Archives de philosophie du droit
Droit et Intelligence Artificielle
Novembre 2025 - Tome 66

Implementing effective surveillance of AI in the financial sector

Article by Denis Beau
Designated Chairman of the Autorité de contrôle prudentiel et de résolution (ACPR), first Deputy Governor of the Banque de France.

SUMMARY — Artificial intelligence is profoundly transforming the financial sector, bringing gains in efficiency, security and personalisation of services. However, it also brings new risks, particularly in terms of explainability, fairness and cybersecurity. The adoption of the European AI Act in 2024 introduces a horizontal regulatory framework that supplements existing sectoral regulations. As the supervisory authority for the financial sector, the ACPR must adapt its methods, strengthen its expertise and cooperate with public, private and academic players to ensure effective surveillance of AI systems. This article explores the legal, methodological and operational challenges of this evolving environment.

KEY WORDS — Financial regulation – ACPR – AI oversight – Cybersecurity – RegTech – SupTech

Artificial intelligence (AI) is now establishing itself as a major driver of transformation in the financial sector, from assessing credit risk and setting insurance rates to estimating asset volatility. Its rapid adoption across all segments of the value chain, particularly with the rise of generative AI, could prove highly beneficial in the banking and insurance sectors. Firstly, it could lead to **significant productivity gains** through increased automation of administrative tasks (machine reading of documents, automated photograph analysis, etc.). AI also makes it possible to **offer better customer services**, particularly through increased personalisation; lastly, it can help to **strengthen security**, particularly for combatting money laundering and terrorist financing (AML-CFT) and in the fight against fraud.

However, this technological revolution also brings with it **new risks**, both for individual players and for the stability of the financial system as a whole. In particular, these risks include the misuse of these technologies (the complexity and novelty of modelling can lead to model calibration errors and potentially systematic losses) – exacerbated by the 'black box' phenomenon of certain systems – or cyber risk, which AI is likely to amplify significantly, both as a new source of vulnerability and, above all, by increasing the degree of danger posed by hackers.[1]

[1] Conversely, AI can also enhance IT security, for example, by helping to detect suspicious behaviour.

In the financial sector, AI therefore represents both an opportunity and a challenge, and this ambiguous impact justifies the need for **regulatory oversight** of these new technologies. While financial sector regulations already provided a framework for most AI-related risks, they were enhanced, but also made more complex, by the adoption of the AI Act in the summer of 2024.[2]

For the financial supervisor, the *Autorité de contrôle prudentiel et de résolution* (ACPR), the main issue raised by this regulation, as well as by the increasingly widespread use of AI in the financial sector, is how to implement both **effective and efficient oversight**. Firstly, this means that we need to consider the theoretical and practical linkages between the AI Act and the existing financial sector regulatory framework (I). We then need to develop the operational capabilities necessary to carry out this new mission (II).

I. — THE LEGAL FRAMEWORK FOR AI

As the legal framework in the financial sector has become more extensive and complex, the challenge for the ACPR is to ensure compliance with appropriately articulated regulations.

1.1 While financial regulations already included objectives that could be applied to AI, the AI Act establishes a "horizontal" regulatory framework for AI systems with a different perspective.

Financial sector regulation is technology-neutral: the objectives it sets out – in particular, effective risk management and, more broadly, preserving financial stability – apply regardless of the tools actually used by institutions to implement their processes. It is therefore only natural that banking and insurance regulations apply to AI algorithms in the financial sector, even if, in practice, they are currently not subject to very comprehensive oversight.

For instance, the DORA package of 14 December 2022 on the sector's digital operational resilience,[3] the European Banking Authority (EBA) Guidelines on ICT[4] and security risk management measures of 2019, and the ACPR Notice on IT risk management of 2021 provide a framework for AI-related cyber risk.

In terms of prudential regulation, the CRR Regulation[5] and CRD Directive[6] for the banking sector, as well as the Solvency II Directive[7] for insurers, allow risks associated with AI to be taken into account in internal model calculations and prudential ratios. These texts treat IT risks, such as those related to AI, as operational risks, whose management can have an impact on institutions' capital.[8]

---

2 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.
3 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector
4 EBA/GL/2019/04,
5 Regulation (EU) No 575/2013 on prudential requirements for credit institutions and investment firms
6 Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms
7 Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).
8 Articles 312 to 324 of the CRR Regulation, Article 85 of the CRD Directive, Articles 100 and 107 of the Solvency II Directive (operational risks).

In contrast, the AI Act follows a very different approach: reconciling the protection of the health, safety and fundamental rights of European citizens with the development of a European market for "trustworthy AI". Furthermore, unlike specific financial sector regulations, which focus on institutions, their activities, operations and organisation, this new Act focuses on product safety and is a "horizontal" regulation, setting out principles that apply to all economic sectors and public services. It will mainly concern the financial sector for two "high risk" use cases: creditworthiness assessments for granting loans to individuals, and risk assessments and pricing in health and life insurance. The ACPR is expected to be assigned the role of **market surveillance authority**, responsible for overseeing high-risk systems in the financial sector.

The coexistence of two sets of regulations with widely differing objectives and formats naturally raises the question as to the legal and practical relationship between them.

I.2 The 'horizontal' framework for AI systems established by the AI Act requires coordination with existing legislation.

The first probable outcome of the adoption of the AI Act is that supervisory authorities will have to ensure that fundamental rights and freedoms are reconciled with companies' prudential requirements for the preservation of financial stability. These different approaches can indeed lead to different risk assessments. Here, the ACPR already balances different goals as part of its prudential, customer protection, and AMLCFT duties.

Moreover, the implementation of the AI Act requires finding a connection, in the strict sense, between this new 'horizontal' regulation and existing sectoral ('vertical') rules, even though this connection is not explicitly provided for in the AI Act, with the exception of certain provisions specific to financial institutions, notably the integration of certain requirements into existing internal control processes.[9] This work of **mapping** the respective requirements of sectoral regulations and the AI Act began within the European supervisory authorities, in particular the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA).[10] This work is not yet complete, but initial findings suggest that the principles applicable to AI systems under sectoral regulations are **very similar** to the requirements of the AI Act – even if the stated objectives and presentation differ.[11]

A comparison of the two sets of regulations also tends to highlight that the scope of "high-risk" systems in the AI Act is **fairly limited** in the financial sector. Many areas are therefore not covered by this regulation, even though the use of AI systems could pose significant risks to the financial system as a whole (e.g. automated trading systems), as well as to various financial entities (e.g.

---

9 See, for example, Article 17.4 of the IA Act: when suppliers are financial institutions, compliance with the governance and internal control obligations set out in sectoral regulations is equivalent to compliance with the obligation to implement a quality management system (with a few exceptions).

10 As regards the interplay between the AI Act and the GDPR, guidelines should be published jointly by the European Commission and the European Data Protection Board (EDPB).

11 For example, an EIOPA opinion currently being published shows that insurance sector regulations essentially impose obligations that are almost equivalent to those in the AI Act, with two minor differences: (i) differences in administrative obligations; (ii) in sectoral regulations, the intensity of the applicable obligations is proportionate to the risks of the AI system.

business lending, AML/CFT, fraud prevention, etc.) and customers (e.g. home insurance, car insurance, etc.). The ACPR is therefore responsible for supervising a broader range of AI systems than merely the “high-risk” systems covered by the AI Act.

In this regard, the fact that the requirements arising from the AI Act and the specific regulations governing the financial sector are reasonably well aligned should make it possible to **establish a relatively unified AI system oversight activity**, which will as such be easier to implement. The ACPR will draw on **two organisational principles** to contribute to this harmonisation: firstly, a risk-based approach, aimed at ensuring that the means employed are **proportionate** to the expected results; secondly, maximum use of **synergies** with its usual supervisory activities. The latter point reflects the intention of the European legislator, who wished to entrust the role of "market surveillance authority" to national financial supervisors. It's also the best way of making sure that we do not make the regulations any more complex, at a time when the common objective should be to **simplify** them.

II. — OVERSIGHT OF AI: THE OPERATIONAL PREPAREDNESS OF THE ACPR

II.1 The assessment of AI systems raises new questions for supervisory authorities

In view of the new AI system oversight activities that will result from both the AI Act and sectoral regulations, the ACPR has set up an internal task force, bringing together all of its business lines, which has been charged with preparing the authority in at least four key areas: legal aspects, internal organisation, European and national cooperation and auditing. One of the major challenges of this preparatory work is to develop a **methodology for evaluating** AI systems in the financial sector. This methodology should make it possible to assess the governance of an AI system, as well as certain characteristics of the system itself, such as its performance, robustness, and cyber security. Some of these areas are fairly traditional in a sector where many processes have long used modelling, even though they could employ new techniques. Others, however, are **entirely new**.

Two examples illustrate this point well. The first is **explainability**: with each advance in this field, AI algorithms have become increasingly opaque, to the extent that it is often difficult, if not impossible, to understand and explain certain results produced by the machine or to identify their sources, even though some tools and devices offer solutions to tackle this shortcoming. In the financial sector, this question is clearly crucial and needs to be addressed at all levels: day-to-day users of AI systems in institutions need to understand how they work and their limitations well enough to use them appropriately and **avoid the two symmetrical pitfalls of systemic mistrust and blind trust in the machine.** The **controllers** who 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. Lastly, end **customers** – who are in direct contact with an AI algorithm – must be guaranteed the right to an explanation of the decision made or the business proposal made to them.

Fairness is another important example. **AI is particularly sensitive to biases*** present in data, and models are 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. However, this is a **technically complex** issue, as simply prohibiting the use of certain protected variables is not enough to guarantee that the algorithms are harmless. This is particularly the case in activities such as lending or insurance pricing, where **customer segmentation is part of normal business and risk management practices** in a competitive environment.

II. 2 To address these new challenges, the ACPR will need to develop its expertise and adapt its methods.

To address these new developments, financial supervisors will need to enhance their skills and adapt their tools and methods. The ACPR had already published some avenues for consideration[12] in the past, but it will need to gradually develop a comprehensive policy on such new issues, particularly with a view to clarifying what it **essentially expects** from the financial sector

Naturally, the ACPR intends to ensure that the **risks associated with AI are effectively managed**: compliance with AI regulations or financial regulations cannot, of course, be limited to an administrative process of internal certification, and institutions cannot simply "tick boxes". Instead, they must ensure that algorithms are managed and monitored by competent individuals who understand how they work in depth.

To move forward with this methodological change, the ACPR – like the financial sector itself – will probably need **external support**. Under the AI Act, the State should therefore establish a "pool of shared technical expertise" to assist market surveillance authorities in their tasks of assessing AI systems, in particular to address certain cutting-edge methodological issues.[13] Similarly, it would be useful for supervisory authorities to establish different types of partnerships with research institutes specialising in AI.[14] Lastly, it may also be necessary to enlist the expertise of private service providers specialising in compliance activities (known as "**RegTech**" for regulatory technology).

More generally, the ACPR plans to **forge synergies with all other AI supervisors** in France and Europe. Supervisors will not be able to sidestep the pressing obligation to cooperate on this issue, which requires such a wide range of expertise. One of the challenges is precisely to facilitate dialogue and mutual understanding between specialists from very different backgrounds: **data scientists, lawyers, human-machine interaction specialists, IT specialists, auditors, etc.** Furthermore, as it has done in the past, the ACPR will seek input from the financial sector to jointly develop, as far as possible, practical methods for assessing and implementing AI-related requirements. Indeed,

---

12 Following an initial discussion paper published in 2018 on the challenges of using AI in the financial sector (Artificial intelligence: challenges for the financial sector, 2018), practical workshops were organised in 2019 with volunteer institutions to explore these topics in greater depth. This gave rise to a second discussion paper (Governance of artificial intelligence algorithms in the financial sector, 2020), which set out technical principles (data, efficiency, stability, explainability) and governance principles for the development of AI algorithms.

13 In addition, the AI Act stipulates that the EU shall gradually establish centres of expertise for AI assessment, known as Union testing facilities (UTFs).

14 In this regard, we note the creation in early 2025 of the French national institute for the assessment of the security of artificial intelligence (INESIA) pooling resources from several research and assessment organisations.

supervisors and supervisees share many challenges, and they will overcome them more easily if they tackle them together.

II. 3 The ACPR already uses AI for its own requirements.

By profoundly changing the way we interact with information, AI technologies offer supervisory authorities unprecedented leverage to enhance the effectiveness, responsiveness and granularity of their controls. Like other European and international authorities, the ACPR has been committed for several years to a proactive approach to technological innovation, known as Supervisory Technology (**SupTech**). It is part of a broader movement, led in particular by the Single Supervisory Mechanism (SSM) under the aegis of the European Central Bank (ECB), which defined a SupTech roadmap in 2020, and by the network of innovation centres of the Bank for International Settlements (BIS).

This strategy is based on a strong conviction: technological innovation should not be endured, but rather integrated in a controlled manner into supervisory practices. This approach should enable the ACPR to continue to carry out its duties effectively, while **achieving more and obtaining better results.** AI can obviously help to **increase efficiency** by further automating processes. However, the ACPR also intends to offer **new capabilities** to its staff.

In 2018, the ACPR set up a pilot programme aimed at providing them with new digital tools. This approach has gradually enabled the ACPR to develop a series of **practical tools** that meet a variety of operational needs: automatic translation of technical documents, transcription of telephone conversations, analysis of advertisements, pre-analysis of regulatory reports, etc. These tools were designed in close cooperation with the business lines to ensure that they are relevant, user-friendly and compatible with existing information systems. The LUCIA tool, for example, allows the ACPR, during its on-site inspections, to assess the performance and appropriateness of the AML/CFT models developed by banks by analysing large volumes of banking transactions.

The advent of **generative AI**, and in particular “large language models" (LLMs)*, represented a new milestone. These models make it possible to interact with complex text corpora using natural language, generate summaries, detect inconsistencies, and even transform text into code. To assess their potential, in February 2024, the ACPR organised a Tech Sprint bringing together external data scientists and supervision experts. The results were **particularly promising:** the prototypes demonstrated the ability of LLMs to perform advanced searches in document databases, produce intelligent summaries of reports, pre-check the compliance of regulatory documents, or even automatically generate visualisations from raw data.

These experiments provided a better understanding of the **benefits**, but also the **limitations**, of these technologies. They highlighted the need for rigorous oversight: traceability of results, explainability of reasoning, bias control, and data security. They also raise **more fundamental questions** about the evolution of supervisory activities: how much of the analysis should be entrusted to machines and how much to humans? How will LLMs transform our relationship with

information and reporting? Indeed, AI may be poised to profoundly transform the way in which all financial supervision activities are organised and carried out.

***

The ACPR is now at a crossroads: it must develop a consistent, proportionate and effective framework for supervising the risks associated with the use of AI in the financial sector, while also adapting its tools to make the best use of the technological advances enabled by AI. **These objectives are in no way contradictory**: using AI for their own needs allows supervisors to gradually acquire a good command of the technology and is a very effective way of properly **understanding its benefits and risks.** AI is therefore becoming a strategic tool that supervisors must master in order to ensure stability, confidence and responsible innovation.