Denis Beau: Mastering AI in the financial sector - let us collectively rise the challenge!

Speech by Mr Denis Beau, First Deputy Governor of the Bank of France, at the Paris financial centre event devoted to artificial intelligence, Paris, 11 December 2024.

* * *

Ladies and gentlemen,

First of all, I would like to thank the organisers for their invitation to this Paris financial centre event devoted to artificial intelligence (AI): it gives me the opportunity to continue the dialogue that we at the Banque de France and the ACPR have been conducting with financial players on this important matter for the industry.

I'll be brief on the observation: **AI is one of the most powerful forces driving the current transformation** of the financial sector. Its adoption has accelerated with the advent of **generative AI**, which has made the opportunities in terms of productivity, customer interaction, compliance management, etc. more accessible - and visible to all. As supervisors, but also as users of these new technologies, every day we can see the speed and potential of this phenomenon.

Naturally, **these technologies can give rise to many risks,** for all financial system participants as well as for the stability of the system as a whole. It is essential that they are properly managed: the following round-table discussion will shed light on these risks and the operational challenges they present. I'll mention just one of them now, but not the least important: **cyber risk.** In my view, it is a good illustration of the complex issues we are facing. AI amplifies cyber risks, not least because it is used by attackers to increase their effectiveness; AI also has its own specific vulnerabilities (such as the risk of data poisoning). Conversely, AI can provide the antidote, and improve IT security management, for example, by helping to detect suspicious behaviour or new threats. **Greater cooperation is needed in this area between data scientists and cyber-security specialists,** in order to unlock the full potential of AI for cybersecurity.

I would now like to turn to the regulatory and supervisory aspects that a supervisor naturally thinks of when discussing the opportunities and risks of AI. **The European Union has been a pioneer in this field, with the AI Act.** This will mainly concern the financial sector for two use cases: creditworthiness assessment for granting credit to individuals, and risk assessment and pricing in health and life insurance. The ACPR should be responsible for enforcing this regulation, as market surveillance authority.

This new regulation, and more broadly the issues associated with AI, are raising legitimate questions from the financial sector: to what extent will the new requirements affect the players? Isn't there a risk of stifling innovation for the sake of mitigating risk? Without providing a blanket answer to these questions, I would like to put the debate into perspective **as far as the financial sector is concerned,** with two simple messages: i) there is no cause for alarm, as the risks linked to AI can essentially be dealt with within the framework of existing risk management systems; ii) however, we should not underestimate certain new technical challenges associated with AI.

As far as risk management in the financial sector is concerned, the AI Act will not bring about a Copernican revolution.

Financial institutions have a sound risk management culture, as well as robust **governance** and **internal control** systems. Very recently, the **DORA** regulation supplemented the traditional regulatory framework with specific rules on operational resilience and IT risk management. The **financial sector is therefore well equipped** to meet the challenge of complying with the new regulations.

Admittedly, the objectives of the AI Act, namely the protection of fundamental rights, and those of prudential regulation - financial stability and the ability to meet customer commitments - **differ. But, operationally,** when the AI Act requires "high-risk systems" to have a risk management process, data governance, traceability and auditability, and measures to guarantee robustness, accuracy and cyber-security throughout the lifecycle, are we really in uncharted waters? I don't think so.

On the contrary, I believe that the **principles of sound risk management and governance in force in the financial sector remain valid for the AI Act.** They will therefore be the ACPR's yardstick for assessing the compliance of systems when it is called upon to exercise its role of market surveillance authority. More specifically, our approach to this new mission can be summed up in a few principles: (i) the implementation of **'market surveillance'** in the regulatory sense, i.e. primarily aimed at identifying systems likely to pose compliance problems; (ii) a risk-based approach to ensure that the means implemented are **proportionate** to the intended outcomes; and (iii) making full use of **synergies with prudential supervision.** I believe that this was the intention of the European legislator, when it entrusted national financial supervisors with the role of "market surveillance authorities". It's also the best way of ensuring that we don't make the regulations any more complex, at a time when our common objective should be to **simplify** them.

Naturally, **the principles** of good governance and internal control also **apply to the algorithms that would not be considered high-risk** by the AI Act, if they pose risks, for example of a prudential nature, to the organisations concerned: in this area, the experience acquired from the implementation of the AI Act and the resulting best practices will be invaluable for both supervisors and supervised entities.

I repeat, risk management culture is an asset. However, **the challenges posed by the use of artificial intelligence should not be underestimated.**

Some of the challenges raised by this technology are entirely new. Let me give you two examples.

Firstly, **explainability:** with each advance in this field, artificial intelligence algorithms have become increasingly opaque, to the extent that it is often difficult, if not impossible, to understand and explain certain results proposed by the machine or to identify their sources, even if some tools are striving to combat this shortcoming. In a regulated sector such as the financial sector, this question is naturally crucial, and needs to be addressed at every level: **day-to-day users** of AI tools need to have a sufficient understanding of how they work and of their limitations if they are to make appropriate

use of them and avoid the two pitfalls of either blindly trusting the machine or of systematically mistrusting it. The **supervisors** that monitor the operation of AI systems and, above all, the **auditors** who review them, need more advanced technical and functional explanations to assess their performance, reliability and compliance. Not forgetting the final **customer** who, if in direct contact with an AI algorithm, is entitled to explanations for the rationale behind the decision taken or the commercial proposal made to them.

The second example is **fairness.** Back in 2016, the chatbot Tay, which became 'racist' in the space of a few hours, made us all aware of this issue; the biases identified more recently in consumer tools such as ChatGPT are a reminder that artificial intelligence is particularly sensitive to the biases present in data, and is likely to reinforce them. Indeed, one of the aims of the AI Act is to detect and prevent these biases before they cause harm to citizens. This is a **technically complex** issue, as banning the use of certain protected variables is not enough to guarantee that algorithms are harmless. This is particularly true for activities such as granting credit or pricing insurance, where **customer segmentation is part of normal business and risk management practices** in a competitive environment.

Speakers at the following round tables will no doubt explain how they are tackling these challenges in practical terms. I would simply like to share one conviction. One of the challenges, if not the main challenge, is to get specialists from very different backgrounds to talk together and understand each other: **data scientists, legal experts, specialists in human-machine interaction, auditors,** etc. I mentioned earlier the need for cooperation between data science and cybersecurity: as you can see, the circle of cooperation that needs to be put in place is actually much wider!

To address these new aspects, and to provide proof that the various regulatory requirements are being met, **financial institutions will need to enhance their skills** by acquiring new human and technical capabilities. As market surveillance authority and prudential supervisor, the ACPR will ensure that risks are effectively managed. Compliance with the AI Act is naturally more than just an administrative process of internal labelling, and the supervisor cannot simply 'tick boxes'. On the contrary, the supervisor will have to ensure that the algorithms are managed and monitored by competent people who understand their inner workings.

This means, of course, that the **financial supervisor** itself has to acquire new skills and **adapt its tools and methods.** We will have to gradually establish a set of rules regarding new issues such as explainability, a topic on which the ACPR has already published some proposals in the past, or the fairness of algorithms. We will also need to develop a specific methodology for auditing AI systems.

We cannot and must not take this methodological step alone: instead, we need to **build synergies with all the other AI supervisors** in France and Europe. AI regulation is cross-sectoral and the supervisors will not escape the pressing obligation of cooperating in this area, which involves so much diverse expertise.

Today, I would like to extend this **call for cooperation** to the whole financial sector. Articulating the AI Act with sector-specific regulations, clarifying expectations, sharing best practices, developing audit methodology: **supervisors and the supervised share**

many challenges, and we will overcome them all the more easily if we are able to move forward together. The ACPR is now preparing itself for the 2026 deadline: as it has already done in the past, it will seek input from the entire ecosystem to co-design practical methods for implementing - and supervising - the AI Act. That is why I am today calling on volunteer companies in the financial sector to contact the ACPR staff to take part in our work.

For the stability of the financial sector, **we must collectively master the uses of AI; together, let's rise to this challenge!** Thank you for your attention.