AI will be good for competition and growth, we question the statement on page 2 where it says: "A common European approach to AI is necessary to reach sufficient scale and avoid the fragmentation of the single market. The introduction of national initiatives risks endangering legal certainty, to weaken citizens' trust and to prevent the emergence of a dynamic European industry." This statement needs clarification whether this regards solely legal initiatives or if it also includes national initiatives in general. We question whether national initiatives aimed at supporting the development of AI poses a threat to citizens' trust or the emergence of a dynamic AI industry in Europe.

Developing the skills necessary to work in AI and upskilling the workforce to become fit for the AI-led transformation is of course pivotal, however we do not believe that the EU of today has the resources and the mandate sufficient with the ambition of large educational ambitions as presented in the White Paper.

Section 2 - Regulatory Framework for AI

We share the view that as with any new technology, the use of AI brings both opportunities and risks. Consequently, the suggested risk-based approach is a sound principle but needs to enhance a degree of flexibility. An approach centered on prescriptive, wider regulation could hamper the adoption of this enabling technology and harm Europe's competitiveness globally.

The human-in-the-loop approach should always be ensured, so that the results of a system can always be overruled by a human. There should always be a clear responsibility for the implementation of an AI system. Even with lower risk applications there may be a need to add extra governance and compliance checks to ensure that the system does not have unintended negative societal impacts, such as restricting the integrity of citizens. However, as the AI landscape continues to evolve, the way in which aspects of human oversight is integrated into AI systems will change. As such we caution against crystalizing an exhaustive list of human oversight examples into any legislative instrument.

The current legislation for finance covers many of the potential risks with AI systems, since they are not physical systems but rather virtual. Banks already monitor and assess systems with high to medium business impact, to ensure that any system that is deployed is monitored, validated and re-evaluated on an appropriate recurring basis (from continuous to yearly reviews).

Sectors that are deemed critical from a societal viewpoint should be included – not just health, transport and energy. For instance: curated news using AI can have a very large impact on the public, and the AI systems that are deployed should be investigated for bias and skewness in the algorithm set up. Risks for bot infiltration in the curation of AI should be highlighted and monitored by news providers such as social media and news software.

Section 3 - Safety and Liability Aspects of AI

Technology itself does not commit a crime – humans do. This principle must be maintained both in terms of a human-in-the-loop approach but also in the way AI is being regulated. We welcome the White Paper's focus on applications rather than on the technology itself and would recommend the adoption of a technology neutral principle. Legal requirements should not apply to the underlying technology but to the use to which it is put. As a result, we warn against including a definition of AI in any possible future legislation. As it is a rapidly evolving field, any definition of AI cannot be future proof and would be in contradiction with the technology neutral principle. In the current version of the White Paper the proposed definition of AI is too broad and vague to be useful for legislative purposes.

New AI specific legislation is consequently not required, and we believe it is key to consider the consequences that any rules could have for the competitiveness of European companies. Guidance on AI issues produced collaboratively by competent authorities for different sectors could help firms apply their obligations under different regulatory regimes effectively to AI use cases, while being more agile and flexible to the variety, and to the rapidly evolving nature of AI-related technologies.

Further to this, a strict ex-ante oversight could delay the launch of services leveraging AI to the market. Therefore, the White Papers' suggestion to not create a new Agency is a positive step. The White Paper's proposal to create a new governance structure in the form of a framework for cooperation of national competent authorities still risks fragmentation of supervisory and or regulatory practices. We therefore recommend that one of the explicit purposes of the network of regulatory authorities should be to encourage information sharing and cooperation on AI issues by different sectoral authorities. This would be for the purposes of avoiding a situation where standards for similar activities are regulated more rigorously in some sectors than others, resulting in ‘regulatory arbitrage’.

Banks are a good example of how such a practice already works. As banks constantly deal with risks, under strict rules, they need to be able to measure, monitor and manage their sources of risk, which includes management of non-financial risk. IT security risk management is a part of this and encompasses product approval processes that ensure risk management on services is performed, controlled, and monitored via the “three lines of defence model” (business, risk/compliance, internal audit). This model sets a high standard in effective risk management and control, and these principles apply irrespective of the techniques used and therefore encompass AI as well. Managing all sources of risk also includes operational risk management to quantitatively indicate the risk impact of different events.

As a result, applications incorporating AI, as any other applications in the banking sector, need to be developed (and continue to be assessed and monitored) based on existing sectoral regulation, managing the necessary financial and non-financial risks as well as requirements under horizontal regulation such as the GDPR.

The GDPR and Law Enforcement Directive already provide strong privacy and data protection regulation, which should not be duplicated. The GDPR is a principle-based, technology neutral regulation that relies on a risk-based approach.

Further progress within the field of AI is however being held back by existing GDPR principles (e.g. data minimisation, storage limitation and purpose limitation) and obligations regarding AI development. This is already flagged by the European Commission’s *Expert Group on Regulatory Obstacles to Financial Innovation* in its Final Report[1]. The report notes that “*currently, firms may be held back due to uncertainties about how to comply with data protection rules when using AI and certain other technologies*” and gives examples on how the interpretation of for example the data minimisation principle can pose questions when it comes to experimentation[2].

It is also important to remember that although anonymization of data in general is good, it can also limit the use of AI-technology. In cases such as Know Your Customer (KYC) or fraud detection and more generally financial crime prevention, where the AI system must be able to learn from meaningful data and determination of false-positives in order to accurately detecting true anomalies, applying anonymisation to the training data could decrease the accuracy of the application.

[1] Final report of the Expert Group on Regulatory Obstacles to Financial Innovation https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf

[2] Ibid.