Competitiveness and stability impacts of technology

The Chair outlined the main themes of discussion of the panel: the impact of artificial intelligence (AI) and the on-going digital transformation on the competitiveness of the EU financial sector, the impacts of digitalisation in terms of resilience and financial stability and whether the EU regulatory and supervisory framework is helping to foster greater competitiveness and increased resilience in the financial sector with the increasing use of technology.

1. The impact of new technologies on competitiveness

1.1 Competitiveness impacts of AI

An official stated that digitalisation and the integration of new technologies such as AI represent a transformative opportunity to reshape the economic landscape. For example, AI will extend the connections between human and technological resources, enhance customer experiences and speed up assessment processes. AI will help automate processes and operations in the financial sector. It will improve data processing, which will enable firms to understand data more deeply and to more efficiently use the knowledge derived from the data. It could also help combat financial crime such as fraud more effectively.

An industry speaker emphasised that technology offers the possibility to rethink how traditional businesses work and how markets could be transformed. AI will be critical to all sectors because it drives competitiveness by helping businesses reduce costs and improve products and customer service. In the financial sector, AI is already being used in several different ways. It is used to improve financial firms' understanding of customers, which helps firms to offer their customers products and services that are more suited to their needs. AI is also used for customer retention, as it can help to identify customer dissatisfaction. AI can also support the management of customer interaction and speed up communication with customers. In this regard, chatbots can be extremely useful.

There have also been evolutions since the pandemic. There is a new generation of customers who prefer to interact with banks and financial services firms through online services. This is facilitated by apps that are easier to use, more user friendly and continuously upgraded to improve customer service. AI can also improve risk management, which is extremely important for banks' performance as the complexity of their operations increases. For example, AI can be used to identify trends such as the deterioration of a customer's credit status. This allows banks to take the best course of action to manage potential credit default risk. Finally, AI might also have a positive effect on financial inclusion. More efficient AI driven risk assessment and management might make it possible to extend credit to customers who might otherwise have failed a traditional credit analysis.

The industry speaker observed that there is also mutual benefit in the finance sector using AI. AI contributes to the competitiveness of the financial sector and the financial sector, which holds a great deal of data, can help to enhance AI. However, there are some important roadblocks to consider. Even if banks and financial services firms have every intention to adopt and use AI, they can be prevented from doing so due to internal company structures, legacy technology and data fragmentation within their organisation or in the financial ecosystem.

A second industry representative concurred that AI can help to enhance the competitiveness of financial firms in different areas. AI is not a new technology and has been developed over the last two decades. Some AI use cases have become routine, such as AI-based contact centres that help to improve consumer experience for end-users and reduce customer waiting times. AI also helps to enhance the efficiency of regulatory reporting, fraud detection and anti money laundering (AML). With AI and machine learning technologies, financial firms can detect two to four times more genuinely suspicious activities than false positives, which are very common in the fraud detection space. There is also a huge potential for generative AI to help financial firms improve their risk management, regulatory reporting and ability to make sense of the huge amount of data they accumulate.

A Central Bank official agreed that digitalisation will bring very significant changes over the next 5 or 10 years. Some of these technologies are already in use, but it is impossible to predict what will happen in the future. In general, people tend to overestimate the short term impacts and underestimate the longer term ones.

1.2 The role of cloud computing

An industry speaker emphasised that cloud technology has become an enabler of access to AI and machine learning for organisations of all sizes, not only financial services institutions but governments, SMEs and start ups,. With cloud computing, these organisations are able to use the same large language and foundational models as those used by the cloud service providers (CSPs) for their own services and have access to adequate computing power. The added value of the cloud is enabling all customers to access state-of-the-art technology and models in order to innovate with their own data. Customers bring their own data into these models and can adjust the models to suit their own use cases. Cloud services therefore have to be as accessible as possible to fully leverage the potential of AI.

Another industry speaker agreed that cloud services are a major enabler of AI. Currently, the best AI services are delivered via the cloud. Hopefully, further additional CSPs, perhaps including some larger European ones, will eventually emerge to support the development of the sector.

1.3 The need for enhanced digital literacy

A public representative observed that competitiveness will only truly be enhanced by using human resources and technological innovation in combination in an efficient way. This means there needs to be a good understanding of AI and digital technologies, which requires the labour force to be well educated.

Digital literacy should not be underestimated. If there is insufficient understanding of how these technologies will be used and the added value they bring, people will be resistant to them and worry about losing their jobs. There also needs to be a good understanding of these technologies within regulatory bodies to ensure that any regulations can be properly implemented. Currently, there are significant differences in the level of knowledge between different regulatory bodies and member states, which may lead to an inconsistent implementation of digital and data legislations.

An industry speaker agreed with the importance of developing an understanding of AI and its potential benefits among market stakeholders. Without this understanding, the market will not be able to take advantage of AI. In this regard, a great deal of education is still needed.

2. The implications of new technologies for resilience

An industry representative observed that the adoption of cloud computing helps to improve resilience and cybersecurity by giving customers access to the defence mechanisms used at scale by CSPs to secure their own activities.

A Central Bank official emphasised the importance of also taking into account the risks to resilience posed by the growing use of new technologies in the financial sector. There are three key risks from a financial stability perspective: operational resilience, governance and contagion risk. Consumer-related risks such as consumer protection and discrimination risks are also important to tackle.

In relation to operational resilience, cybersecurity is the main risk. Each time a new technology is introduced in the financial system, it opens a new channel for cyber-risk. In addition, adversaries such as criminals and hostile governments are also increasingly using these new technologies. Outsourcing is also a critical aspect of operational resilience risk. This is quite a complex issue which could have serious implications in terms of tail risks and crisis situations, in addition to everyday business continuity issues. The financial sector is increasingly dependent on outsourcing to tech companies and cybersecurity firms, including both large CSPs and smaller providers. The issues related to governance risk are mainly connected to AI. These include explainability, accountability, data governance and model governance risks, as well as black box algorithm and algorithm validation issues. There are particular risks when AI systems are used for liquidity measurement and risk management. As for contagion risk, its importance is illustrated by the SVB and Credit Suisse crises during March 2023. If the same AI models are used across the market, it could lead to herd behaviour and market manipulation. This risk should be taken seriously because markets are very fragile.

A public representative noted that two key aspects of resilience came up in the debates in the EU Parliament around digital and data legislation. The first is the safety and resilience of digital infrastructure which requires sufficient investments to be made. The second is the potential lack of accountability for example in some decentralised platforms based on blockchain.

3. Regulatory and supervisory implications of the ongoing digital transformation

3.1 The objectives and challenges of digital regulations

An official noted that the Spanish EU Presidency is currently managing several important and sensitive dossiers that aim to pave the way for a new digital economy based on human centric technology and an adequate protection of rights. These include the AI Act and the Cyber Resilience Act, on which work is ongoing. A close collaboration will be needed between the public authorities and all the relevant stakeholders to finalise these frameworks and ensure their sustainability.

While short term initiatives on competitiveness are important for the development of a digital economy, longer term policies focusing on resilience will ensure that the development of AI is sustainable over time. To accomplish this, Spain is pursuing the Digital Spain 2026 agenda, which has three areas of focus: (i) infrastructure and technology, which covers AI and quantum computing; (ii) building awareness among companies of the opportunities of digitalisation; and (iii) ensuring people are trained and have sufficient digital skills. Training and digital skills will ensure that people understand the key risks from digitalisation, such as biased information and explainability and the importance of data. People also need to understand the cybersecurity risks from the poisoning of data and how data-related issues might affect their lives.

A public representative stated that the EU has led the way on establishing a regulatory framework for technological developments such as AI, but the challenge for policy-makers is about how to balance safety and innovation and how to preserve competitiveness as further technological developments take place.

A first challenge is to ensure that small and medium sized enterprises (SMEs) can remain competitive in the

global market. In the Data Act, which is the first legislation to put an economic value on data and properly define it, there is an important emphasis on SMEs. The Data Act seeks to ensure they can benefit from access to bulk data which they cannot generate themselves. This is the only way for them to be competitive in global markets. Secondly, the competitiveness of the start up sector needs to be further promoted and boosted. The European Parliament is developing initial legislation on European start ups with the idea of guaranteeing small entities within the EU access to private capital to help them grow. This includes properly defining what a start up is, which should include notions around innovation and technological development. Finally, progress must be made on digital and financial literacy in the coming years in order to leverage the potential of technology in society.

An industry representative noted that the Data Act has tremendous value for cloud services because it facilitates the interoperability and portability of data, which will enable industries to adopt a multi cloud or open cloud approach and facilitate choice between providers. The AI Act is also an essential piece of legislation, as it defines how Europe should deploy AI for decades to come. As Google's CEO has suggested, AI is too important not to regulate and too important not to regulate well. A responsible development of AI is needed, which means not only mitigating the risks from its use but also ensuring that AI can improve people's lives and address social and scientific challenges.

Another industry speaker added that AI also requires appropriate data regulation. This is a challenge because the European data space is fragmented. Some sectors are subject to open data requirements, for example, while others are not. Concerning the AI Act, the European public authorities, which are endeavouring to be trendsetters in this field, should be careful not to over-regulate. That would only limit the capacity of European companies to take advantage of the technology.

3.2 The possible need for sectoral AI regulation

Answering a question from the Chair about whether a more targeted and sectoral legislation of AI would be needed, an industry representative stated that the risk based and outcomes based approach of the AI Act needs to be preserved. AI models are purpose-agnostic, which means that the same models can be used for multiple activities. The same technology that can be used for abusive activities can also be used to tackle abuse. Regulating all the different activities using AI and foundational models would be an extremely broad scope. This does not seem like a relevant approach to take. This is important to bear in mind as trialogues are progressing.

For the time being, there should be a focus on high-risk applications, the industry representative suggested. If sector specific AI requirements are needed at some point, this could be achieved without developing a new AI regulation. Existing financial services regulation may be adjusted to make it applicable to AI. The use of sandboxes could also be a helpful approach. For example, the Monetary Authority of Singapore (MAS) has created a principles-based framework and assessed the ability of tech providers and banks to implement AI in line with it.

3.3 Supervisory implications

A Central Bank official emphasised that new technologies create new supervisory challenges. Supervisors need to understand any new technology and they need to be able to check whether supervised entities understand how it should be used and the risks it may create. This can be a challenge for supervisors because some of the risks posed by these technologies are still not fully understood, especially when several different technologies are being used in combination. In addition, the risk profiles may differ when technologies are used for different services.

Significant changes in the division of competencies between supervisory authorities will be needed in the coming years to tackle these risks. Financial supervisory authorities (FSAs) should become increasingly involved in digital issues. There should also be a new culture of cooperation with other supervisory authorities, including financial intelligence units (FIUs), data protection authorities and cyber protection authorities. Secondly, the deployment of technologies such as AI will require agile and adaptive partnerships between financial entities and supervisory authorities. It is extremely important for supervisors to have open and feedback based communication with financial entities. Eventually, all FSAs will also use AI systems. If both banks and FSAs use AI systems, it will create the possibility of real time supervision.

The Central Bank official added that further clarity will also be needed on the rules regarding data sharing both between banks and with supervisory authorities for addressing issues such as AML and sanctions. This kind of data-sharing is highly beneficial, but there are currently some restrictions.

An official emphasised that sandboxes can also be useful when developing AI systems. For example, Spain is developing an AI sandbox. The goal of this initiative is to set up a environment in which stakeholders can discuss and collaborate on the use of AI and the effects of the AI Act. In order to track how companies and institutions apply these measures, Spain has created an AI supervisory agency, which should also foster the Spanish authorities' understanding of how to apply any future regulatory measures.