Legal high Committee for
Financial markets of Paris

THE LEGAL AND REGULATORY IMPACTS OF ARTIFICIAL INTELLIGENCE IN BANKING, FINANCIAL AND INSURANCE MATTERS

of the Legal High Committee for Financial Markets of Paris

June 20, 2025

9 rue de Valois, 75001 Paris, France - Tel.: +33 (0)1 42 92 20 00 - hautcomite@hcjp.fr - www.hcjp.fr

Table of contents

Paragraphs **Page**

INTRODUCTION/SUMMARY

Artificial intelligence (**AI**) is not a recent innovation. It dates back to the very origins of computing – more than 70 years ago – when the British mathematician Alan Turing considered (in an article published in 1950[1]) whether machines could think. The Dartmouth Conference in 1956 is another example of AI development when around twenty researchers came together to lay the foundations of AI as a scientific discipline, under the impetus of John McCarthy[2].

AI has grown exponentially in recent years thanks to the development of *Big Data* and its democratisation among the general public, particularly with the emergence of generative AI systems from 2022 onwards. Developments in AI are set to continue, with the aim of representing a market worth several hundred billion dollars with half a billion users by 2027[3]. The European Union aims to become the global leader in AI[4] and has announced a plan to invest €200 billion via the "InvestAI" initiative with this in mind[5].

AI affects all sectors, including banking and finance. It appears to be "the main growth driver of digital transformation"[6] for companies in this industry, such as credit institutions, investment firms, insurance companies, payment institutions, electronic money institutions and management companies (**Financial Institutions**).

The use of AI by Financial Institutions led the French supervisory authorities to ask the *Haut Comité Juridique de la Place Financière de Paris* (the **HCJP**) to study the legal and regulatory impacts of AI in banking, finance and insurance by setting up a working group, bringing together business experts, representatives of the authorities, law professors and lawyers at the end of 2023 (the **working group**)[7].

The mission entrusted to the working group excludes from the scope of the analysis the use of AI for the purposes of the supervision and control of Financial Institutions, in particular the fight against money laundering and terrorist financing, or the issues of disciplinary liability for Financial Institutions in relation to AI. The issue of the insurability of AI risks is also excluded from scope.

After a year's work, the working group has drawn up this report (the **Report**).

---

1 *A. M. Turing, Computing Machinery and Intelligence, Mind, 49, 1950, p.433-460.*

2 *J. Henno, 1956: et l'intelligence artificielle devint une science, Les Echos, 21 August 2017.*

3 *BPI France, Marché de l'intelligence artificielle: où en sommes-nous? 4 June 2024 (https://bigmedia.bpifrance.fr/nos-actualites/marche-de-lintelligence-artificielle-ou-en-sommes-nous); BPI France, Les chiffres 2023-2024 du marché de l'AI dans le monde, 23 June 2024 (https://lehub.bpifrance.fr/les-chiffres-2023-2024-du-marche-de-lia-dans-le-monde/).*

4 *European Commission, Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions – AI Continent Action Plan, 9 April 2025, p. 1: "The European Union is committed and determined to become a global leader in Artificial Intelligence, a leading AI continent".*

5 *Ursula von der Leyen, President of the European Commission, Speech by President von der Leyen at the Artificial Intelligence Action Summit, 11 February 2025.*

6 *Denis Beau, Senior Deputy Governor of the Banque de France, L'intelligence artificielle: bénédiction ou malédiction pour la transformation du secteur financier, Speech, Singapore, 8 November 2024.*

7 *See Annex 1 – Participants in the working group.*

It quickly became apparent that Financial Institutions have been using AI for a number of years for a variety of purposes. The technology offers more and more possibilities, creating new opportunities. The working group observed that AI has become an essential tool for the provision of regulated services in this sector (e.g. credit scoring, robo-advisers, chatbots, etc.)[8]. This development has established a natural dichotomy between "AI assistants", who help humans with their tasks, and "AI performers", who have a higher degree of autonomy. This AI-driven digital transformation promises to redefine traditional practices and open up new opportunities for the financial industry.

In view of the increasing number of use cases for AI by Financial Institutions, the working group looked at the current regulatory framework for AI in the financial sector, in particular by analysing the applicable sectoral regulations. The Paris Europlace association, in its response[9] to the European Commission's consultation on AI in the financial sector[10], has already conveyed the message that there is existing sectoral regulation covering – at least in part – AI technology[11].

The working group then looked at how these existing sector-specific regulations could further take account of these risks generated by AI (e.g. algorithmic biases, hallucinations, etc.), and examined the governance issues for each type of Financial Institution and the control framework that could be defined.

Certain subjects covered by regulations specific to Financial Institutions, such as customer protection, customer data protection (in particular professional secrecy), prudential requirements, or relations with third-party service providers, in particular in the case of outsourcing, already define a regulatory regime that makes it possible to supervise the use of AI.

The analysis of the AI regulatory framework for Financial Institutions has of course taken into account the brand new AI regulation produced by the European Union, the Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (the **AI Act**).

---

8 *International Organisation of Securities Commission (**IOSCO**), Artificial Intelligence in Capital Markets: Use Cases, Risks, and Challenges, March 2025.*

9 *Paris Europlace, Target consultation on AI in the financial sector, Paris Europlace AI Working Group response, 13 September 2024.*

10 *European Commission, Consultation document – Target consultation on artificial intelligence in the financial sector, 18 June 2024.*

11 *Paris Europlace, op. cit. n°9, "In itself, AI is not new, having indeed quite a long history in the financial services industry (for credit risk scoring, high-frequency trading, and robo-advice) and being already subject to existing risk frameworks. Specifically, AI applications in finance are already subject to regulation through sectoral or cross-sectoral specific rules, such as consumer data privacy regulation, consumer protection regulation in lending operations, or prudential requirements concerning data governance, cyber risk, third-party risk, information systems outsourcing, and operational risk. We thus consider that the financial industry is already more heavily regulated than other sectors. We stand for that reason against an additional, sectoral regulation", p. 1.*

The AI Act is an innovative legal framework that governs the design, development, deployment and use of AI systems, in order to ensure their proper use while minimising the risks to human well-being and society. It is still necessary to identify which AI tools are within the scope of the AI Act. The demarcation between AI and much simpler software systems is fine because of the complexity of AI and continuous technical evolution. The European Commission itself admits it is not possible to automatically determine, or to draw up an exhaustive list of, systems that do or do not fall within the definition of an AI system[12].

In drafting the Report, the HCJP based itself on the European definition of AI, itself taken from the OECD definition[13]. According to Article 3(1) of the AI Act, an "AI system" (**AI System** or **AIS**) is an automated system, designed to generate outputs from the inputs it receives, such as recommendations, predictions or decisions influencing its environment.

These systems include logical reasoning, predictive analysis, machine learning techniques and their deep learning subset. Natural language processing (NLP) technologies, which enable algorithms to process data encoded in human language, are also understood as AIS. Deterministic AI co-exists alongside generative AI. The former is often described as "basic" because it follows predefined rules to process repetitive tasks[14]. Technically less advanced than generative AI, deterministic AI is mainly used for automating administrative tasks or simple data analysis. However, this type of AI is sufficiently advanced not to be considered as a simple automation of a process usually carried out by a human.

However, the European Commission decided to exclude linear regression, logistic regression[15] and classical heuristic methods[16] because they are virtually identical to basic data processing.

Simple prediction models will also be excluded from scope of the AI Act[17]. This includes systems using basic statistical learning rules such as financial forecasting models, including those predicting future share prices. These tools are cited by the European Commission as examples and, given the speed of technological developments, are not intended to amount to an exhaustive list of simple prediction models that fall out of scope of the AI Act. In any case, the boundary between AI tools and simple software systems can be difficult to determine but is fraught with consequences. As a result, Financial Institutions will not be able to spare themselves a detailed definition exercise to determine whether or not their tool falls within the scope of the AI Act (see paragraph IIA).

---

12 *European Commission, Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), guidelines, 6 February 2025, para. 62.*

13 *OECD, Recommendation of the Council on Artificial Intelligence, adopted on 22 May 2019, amended on 3 May 2024.*

14 *Association Française de la Gestion d'Actifs (**AFG**), Guide Professionnel Principes et bonnes pratiques pour une utilisation responsable de l'AI par les sociétés de gestion, January 2025, p. 7.*

15 *It is commonly accepted that linear regression and logistic regression methods are machine learning techniques that calculate predictions from previous data, for example by looking at customers' past buying patterns, regression analysis estimates future sales.*

16 *A heuristic is a computational method that uses a rule-based approach, pattern recognition or trial-and-error strategies rather than data-based learning. This method therefore lacks the adaptability of AIS that learns from experience. (See European Commission, Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), Guidelines, 6 February 2025, para. 48).*

17 *Ibid, p. 8.*

Finally, a semantic clarification is necessary: the AI Act regulates AI Systems as a whole. These are made up of an "AI model", the essential component, augmented by other components such as a user interface, to form an AI System. Thus, the AI model is part of the AI System. This distinction, although sometimes tricky to articulate in practice, is essential because it will enable Financial Institutions to better identify the applicable regulatory obligations according to the type of system used.

The AI Act adopts a risk-based approach, a concept which is already familiar to Financial Institutions. This risk-based approach will impact the nature of new obligations applicable to the technology for stakeholders.

Financial Institutions are thus confronted with two distinct sets of rules: the horizontal rules stemming from the AI Act and those stemming from sector-specific regulations. There is a question of the relationship between these two sets of rules, as interactions between these two regulatory regimes can be seen at several levels. It should be emphasised, however, that legislators have followed a general approach of complementarity between these two sets of rules (as the European Commission pointed out in its consultation[18]) and bridges have been built between the two.

The aim of the Report is to present and propose a methodology for understanding the issues surrounding the relationship between the AI Act and the sector-specific regulations governing Financial Institutions. It also addresses the application of other sets of texts, such as those relating to data (in particular DORA and GDPR), environmental protection and intellectual property.

Finally, AI cannot be addressed in such a Report without paying particular attention to the liability issues for Financial Institutions, even if the draft directive on liability has been withdrawn from the European Union's current priorities.

The Report will therefore examine the existing framework for AI in sector-specific regulations (paragraph I). The framework, in particular the material and territorial scope of the AI Act, and the classification by risk specific to the AI Act, will be set out in the light of the uses of AI by Financial Institutions. The different roles of AIS operators – provider, deployer, importer and distributor – will also be discussed, along with their special obligations (paragraph II). The working group intends to provide answers and food for thought on the relationship between the AI Act and the sectoral or cross-sectoral regulations governing Financial Institutions (paragraph III) and lastly will address the liability issues relating to Financial Institutions in their dealings with AI (paragraph IV).

[18] *European Commission, op. cit. no.10, "The AI Act is designed to complement the already existing financial services acquis, that, while not explicitly targeted at regulating AI, is an important framework to manage the related risks in specific applications and includes several relevant requirements for financial entities when providing financial services.".*

I. The existing regulatory framework for AI in sector-specific regulations

The regulation of Financial Institutions is technologically neutral. It covers all forms of technology, without imposing constraints specific to any or all of them. However, the use of AI, like any technology used to provide financial services, generates new risks that need to be mapped and managed.

In addition to international bodies[19], national and European supervisors of Financial Institutions have already campaigned for a framework for the use of AI by such institutions[20]. This framework should be able to draw on existing regulations, which already provide for a corpus of sector-specific rules, applicable to a large extent in the event of the use of AI and AI Systems by Financial Institutions, particularly in terms of governance, risk management, outsourcing or customer data protection.

A. AI as a tool for the provision of regulated financial services

In principle, Financial Institutions are free to use AI to provide regulated services to their customers, including banking, payment, investment and insurance services.

Each industry uses AI as tool in the execution of regulated services with a degree of autonomy of certain services, or as a tool for assessing, managing and/or controlling the risks involved. The number of cases in which AI is being used by Financial Institutions has been increasing for several years now, with AI as a tool for the autonomous execution of regulated services remaining the least developed for the time being.

1. The assistant AI

An important function of AI is to assist individuals by automating complex tasks, rapidly analysing large quantities of data or offering suggestions or solutions based on these analyses. Financial Institutions will benefit from using AI.

In the banking sector, AI can play this role by, for example, making it possible to: identify a target market on the basis of available data regarding potential customers (mapping), to answer simple

---

19 *Cf. in particular the report by the Financial Stability Board (**FSB**) entitled "Financial Stability Implications of Artificial Intelligence", dated November 2024; following an initial report in 2021, the International Organisation of Securities Commission (**IOSCO**) published a new report in March 2025 on the use of AI in capital markets, describing the use cases, risks and associated issues (the **IOSCO Report**), subject to consultation until 11 April 2025.*

20 *ACPR, Le développement des big techs dans le secteur financier: quels risques, quelles réponses réglementaires, Dossier, October 2024; ACPR, Intelligence artificielle: quel impact à l'ACPR? ACPR Review, July 2024; ACPR, La transformation numérique dans le secteur français de l'assurance, Analyses et synthèses n°132, 14 January 2022; ACPR, Gouvernance des algorithmes d'intelligence artificielle dans le secteur financier, Discussion paper, June 2020; EIOPA, Factsheet on the regulatory framework applicable to AI systems in the insurance sector, Facthseet, 15 July 2024; EIOPA, Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector, 17 June 2021; EIOPA, Consultation Paper on Opinion on Artificial Intelligence Governance and Risk Management, 10 February 2025; European Commission, White Paper – Artificial Intelligence: an approach based on excellence and trust, 19 February 2020; ESMA, Public statement – on the use of Artificial Intelligence in the provision of retail investment services, 30 May 2024, ESMA35-335435667-5924.*

customer questions, to help assess the credit risk (credit scoring) of a potential borrower, to carry out the documentary analysis required when opening an account (i.e. know-your-customer analysis), or even to optimise transaction flows and detect the fraudulent use of payment methods.

AI can also play a real role as an assistant in the provision of investment services. AI is already part of the tools used by investment firms and AI-based tools have been developed to provide financial advice, for example.

In the provision of investment services, AI plays this role in particular through robo-advisers, which automate the management of investment portfolios (in the form of advised management and/or discretionary management under mandate). These systems are based on algorithms and use machine learning techniques to personalise investment strategies according to the objectives and risk profile of clients[21]. Thanks to this personalisation, robo-advisers can provide investment services tailored to clients' individual needs, while facilitating and even democratising access to potentially sophisticated financial advice and/or strategies. This personalisation can also be seen in the criteria that investors can define upstream of any investment. In a context where ESG criteria (Environmental, Social and Governance criteria) are becoming increasingly important, this degree of personalisation meets a need. AI can therefore be offered by investment firms as a tool to help investors better align their investment decisions with their values. It should be remembered that only investment service providers may use AI or AI Systems that are essential to the provision of investment services. The mere use of AI does not make it possible to evade the application of the rules governing the exercise of this type of service (including authorisation).

Similarly, the use of AI in collective management activities involving the management of investment funds by management companies is gradually increasing, thereby changing the investment processes implemented by those managers. This was highlighted by ESMA in an analysis of the trends, risks and vulnerabilities inherent in the use of AI in fund management[22]. Although the use of AI is not yet perceived as replacing the decisive role of fund managers in many investment strategies, its use in their decision-making process is nonetheless growing. AI is considered by managers as a means of improving their operational efficiency by facilitating their decision-making.

In banking, finance, insurance and payment services, AI-powered chatbots and virtual assistants are helping investors or customers, as the case may be, to quickly access information about their accounts, ask questions about how their contracts work and receive initial guidance. Financial Institutions report that their dedicated claims processing teams can receive several thousand claims requests a week. These AI-powered chatbots can help to optimise the process. This frees the teams up to concentrate on more complex cases or those that require special attention. It remains to be seen whether this will improve efficiency and customer interaction[23], at a reduced cost to the

---

21 *IOSCO Report, op. cit. p. 26.*

22 *ESMA TRV Risk Analysis, Artificial intelligence in EU investment funds: adoption, strategies and portfolio exposures, ESMA50-43599798-9923, 25 February 2025.*

23 *ESMA, TRV Risk Monitor No. 2, 2023, p. 36: "One area of concern is the transparency and quality of consumer interactions if generative AI is deployed in tools such as virtual assistants and robo-advisers".*

service provider, in the context of the rules for handling complaints (which continue to apply irrespective of the use of AI technology alone).

Looking to the future, we can anticipate that at the stage of subscribing to financial products, the use of chatbots to answer questions from potential subscribers would make it possible to guide them towards products that correspond to their needs. In areas such as insurance and/or financial services, the use of chatbots should be fully in line with the existing regulatory framework governing the duty to provide information and advice.

In life insurance, AI can be used to analyse a large number of beneficiary clauses in order to identify, during the life of the contract, those that are unclear in their wording or are no longer up to date. Policyholders can then be invited to check and amend the clause, thus facilitating the identification of beneficiaries. When the policy terminates in the event of the policyholder's death, it can also be used to analyse mass documents in order to facilitate the search for beneficiaries and thus improve the fight against unclaimed policies.

2. The AI as a tool for providing regulated services

Today, AI is no longer limited to its traditional role of assistant. It is now becoming a true performer, capable of making decisions and implementing them autonomously.

For example, algorithmic trading relies on the use of algorithms that automatically place buy or sell orders based on predefined parameters and market signals. High-frequency trading, a subset of algorithmic trading, executes transactions at extremely high speed, often in the space of milliseconds or even nanoseconds. AI can improve the ability to anticipate market movements and even to take advantage of price fluctuations, if necessary by providing liquidity to the market.

In a similar way, the use of robo-advisers – for both investment advice and discretionary management – would enable significant or even complete automation of advisory and/or investment portfolio management activities, with arbitrage. Where applicable, transaction execution based on the use of algorithms combined with automatic data analysis by the AI System, without the intervention of the management team or an investment adviser is considered.

AI Systems could also be used to improve customer relations at the contract management stage, particularly in insurance. First of all, claims management could be simplified, with automated and virtually quasi autonomous resolution of a large proportion of the claims received from customers. Loss management could also be accelerated, whether at the declaration stage, via the analysis of all the supporting documents provided, or at the assessment stage, for example by avoiding the need for experts to travel on-site thanks to the use of image recognition (particularly in car or home insurance). The compensation stage could also be simplified by reducing the time taken to pay out insurance indemnities (particularly in the case of parametric insurance), increasingly limiting the need for human intervention.

3. AI as a tool for improving risk awareness

AI can also be used by credit institutions, investment service providers, payment institutions and electronic money institutions to meet the regulatory requirements that apply to them. For example, AI can be used as part of capital calculations to optimise the identification and management of risks to which institutions are exposed (IT, operational, fraud risks, etc.).

Banking regulation, including prudential regulation, were drafted in a technologically neutral way in order to adapt to technical and technological developments in the banking sector. As such, they encourage, to a certain extent and under certain conditions, the use of AI by banking institutions for the purposes of calculating their capital requirements. As noted by the *Autorité de contrôle prudentiel et de résolution* (**ACPR**), a number of credit institutions are already using AI to design the internal credit risk assessment models they use to calculate their capital requirements[24]. In addition, the use of AI can enable certain operational, liquidity and concentration risks to be taken into account in a more rapid, relevant and granular manner.

Today, AI can also play a role in compliance, risk management and operational efficiency within Financial Institutions. AI Systems can, where appropriate, monitor and analyse certain financial regulations, detect non-compliant (or potentially non-compliant) behaviour and assess the risks associated with different investment options. AI can also detect unusual patterns in transactional data and communications, helping to prevent fraud. Given the sheer volume of data and the speed with which stock market orders are executed, AI can be a tool for analysing data and detecting irregular behaviour or situations that may be in breach of regulations.

The automation of repetitive tasks such as data entry and report generation is now possible thanks to AI; this should improve operational efficiency, while reducing errors due to human intervention and, conversely, enabling employees to concentrate on higher value-added tasks.

In the insurance sector, the growing amount of data available to insurers enables them to assess risks much more accurately and, as a result, to adjust product pricing more precisely. According to the ACPR, "Big Data technologies combined with AI make it possible to increase the precision and scope of risk assessment and to improve risk modelling and control"[25]. For example, AI can now be used to identify areas at risk in an automatic and scalable way, by analysing weather data in real time. AI Systems are also helping to combat insurance fraud more effectively, which is itself becoming increasingly sophisticated as a result of the growing use of AI by fraudsters.

---

[24] *Henri Fraisse and Christophe Hurlin, "Modèles internes des banques pour le calcul du capital réglementaire (IRB) et intelligence artificielle", ACPR, Débats économiques et financiers No. 44, March 2024.*

[25] *ACPR, Transformation numérique dans le secteur français de l'assurance, Analyses et Synthèses no 132, 14 January 2022.*

B. The new risks associated with the use of AI

The introduction of AI into financial services brings with it a series of risks[26] that Financial Institutions need to address.

Firstly, the automation of processes involved in the provision of financial services by AI exposes Financial Institutions to increased operational risks. The gradual reduction in human intervention in certain essential tasks may lead to technical failures, algorithmic errors or even cyber attacks, potentially jeopardising the continuity of Financial Institutions' activities and raising questions about the place of human intervention in operations involving the use of AI.

Furthermore, while AI promises efficiency gains for Financial Institutions, it also presents risks for the stability of financial markets. Indeed, AI could exacerbate market volatility, in particular by amplifying already existing movements, which could create liquidity imbalances, or even a misinterpretation of certain market signals. This may lead to an excessive response to certain trends or even a response, by a Financial Institution, to its own market signals.

Another risk lies in the possible algorithmic biases that may arise, with a consequent risk of discrimination. AI Systems can generate biases depending on the quality and reliability of the data they are trained on. A model based on biased data will reproduce and even accentuate these biases. These biases can also persist, even with high-quality data, due to approximations or correlations specific to historical datasets. The criteria of gender, age or ethnic origin obviously raise questions.

Over and above algorithmic bias, there is a risk that, insofar as AI Systems are based on a multitude of data, it will become impossible to explain which data was used to provide the information sought or to make the decision concerned (the problem of the limited explainability of certain AI Systems, also known as the “black box”).

In addition, the over-representation of a small number of technology providers supplying AI solutions is likely to pose problems of concentration and dependence that could have systemic consequences[27]. The lack of competition between these providers[28], due in particular to the high cost of developing AI models, accentuates this risk. This concentration could not only leave user Financial Institutions vulnerable in the event of failure, but could also lead to homogeneous data and models, limiting the diversity of learning sources and amplifying biases. The emergence of AI providers and the potential consolidation phenomena that could arise (to enable them to achieve the critical mass necessary for their economic viability) also raises questions regarding their possible failure or bankruptcy, and the consequences that such events could have on the activities of Financial Institutions. In addition, such a concentration would entail a non-negligible risk in terms

---

[26] *See also ESMA, Public Statement on the use of Artificial Intelligence (AI) in the provision of retail investment services, 30 May 2024, ESMA35-335435667-5924, spec. no. 5 et seq.*

[27] *ESMA, Institut Louis Bachelier, The Alan Turing Institute, Leveraging Large Language Models in Finance: Pathways to Responsible Adoption, Working papers, 2025, p. 28.*

[28] *On the competitive risks upstream in the value chain, see Autorité de la concurrence, Intelligence artificielle générative: l'Autorité rend son avis sur le fonctionnement concurrentiel du secteur de l'intelligence artificielle générative, 28 June 2024.*

of cybersecurity and could also give rise to issues of sovereignty, as the major suppliers of AI Systems are not always European.

In addition, the reliability of the results generated by AI is another source of concern. Some AI models can produce errors, commonly known as "hallucinations", i.e. provide false but consistent information, which can undermine the reliability of the results. This can have serious consequences for underwriting decisions on financial products if not corrected in time.

The risk of using sensitive and protected customer data is also a major challenge associated with AI. Banking secrecy or, more generally, the professional secrecy to which Financial Institutions are bound, strictly regulates the use of customer data[29].

Automated processing of vast quantities of data, particularly via external algorithms or cloud platforms, exposes companies to increased risks of data leakage. Outsourcing and subcontracting can also lead to increased risk for financial stakeholders. However, the Regulation on digital operational resilience in the financial sector (**DORA**), No. 2022-2554 dated 14 December 2022, makes it possible to reduce these risks by incorporating security obligations relating to service providers. These risks also raise issues of compliance with the strict rules imposed by General Data Protection Regulation No. 2016-69 dated 27 April 2016 (**GDPR**).

Finally, over-reliance on algorithms, without adequate human supervision, can lead to unpredictable or inappropriate decisions, particularly in volatile market conditions. Maintaining sufficient human supervision to correct any errors and ensuring the use of AI does not entirely replace human judgement, particularly in unforeseen situations where algorithms may fail to predict appropriate outcomes, is a necessity[30].

Generally speaking, the increased use of technological levers by Financial Institutions, whatever the automated process used (and whether or not it is based on AI-related technologies), can certainly have the effect of reducing the risks relating to the human factor. It can also have the effect of increasing the operational risks resulting from the use of such technological processes: anomalies, hacking, misconfigurations, etc. A poorly calibrated or insufficiently trained AI System can therefore degrade the quality of the services offered by a Financial Institution, negatively influence its decision-making processes, and expose the institution to legal and reputational risks[31]. It would therefore seem necessary for Financial Institutions to weigh up the risks associated with human factors against those arising from an AI-based solution. This risk-based approach would enable them to determine if, when and to what extent human intervention is more appropriate than algorithmic intervention.

---

[29] *See Article L. 511-33 of the French Monetary and Financial Code (the **French Financial Code**) for credit institutions, Article L. 522-19 of the French Financial Code for payment institutions, Article L. 531-12 of the French Financial Code for investment firms and portfolio management companies.*

[30] *See this risk factor highlighted by ESMA in Public statement – on the use of Artificial Intelligence in the provision of retail investment services, 30 May 2024, ESMA35-335435667-5924.*

[31] *ESMA, Institut Louis Bachelier, The Alan Turing Institute, Leveraging Large Language Models in Finance: Pathways to Responsible Adoption, Working papers, 2025, p. 12.*

C. AI specific governance is essential

The establishment of a governance framework for the designed use case of AI by Financial Institutions is essential. This framework must include the stakeholders via an appropriate committee structure to understand the relationships with AI providers, manage the operation, ownership and processing of the system's input and output data and, *a fortiori,* establish a rigorous control framework, not forgetting the ongoing training programmes set up[32] to adapt to developments in AI.

International supervisors have identified the key governance principles of transparency, accountability, human intervention and data protection[33].

1. AI governance required for credit institutions

The use of AI must not lead credit institutions to shirk their responsibilities simply because they have used an algorithm.

The use of AI must therefore be integrated for example, into the organisation and internal control framework of credit institutions as provided for by, in particular, Articles L. 511-55 et seq. of the French Financial Code and the Order of 3 November 2014 on the internal control of undertakings in the banking, payment services and investment services sector subject to supervision by the ACPR (the **Order of 3 November 2014**), intended to transpose Articles 74 et seq. of Directive 2013/36/EU of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions (**CRD**).

These requirements relating to the development of governance for the detection, control, management and monitoring of risks are included in the assessment of a credit institution at the authorisation application stage and as part of its ongoing supervision by the authorities. The deployment of AI solutions requires appropriate governance, based in particular on specific control and monitoring of the risks generated by this technology, by the person responsible for the institution's risk management.

Article 215 of the Order of 3 November 2014 requires the validation of a business continuity management system, including IT, by the credit institution's supervisory body. Credit institutions will have to include the use of AI in their policies, procedures and controls for monitoring and controlling risks, including those relating to IT. This could involve, for example, recruiting competent people to carry out these controls and, if necessary, implementing the necessary corrective measures such as checking that the algorithm is working properly, the results it provides are consistent, and the data used is of high quality and relevant. In particular, credit institutions will need to determine the frequency and extent of algorithm checks according to the sensitivity of the use case concerned. For example, the use of AI to respond to customer queries should be able to

---

32 *Article 4 of the AI Act.*

33 *IOSCO Report, op. cit. p. 49.*

identify a “complaint” and provide the corresponding treatment such as referral to an adviser or application of the rules laid down in this area (for example time taken to process the request, etc. in accordance with Recommendation 2022-R-01 of 9 May 2022 on the treatment of complaints issued by the ACPR).

The integration of AI into the internal control framework of credit institutions remains subject to the principle of proportionality, which is generally applicable in this area. As this proportionality requirement is essentially relative, it must be assessed on an ongoing basis. A credit institution should therefore review its requirements in the light of, on the one hand, the new risks induced by AI (requiring appropriate monitoring and governance) and, on the other hand, the opportunities offered by AI in terms of risk management and business development.

In addition to these rules, new security and digital operational resilience requirements have been introduced by DORA, the aim of which is to achieve a high common level of digital operational resilience. Credit institutions will therefore also have to ensure that AI Systems falling within the scope of this regulation comply with its requirements.

The AI Systems need to be documented in internal procedures and policies and integrated into the risk and compliance review cycle. This may require, for example, the establishment of New Product Committee.

AI involves analysing a large amount of data. The quality and effectiveness of the AI Systems used by credit institutions therefore depend on the quality and up-to-date nature of this data. Using data that is too old or unsuitable would result in the introduction of biases, or even errors, into the AI Systems. It is therefore essential that banks put in place a framework for managing the data used by their algorithms, while respecting regulations on the processing of personal data and professional secrecy.

The technical nature of the algorithms also requires significant investment from credit institutions. They must train their staff, create new posts and/or call on external service providers capable of developing algorithms tailored to their needs, checking that they are working properly, updating them and making corrections where necessary. In addition to the financial investment required, credit institutions must be able to meet the requirement for their AI Systems to be explainable. The complexity of certain algorithms may therefore act as a brake on their use by credit institutions, for example if they are unable to clearly explain to regulators how these tools work and how the tools take decisions or make suggestions to the credit institution. This may increase the liability of credit institutions.

2. AI governance for payment and e-money institutions

From a general point of view, payment institutions and electronic money institutions must ensure, in the same way as credit institutions, that their governance is adapted to AI that it is used in accordance with the regulations in force. If they integrate AI, payment institutions and electronic

money institutions must comply with all the governance and internal control standards imposed on them by virtue of their authorisation[34], and in particular pursuant to the Order of 3 November 2014.

In terms of standard and approach, payment and e-money institutions must ensure that the integration of AI into their internal controls takes into account the principle of proportionality and that security and operational resilience requirements are met. The quality of the data and the explainability of the algorithms are also essential to avoid algorithmic biases and errors in the AI System.

Investment in training and human resources is needed to meet regulatory requirements. This can be a challenge for smaller establishments with limited resources. The issue of human involvement in decision-making is particularly crucial for these smaller establishments. Indeed, faced with a lack of resources and with a view to "over-efficiency", there is a potential risk of dependence on AI. This could also lead to a dependency on the company providing the service, raising questions about their ability to act in a sound and prudent manner, in accordance with their regulatory requirements.

Payment and e-money institutions, particularly those dealing with consumers, will also have to ensure that their AI algorithms and their use of them are transparent.

3. AI governance required for investment firms

Investment firms must put in place appropriate AI governance, ensuring that AI Systems are subject to regular controls, and that audit mechanisms are in place to verify their proper functioning[35].

Company directors will have to implement a decision-making and supervisory process adapted to the nature of the AI tool. Indeed, ESMA has emphasised the need for corporate officers to develop a thorough understanding of the AI tools they deploy[36]. Corporate officers should ensure that algorithms comply not only with the regulatory requirements applicable to investment firms (including in particular those resulting from the Order of 3 November 2014), but also with the principles of good conduct, ensuring that the decisions taken always serve the best interests of the client, in accordance with the requirements of Directive 2014/65/EU of 15 May 2014 on markets in financial instruments (**MiFID II**). To achieve this, investment firms are required to implement human supervisory processes and regular checks to ensure the proper functioning of AI Systems.

Supervision of automated systems needs to be addressed. The need for frequent audits and regular controls to ensure that AI Systems comply with risk management objectives and regulatory requirements thus seems well-founded. In addition, investment firms should adopt rigorous mechanisms to assess the quality and reliability of the results generated by their AI Systems, particularly when these results influence investment decisions.

---

34 *Article L. 522-6 of the French Financial Code for payment institutions and article L. 526-8 of the French Financial Code for electronic money institutions.*

35 *Article L. 533-29 of the French Financial Code .*

36 *ESMA, Public Statement on the use of Artificial Intelligence (AI) in the provision of retail investment services, 30 May 2024, ESMA35-335435667-5924, no. 10.*

Ongoing training programmes will need to be put in place and evolve in line with changes in this technique. This training will need to cover not only the use of AI tools, but also the associated risks, such as algorithmic bias and data security, etc. Well-trained staff are essential to meet the challenges posed by the integration of AI into investment services and to ensure compliance with regulatory obligations.

4. AI governance required for insurance companies

EIOPA pointed out in its Report on AI Governance Principles, published in 2021, that "The toolset provided by AI to insurance companies presents risks that will require regulatory and supervisory oversight."[37].

The purpose of this report, prepared by a group of experts, was to present their work on good governance practices for insurance undertakings without ruling out other possible approaches. In this respect, it is interesting to note that EIOPA is currently preparing an Opinion on the governance and risk management of AI in the insurance sector, in order to give a broader importance to its recommendations on AI[38].

If Article L. 354-1 of the French Insurance Code states that insurance and reinsurance undertakings must put in place a system of governance which guarantees the sound and prudent management of their business and is subject to regular internal review, the AI Act states that these rules continue to apply when AI Systems are used.

Existing legislation should indeed form the basis of any AI governance framework, but this needs to be further clarified in the context of AI.

EIOPA recalls the governance principles for ethical and trustworthy AI in the insurance sector, which are based on the following principles: the principle of proportionality, the principle of fairness and non-discrimination, the principle of transparency and explainability, the principle of human oversight, the principle of data governance and record keeping, and the principle of robustness and performance.

EIOPA has also specified that insurers' governance systems should in principle address the impact of AI in terms of the skills required of members of the board of directors (or supervisory board) and the key functions holders.

In addition, while recalling the principle of proportionality, EIOPA invites insurance companies to define, in their internal policies, the different roles and responsibilities of the staff involved in AI processes and sets out, in this respect, certain good practices in terms of governance.

---

37 *EIOPA, Artificial Intelligence governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector, 17 June 2021. This document represents the views of the members of the EIOPA Expert Advisory Group on Digital Ethics in the Insurance Sector, without necessarily representing the position of EIOPA itself on these subjects.*

38 *A consultation on this subject was launched in early 2025, with responses from stakeholders (insurers, intermediaries, unions, federations, regulators, etc.) expected by 12 May 2025; EIOPA is seeking feedback on its Opinion on Artificial Intelligence governance and risk management, 12 February 2025.*

For example, administrative, management or supervisory bodies should have a sufficient understanding of how AI is used in their respective organisations and the risks it entails.

As for the various key functions holders, their missions will necessarily evolve in line with the use of AI within the insurance company. For example, EIOPA points out that[39]:

- the compliance function should ensure that the use of AI within the entity complies with the applicable rules;
- the internal audit function should assess the quality and efficacy of algorithms and implements appropriate controls;
- the risk management function should enhance controls over the underlying data of AI Systems, in particular by ensuring that they remain free from prohibited biases;
- the actuarial function should be responsible for the controls applied to AI Systems used in the context of its missions (calculation of technical provisions, opinion on underwriting policy, etc.).

In addition, and based on Article 260 of Delegated Regulation (EU) 2015/35[40] (which provides that the risk management system should include policies on the sufficiency and quality of relevant data to be considered in the underwriting and reserving processes) EIOPA provides that insurance undertakings should implement a data governance policy that is aligned with the potential impact of AI use cases on customers or the business and that is compliant with applicable data protection legislation[41].

5. AI governance required for asset management companies

The directives and regulations specific to the asset management sector do not provide any particular framework for the risks likely to result from the use of AI.

That said, certain generally applicable means of control resulting from these regulations make it possible to provide a framework for the use of such AI technologies. These varied measures are in addition to those resulting from separate horizontal regulations (DORA, GDPR etc. – see paragraph III).

For example, in France, authorisation of management companies gives rise to a review, by the AMF, of the presentation of investment processes and other technological tools and resources used by all French management companies in the course of their management activities.

---

39 *EIOPA, consultation paper on its Opinion on Artificial Intelligence governance and risk management, 10 February 2025.*

40 *Supplementing Directive (EU) No 2009/138 on the taking-up and pursuit of the business of insurance and Reinsurance (Solvency II).*

41 *Ibid.*

As a result, the AMF already has the right to be informed both of the technological tools (including those based on AI) used by any management company, and of the resources used by the management company to monitor these tools and their configuration. The right to be informed applies both during the authorisation phase and also throughout the life of the management company (through the mandatory updating of the programme of operations via the ROSA interface as it changes)..

The AMF is thus already able to examine and, if necessary, regulate the use of AI by any French management company, so that no additional mechanism for separate approval of any AI System seems to be required in this context.

Similarly, the authorisation of a French management company already requires the company to demonstrate that it has a back-up plan so as to establish the management company's ability to manage any incidents and/or technological failures and thus ensure the continuity of its activities[42]. Such a plan must detail the concrete means envisaged by the management company to avoid any interruption of its activities, regardless of the nature of the technologies likely to be affected by any possible failure (including any technology based on AI).

These aspects are further strengthened by the developments to be included in the area of cybersecurity, to which the AMF is paying close attention. This interest is evidenced by the summaries of the various SPOT AMF inspections of cybersecurity systems (published in December 2019, April 2021 and December 2023) which identify a range of good and bad practices in this area, in terms of governance, reporting, the mapping of service providers and incident management. The aforementioned AMF doctrine also states that a management company must detail the cybersecurity measures it has put in place[43].

Finally, a new professional guide from the AFG proposes principles advocating the responsible use of AI by asset management companies, including the introduction of appropriate governance to ensure that the use of AI complies with asset management company regulations[44].

This regulatory environment must also be integrated by the management company as part of its internal control system.

D. Customer protection must be ensured

Customers will in any case be protected by the fact that organisations wishing to provide regulated services must be authorised. Regardless of the medium or means used to provide the regulated service – AI or otherwise – as long as the service provided to the customer qualifies as an

---

42 *See Article 321(25) of the AMF General Regulation (UCITS), Article 57(3) of Delegated Regulation (EU) n°231/2013 (known as the AIFM Regulation) and Article 21(3) of Delegated Regulation n°2014/65/EU (if investment services are provided) as well as AMF Position-Recommendation n°2012-19.*

43 *There will also be workshops on these topics, notably as part of the RCCI-RCSI training days in March 2023, with ANSSI in attendance.*

44 *AFG, op. cit, Guide Professionnel Principes et bonnes pratiques pour une utilisation responsable de l'AI par les sociétés de gestion, January 2025.*

investment, banking, payment or insurance service or is part of a collective management activity, authorisation will, in principle, be required and the applicable rules of good conduct must be complied with.

Over and above compliance with the rules of good conduct inherent in the provision of regulated services, when AI is used to provide these services, other issues relating to the use of this technology are highlighted.

1. Explainability and transparency are key concerns

The response provided to the customer by the algorithm must satisfy all the requirements applicable to the Financial Institution in the context of its communication with customers or potential customers (transparency, clarity, professional secrecy), but also with regard to their supervisors.

The use of AI, if properly controlled, can enable Financial Institutions to gain in efficiency and reduce their costs, but also presents a source of potential risk. Generally speaking, this means that Financial Institutions must be able to explain how the relevant model works, and explain the product of the analysis provided by the algorithm (for example, an analysis of the credit risk of a potential borrower). This requires Financial Institutions to document explainability and to define appropriate governance procedures and processes, which must be reviewed regularly[45].

In any event, the Financial Institution using AI must retain control over the decisions made using the AI tool, and must be able to deviate from it in the event of an analysis that is difficult to explain or interpret, or is even inconsistent. This requirement is likely to constitute an additional practical difficulty for the Financial Institution.

The MiFID II rules of conduct already address the issues of information and transparency for investors[46]. In application of its general obligation to put the client's interests first and its general obligation to provide information, a Financial Institution providing an investment service within the meaning of the MiFID II Directive must ensure that its clients are informed of its use of AI in the provision of its services. This transparency seems to us to be particularly important given the risks associated with the use of AI in this context. For example, a Financial Institution offering an investment advice service whose recommendations are optimised by an AI solution must inform its customers, as the risks inherent in the use of this technology may influence the advice given[47].

Similarly, AI must be the subject of clear, accurate and non-misleading communication on the part of Financial Institutions, and in particular portfolio management companies and investment services

---

45 *ESMA, Public Statement on the use of Artificial Intelligence (AI) in the provision of retail investment services, 30 May 2024, ESMA35-335435667-5924, no. 25 "By fostering transparency, implementing robust risk management practices, and compliance with legal requirements, ESMA would aim to help firms ensure they harness the potential of AI while safeguarding investors' confidence and protection".*

46 *Ibid, spec. no. 7 et seq.*

47 *ESMA, Guidance on certain aspects of the MiFID II matching requirements, ESMA35-43-3172, 3 April 2023, para 17.*

providers, in accordance with their respective regulatory obligations[48]. More specifically, this obligation should require Financial Institutions to refrain from "AI washing", i.e. presenting the use of AI in a way that is disproportionate to its actual use, so as to mislead the client/investor as to the added value or performance of the service provided. To our knowledge, no penalties have been imposed for such conduct in France, but the U.S. Securities and Exchange Commission has already fined two investment advisory firms, in early 2024, for false and misleading communications based on AI washing[49]. ESMA is keeping a close eye on this phenomenon and has published a public information document on the subject[50].

Financial Institutions should use their best efforts to ensure that the data used to drive their AI Systems is free from bias, applying, in any event, the requirements arising from the MiFID II regulation, in particular by ensuring the quality of their procedures[51].

2. Regulatory framework for the responsibilities of Financial Institutions

The chains of liability will also have to clearly integrate the use of AI. The risks incurred in this respect also need to be mitigated via agreements, contractual documentation and internal policies and procedures[52].

Given the growing role of AI in the day-to-day operations of Financial Institutions, but also more generally of any other stakeholders(e.g. suppliers, service providers, etc.), a specific contractual framework for this technology seems necessary. This is necessary not only when the service provider is specialised in providing an AI solution, but also when this technology is used by a non-specialised service provider. The introduction by Financial Institutions of a specific clause on AI could be envisaged, covering various aspects such as the transparency of algorithms, the protection of customer and confidential data, and respect for professional secrecy.

For specific relationships with AI providers, and subject to European technical regulations on the subject, additional contractual clauses are required by DORA in the context of the use of information and communication technology (**ICT**) services[53]. For example, a reversibility clause may be included to guarantee the continuity of the Financial Institution's services in the event of a change of service provider or termination of the contractual agreements; or stricter provisions concerning the processing of customer data and confidentiality, given the sensitivity of the information processed by these stakeholders.

---

48 *Article L.533-22-2-1 of the French Financial Code for portfolio management companies; Article L. 533-15 of the French Financial Code for investment service providers.*

49 *SEC v. Global Predictions, Inc, No. 3-21894 (SEC, March 18, 2024); SEC v. Delphia (USA) Inc, No. 3-21894 (Sec, March 18, 2024).*

50 *ESMA, Using Artificial Intelligence for Investing: What you should consider, 2025.*

51 *ESMA, op. cit. public statement on the use of artificial intelligence (AI): "Investment firms should implement rigorous quality assurance processes for their AI tools.*
This should include thorough testing of algorithms and their outcomes for accuracy, fairness, and reliability in various market scenarios."

52 *See paragraph IV of this Report.*

53 *Article 30 of DORA.*

E. Prudential regulation is also essential in regulating the use of AI

1. Prudential supervision of the use of AI to provide financial services

The use of AI Systems by Financial Institutions is likely to have an impact on capital requirements for operational risk, as set out in the prudential framework applicable to credit institutions (consisting of the Directive on the prudential supervision of credit institutions (CRD) and Regulation (EU) 575/2013 of 26 June 2013 on the prudential requirements for credit institutions (**CRR**)), that applicable to investment firms (consisting of Directive (EU) 2019/2034 of 27 November 2019 on the prudential supervision of investment firms (**IFD**) and Regulation (EU) 2019/2033 of 27 November 2019 on the prudential requirements applicable to investment firms (**IFR**)) as well as, with regard to insurance companies, Solvency II and Delegated Regulation (EU) 2015/35, which supplements it.

The use of AI must therefore be integrated into the systems for assessing the risks incurred by Financial Institutions, like all the risks associated with the use of technology. The use of AI Systems is already supervised by the competent authorities in terms of the operational risks likely to arise.

2. Regulation of the use of AI for prudential purposes

Prudential regulation is considered, as a whole, to be technologically neutral. It does not, in principle, prohibit, impose, favour or penalise the use of one technology rather than another, provided that the technology used does not give rise to new risks that are not precisely identified and controlled[54]. Thus, in principle, it does not prevent Financial Institutions from using AI to meet the prudential requirements applicable to them, whether in terms of internal control and compliance or for determining their capital requirements. AI can indeed prove to be a particularly useful tool to enable Financial Institutions (first and foremost credit institutions) to cope with the continuous increase and growing complexity of prudential regulations.

The rules governing internal control and compliance do not exclude, *a priori*, the possibility for regulated Financial Institutions to use AI as part of the overall internal control and compliance system they are putting in place[55]. However, as the ACPR points out, the internal control rules were drafted "in the view that controls were carried out by humans"[56]. Permanent controls and periodic controls must in fact be carried out by natural persons, whether they are dedicated to these controls or otherwise engaged in operational activities, as the case may be. This requirement for human

---

[54] *According to the European Central Bank (ECB), "the EU financial services regulatory framework is already broadly technology neutral" (ESCB/European banking supervision response to the European Commission's public consultation on a new digital finance strategy for Europe/FinTech action plan, August 2020, p. 17). This technology-neutral approach is also implemented by the ECB in the context of banking supervision ("The ECB follows a technology-neutral approach to its areas of competence, including banking supervision and the oversight of payment systems, in accordance with the SSM Regulation and the Treaty on the Functioning of the European Union" or "The ECB supports a technology-neutral approach to regulation, supervision and oversight" (same ESCB/European banking supervision response, p. 11)). The position of the European banking regulator in this respect is constant and regularly reaffirmed: "In my view, supervisors should essentially be technology-neutral" (Panel remarks by Andrea Enria, Chair of the Supervisory Board of the European Central Bank, at the Financial Stability Institute 20th anniversary conference, Basel, 12 March 2019).*

[55] *Nothing in the Order of 3 November 2014 prohibits the use of AI in the internal control arrangements put in place by Financial Institutions falling within its scope.*

[56] *ACPR, Discussion paper, Artificial Intelligence – Challenges for the financial sector, December 2018, paragraph 3.1.3 p. 22.*

involvement does not rule out the use of AI. That said, it tends to confine AI to the role of human assistant, or at least to minimise its use as a performer. The use of AI in internal control and compliance thus calls for a careful review of the applicable requirements, so as to determine the part of the controls that can be carried out using AI Systems and the part that must imperatively be entrusted to humans in order to comply with the applicable requirements.

Prudential regulation applicable to credit institutions (i.e. CRR/CRD) does not oppose the use of AI to meet the requirements, where this appears possible. On the contrary, it encourages, to a certain extent and under certain conditions, the use of AI by credit institutions for the purposes of calculating capital requirements. This use, via the models developed by institutions using internal model approaches to comply with prudential requirements, is however subject to very strict supervision.

Credit institutions are in fact required to comply with the requirements laid down by CRR for internal model approaches, which can raise difficulties and a certain level of complexity for complex AI Systems (known as "black boxes"), particularly to meet the interpretability and explainability requirements laid down by CRR. Recent publications by the supervisory authorities (in particular the European Banking Authority (**EBA**) and the ACPR) indicate that the supervisors are aware of the difficulty, but also of the stakes represented by the use of AI for credit institutions (due in particular to its potential for improving predictive capacities for assessing credit risk). This is why the supervisors have moved towards a framework based on principle-based recommendations intended to refine the application of the CRR regulations governing internal models in cases where AI is used.

The EBA has drawn up a series of recommendations[57], calling on institutions to ensure that the AI-based models they use are understood by their users at all required levels, do not exceed the degree of complexity necessary for their purpose, are interpretable and properly documented, are regularly monitored and updated, and involve human control. Regarding this latter recommendation, the EBA specifies that human involved in the control of AI-based models must be able to understand the assumptions and behaviour of the model in relation to the predictions it makes (both at the development and application stages).

The recent amendments made to the CRR by the so-called CRR3 regulation[58] (in force since 1 January 2025) do not call into question the possibility that in-scope institutions may use AI for the purposes of determining their capital requirements[59]. However, the amendments could, to some extent given their objective (i.e. to reduce the arbitrage possibilities offered by the use of internal

---

[57] *EBA, Machine Learning for IRB models – Follow-up report from the consultation on the discussion paper on machine learning for IRB models, (EBA/REP/2023/28),4 August 2023.*

[58] *Regulation (EU) 2024/1623 of the European Parliament and of the Council of 31 May 2024 amending the CRR as regards requirements for credit risk, credit valuation adjustment risk, operational risk, market risk and the output floor (**CRR3**).*

[59] *Note in this respect the introduction of a definition of model risk by CRR3 (Article 4(1)52b of CRR) which, by its generality, makes it possible to capture the various forms of AI, and as such seems to confirm the principled non objection to recourse to AI for the purposes of satisfying the prudential requirements laid down by CRR/CRD (CRD already included, since its adoption on 26 June 2013, a rather similar flexible definition of model risk capable of capturing AI in its various forms – transposed in Article 10(aa) of the Order of 3 November 2014).*

model approaches), make the use of AI in this area less attractive for certain credit institutions[60] or lead to rethinking/redirecting AI use in this context[61]. In this respect, the new forms of AI in the pipeline (in particular the so-called natively interpretable AI Systems[62]) could make it easier to comply with regulatory requirements when using AI to determine capital requirements, by considerably reducing interpretability difficulties (i.e. thanks to the reduction or even elimination of the "black box" effect) without losing predictive performance[63].

In any case, whether for the determination of capital requirements for credit risk, counterparty credit risk, operational risk or market risk, the use of internal models – and therefore AI – for prudential purposes is systematically subject to prior authorisation by the competent authorities. This authorisation, made necessary by the fact that the use of internal approaches allows credit institutions to deviate from the standard requirements so as to define their own methodology for calculating regulatory capital, is only granted once the competent authorities have been able to verify that the envisaged model meets all the quantitative and qualitative requirements set out in the regulations (in this case essentially CRD/CRR and the Order of 3 November 2014). This includes notably the establishment of sound governance for the management of model-related risk (i.e. a clear division of responsibilities, and clear policies and procedures for detection, management, monitoring, reporting, etc).

Logically, and for the same reasons, changes to internal models implemented by credit institutions are also subject to authorisation by the competent authorities. Furthermore, in the event of non-compliance with the required conditions or shortcomings in the accuracy of the model, the competent authorities are empowered to revoke the authorisation to use the model or to impose appropriate improvement measures within a short period of time.

The use of AI is also permitted for the purposes of calculating capital requirements for investment firms. This approach is in line with the regime under the IFD/IFR framework for capital requirements, which allows investment firms to use internal models to calculate the K-factor reflecting net position risk (K-NPR), in a manner aligned with the prudential framework for credit institutions (CRD/CRR). This use of AI for prudential purposes is likely to remain marginal for investment firms insofar as it will only affect firms dealing on own account that opt to use internal models to calculate K-NPR (instead of the Standardised Approach or the Alternative Standardised Approach). Where applicable, this use of AI will, as for credit institutions, be subject to prior authorisation by the

---

60 *The changes introduced by CRR3 impose additional constraints on the use of internal models to determine their capital requirements (notably by requiring the use of the standardised approach for certain exposures and by introducing minimum values ("input floors") for credit institutions' own estimates of risk parameters, whether probability of default, LGD or conversion factors, as well as an overall capital floor ("output floor")).*

61 *For example, CRR3 refines the Standardised Approach for credit risk and makes it more risk-sensitive, as well as it makes the Alternative Internal Models Approach (A-IMA) binding, alongside the Alternative Standardised Approach (A-SA) and the Simplified Standardised Approach for market risk.*

62 *Such systems make it possible to link the model's predictions to the variables used by the model. This is the case, for example, with models based on logistic regression or a decision tree (as opposed to "random forest" models, which are virtually impossible to interpret).*

63 *On this proposal, see in particular the publication entitled "Modèles internes des banques pour le calcul du capital réglementaire (IRB) et intelligence artificielle" by Henri Fraisse and Christophe Hurlin, published in Débats économiques et financiers (No. 44) by the ACPR and the Banque de France in March 2024.*

competent authorities, which will ensure that the necessary quantitative and qualitative requirements are met, *ab initio*, and then as part of regular monitoring.

Similarly, insurance companies subject to Solvency II may use AI to calculate their Solvency Capital Requirement when they perform this calculation using an internal model (full or partial), provided that this internal model has been approved by the supervisory authorities [64]. The use that insurance companies can make of AI for the purposes of determining their capital requirements when they use internal models is therefore not only governed by regulation (which imposes numerous requirements including with regard to the data used and the explainability of the models), but is also subject to ongoing supervision by the ACPR, which may, in the event of non-compliance with the applicable requirements, impose additional capital requirements or even withdraw the authorisation granted.

Other types of Financial Institutions, when required to determine all or part of their capital requirements based on (for instance) the risks they incur, could also potentially make use of AI to carry out this determination, provided that the applicable regulations do not prevent this. Where applicable, the use of AI should not generate unidentified or uncontrolled risks and should be carried out in compliance with all the regulations applicable to the relevant Financial Institution. For example, depending on the risks they bear[65], AI could be used by portfolio management companies (authorised under the AIFM Directive) to determine the additional capital requirements they must meet to cover the possible risks of their professional liability being called into question when managing AIFs+.

The recourse to AI by Financial Institutions for the purpose of satisfying prudential regulatory requirements must be integrated into their systems for assessing any potential risks, as is the case for any other risks linked to the use of all other technologies (just as when AI is used for the purposes of providing regulated services to customers, see on this point in particular paragraph B above).

---

64 *Articles 112 and 113 of Solvency II, as transposed into Articles L. 352-1 et seq. and R. 352-2 et seq. of the French Insurance Code, and supplemented by Articles 228 et seq. of Delegated Regulation (EU) 2015/35.*

65 *In accordance with Article 317(2), IV of the AMF General Regulation, the additional own funds of a portfolio management company authorised to manage AIFs must be "of an amount sufficient to cover potential liability risks arising from professional negligence". The rate of 0.01% referred to in paragraph 2 of Article 14 of Regulation (EU) 231/2013 being a minimum rate, "the rate actually retained by the asset management company must result from its own analysis of the risks it faces and how they are quantified. The amount defined in this way must correspond to the risks borne and must be of a sufficient level to allow any necessary remedial measures to be taken" (AMF Position-Recommendation – DOC-2012-19 – Programme of operations guide for portfolio management companies and self-managed collective investment, updated to 18 December 2024, p. 57). The use of AI to estimate the additional capital required in this respect (in particular for the operational risks borne by the portfolio management company) seems conceivable, although this is not a case of use that has already been identified.*

F. The framework for the protection of customer data must incorporate the use of AI

Banking secrecy is not one of the provisions subject to harmonisation at European level. Under French law, in principle, members of the supervisory body of a regulated institution[66] and any person who in any capacity participates in the management or administration of such an institution or who is employed by it, are bound by professional secrecy. Exemptions are provided for, in particular with regard to certain authorities (ACPR, Banque de France, judicial authorities in criminal proceedings, etc.) or in certain cases (sales and transfers of contracts, acquisitions of holdings or control, contracts for the provision of services, etc.), subject to certain conditions[67]. In any event, the beneficiary of the protection has the right to waive it.

Not only is French banking secrecy relatively strict compared with other EU jurisdictions, it also raises a number of questions, as demonstrated by case law: are the clients of an institution subject to the confidentiality obligation the only beneficiaries of the secrecy? Does the obligation of confidentiality survive the end of the business relationship? What information should be considered as covered by confidentiality? What form should the beneficiary's waiver take? Is the list of persons to whom confidentiality is not enforceable comprehensive. In addition to these questions, there is also the question of the relationship between the provisions relating to banking secrecy and those relating to professional secrecy under the Criminal Code, of which banking secrecy would be an offshoot.

These questions obviously arise in the context of the adoption of AI by Financial Institutions – more so as data is a key element in the effectiveness of algorithms. It is therefore crucial for Financial Institutions to determine which data they can use and, if applicable, to what extent, in order to 'feed' the AI Systems they use. Indeed, the data considered to be covered by professional secrecy may be prohibited by the Financial Institution in certain AI Systems, depending on their purpose and the people likely to have access to them, particularly when the latter are designed by a third party (thus raising issues of confidentiality and control of the information processed). As a result, in the event of collaboration with external partners, Financial Institutions will have to be able to demonstrate that the data used does not leave their perimeter, in order to guarantee confidentiality.

The stakes are higher in the European context: as the AI Act applies directly within the EU, Financial Institutions in jurisdictions other than France could benefit from a competitive advantage if they can use data considered confidential under French law in their AI Systems, or at least more easily

---

66 *Article L. 511-33 of the French Financial Code for credit institutions and finance companies; Article L. 522-19- of the French Financial Code for payment institutions; Article L. 526-35 of the French Financial Code for electronic money institutions; Article L. 531-12 of the French Financial Code for investment firms and portfolio management companies; Article L. 421-8 of the French Financial Code for market undertakings; Article L. 440-8 of the French Financial Code for clearing houses; etc.*

67 *Article L. 511-33 of the French Financial Code for credit institutions and finance companies; Article. L. 522-19 of the French Financial Code for payment institutions; Article L. 526-35 of the French Financial Code for electronic money institutions; Article L. 531-12 of the French Financial Code for investment firms and portfolio management companies; Article L. 440-10 of the French Financial Code for clearing houses; etc.*

than French Financial Institutions. Their AI Systems could then run on more accurate, up-to-date, relevant data, etc., and consequently produce more accurate analyses than systems fed with "filtered" data. For example, the waiver of banking secrecy by a Financial Institution's beneficiary would appear validly provided for in general conditions in certain European jurisdictions, whereas French requirements would appear to exclude it, with consent having to be given on a "case-by-case" basis.

We will not be addressing the issue of legal exceptions to banking secrecy mentioned above (which have already been researched and a report produced by the HCJP), but we would present an initial grid for analysing compliance with banking secrecy provisions within the context of AI Systems by Financial Institutions subject to these AI System provisions.

Financial Institutions could not make use of their customers' data by means of AI Systems offered to the general public in compliance with the aforementioned provisions. The conditions of use of these systems are, in fact, explicit with regard to the re-use of user data, which therefore constitutes communication to third parties requiring the express consent of the customers concerned.

However, it would appear that the use of AI Systems deployed within the framework of secure IT infrastructures (either on the institution's own servers, or via outsourced environments that are not pooled and offer satisfactory security and confidentiality commitments) would not constitute disclosure to third parties of protected information, subject to the provisions applicable to banking secrecy.

The system for protecting confidential data applicable to Financial Institutions subject to regulation in France, as provided for by the French Financial Code, does not therefore appear to constitute an obstacle, in principle, to the deployment of AI Systems, subject to the implementation of certain safeguards that Financial Institutions have in place. This is true of technical as well as organisational and contractual measures, particularly when sensitive data is shared/transferred to feed a third-party AI System. From this perspective, AI for Financial Institutions would be a technical novelty to be used in accordance with the existing regulatory framework, without there being any need to reserve a specific treatment for it.

G. Supervision of AI through the use of third-party service providers

1. Outsourcing regulations

As the ACPR pointed out in a June 2020 discussion paper[68], Financial Institutions use different types of third-party service providers to develop their AI: the design and development may be entrusted to an external company, and the hosting and operation of AI services may be outsourced to a traditional hosting provider or a *cloud* services solution provider[69].

---

[68] *ACPR, Gouvernance des algorithmes de l'intelligence artificielle dans le secteur financier, discussion paper, June 2020.*

[69] *The working group refers to the work carried out by the HCJP in its report on the banking cloud dated May 2021; HCJP, Rapport sur le cloud bancaire: état des lieux et propositions, Mai 2021.*

In this respect, the ACPR stresses that the implementation of outsourcing implies providing for the reversibility of outsourced AI solutions and must be preceded by an *ex-ante* risk analysis. The Financial Institution must also be able to access the source code and models, and offer the same guarantee to the supervisor in order to enable an audit covering the systems, software code and data.

In light of Articles 231 et seq. of the Order of 3 November 2014 and the EBA's guidance on outsourcing[70], the question arises as to whether the contractual arrangements with these external providers should be classified as outsourced essential services (**OES**), or the "Provision of services or other essential or important operational tasks", as expressed in the Order of 3 November 2014[71].

In the insurance sector, the ACPR could qualify the outsourcing of AI solutions as the outsourcing of a critical or important operational activity, within the meaning of Articles L. 354-3 and R. 354-7 of the French Insurance Code, which require prior notification to the ACPR via a dedicated form (*see* Instruction 2020-I-09, recently amended to include outsourcing to a cloud service provider).In its *Factsheet* on the regulatory framework for AI in insurance published on 15 July 2024, EIOPA points out that "using third-party AI systems could be considered outsourcing under Solvency II"[72], with all the consequences that this implies (particularly in terms of liability, etc.). In such a case, the insurer and the ACPR will have effective access to all information relating to the outsourced functions and activities, including the possibility of carrying out on-site inspections at the premises of the service provider (Article 274(4) of Delegated Regulation (EU) 2015/35 supplementing Solvency II).

It is specified that insurance undertakings shall refrain from outsourcing critical or important operational functions or activities where such outsourcing would be likely to be detrimental to the continued provision of a satisfactory level of service to insureds, policyholders and beneficiaries of contracts and reinsured undertakings.

Outsourcing arrangements for Financial Institutions can prove complex to implement when faced with highly concentrated AI providers who refuse any form of control or even audit of their systems by supervisors.

---

70 *EBA, Guidelines on outsourcing arrangements, EBA/GL/2019/02, 25 February 2019.*

71 *As a reminder, Article 10, r) of the Order of 3 November 2014 defines the provision of services or other essential or significant operational tasks as "(i) banking operations within the meaning of Article L. 311(1) of the Monetary and Financial Code, the issuance and management of electronic money within the meaning of Article L. 315(1) of the same code, payment services within the meaning of II of article L. 314(1) of the same code and investment services within the meaning of article L. 321(1) of the same code, for which the entity has been authorised; (ii) the related transactions referred to in 1, 2, 3, 7 and 8 of I of article L. 311(2),(1),(2), (5) and (6) of article L. 321(2) and articles L. 522(2) and L. 526(2) of the Monetary and Financial Code; (iii) services directly involved in the execution of the transactions or services mentioned in the first two indents; (iv) or any provision of services where an anomaly or failure in its performance is likely to seriously impair the ability of the entity to comply on a permanent basis with the conditions and obligations of its authorisation and those relating to the performance of its business, its financial performance or the continuity of its services and activities".*
The following are expressly excluded: "(i) the provision to the relevant entity of consultancy and other services not forming part of the activities covered by its authorisation or license, including the provision of legal advice, staff training, invoicing services and the security of the business's premises and staff; and (ii) the purchase of standard services, including services providing market information or price data feeds".

72 *EIOPA, Regulatory framework applicable to AI systems in the insurance sector, July 2024.*

Outsourcing required by the use of AI may entail significant regulatory issues for asset management companies. In theory, there are several possible approaches, and their relevance is likely to change as new AI-based technologies emerge and/or mature:

- service providers may simply offer AI solutions that fit into the decision-making process (and/or other procedures) implemented by management companies, in which case various means of control already exist to cover this situation (see outsourcing regime below, or the description of the technical means implemented by the management company and controlled by the AMF at the time of its authorisation); or

- where appropriate, service providers could also offer genuine "management tools" that AI could potentially make autonomous and self-sufficient to a certain extent. In such a scenario (which we do not believe is currently the case[73]) service providers would offer technological solutions based on AI which already incorporate a decision-making process relating to management activities on certain strategies. This hypothesis would then raise the question of the supervision of such service providers, but also of the role of the management company, which could thus be relegated to the rank of a mere recording room for decisions resulting from the AI software and developed by the AI service provider. In the absence of any real parameterisation of this tool by the management company and/or integration of the relevant data necessary for its effective operation, the "discretionary" role of the management company could be called into question, or even transferred to the service provider offering such turnkey tools, the latter then becoming the true project manager of the management strategy thus envisaged. In the absence of authorisation as a portfolio management company (or equivalent authorisation in a third country) for such a third-party service provider, such a scenario could also be assimilated to a form of circumvention of the rules applicable to the monopoly on asset management services due to the use of a technology which would be contrary to the principle of technological neutrality of the regulations.

In other words, the more advanced and autonomous the technological solutions offered by AI service providers, the greater the stakes involved in using such service providers and the more likely they are to involve outsourcing schemes for essential services (see below). This is already being interpreted widely in practice, but also potentially of qualification of a management activity at the level of the service providers themselves, even though the latter do not *a priori* have any regulated status in asset management (see issues of authorisation and risks of circumvention mentioned above). Demonstrating the discretionary nature of the prerogatives exercised by management companies, in particular through the configuration of such AI tools, but also through maintaining control over their operation, will therefore prove to be a key element in maintaining the management discretion inherent in their status.

---

[73] *ESMA TRV Risk Analysis, Artificial intelligence in EU investment funds: adoption, strategies and portfolio exposures, ESMA50-43599798-9923, 25 February 2025.*

In addition to the human intervention required for automated processing, the AI of a third-party service provider used for the provision of a regulated service could call into question the Financial Institution's authorisation but also make the service provider subject to the authorisation requirements of Financial Institutions.

2. Towards a regulatory framework for Big Tech

In an October 2024 publication[74], the ACPR envisages a new prudential framework for technology companies, commonly known as Big Techs.

As noted in the ACPR publication, DORA has introduced a new framework in the European Union for Financial Institutions' use of ICT (including potentially AI solutions – see paragraph 1 above) and their service providers. In this respect, DORA introduces a specific supervisory framework for ICT service providers considered critical for Financial Institutions[75]. The aim of this framework is to provide an initial regulatory response to the growing involvement of certain technology companies within the banking and financial sector.

More broadly, however, the ACPR points out that the hitherto limited role of Big Techs in the financial industry continues to grow, driven by "technological innovations that give them a significant comparative advantage"[76]. Among the competitive advantages of these stakeholders, the French regulator points to their "capacity to collect, analyse and exploit large-scale data, coupled with their mastery of advanced artificial intelligence (AI) and machine learning technologies"[77], which potentially enables them to "offer presumably more adapted services, based on the identification of customer needs, and thus capture market share and generate new sources of revenue"[78]. Given this growing importance and the associated risks, the ACPR is considering the need to change the framework applicable to these stakeholders.

This initiative is particularly based on the observation that European regulations do not provide for consolidated supervision of groups of payment or electronic money institutions. This situation prevents the supervisory authorities from developing an comprehensive view of the risks borne by such groups, in a context where the growing use of AI Systems could give rise to Big Techs. To address this shortcoming, a consolidated supervision requirement could be introduced into the Payment Services Directive (**PSD**) whenever a financial group that is not already subject to prudential supervision under the CRR has at least one payment or electronic money institution. Such supervision could be based on the introduction of the concept of a payment holding company, similar to that of a financial holding company.

---

74 *ACPR, Le développement des big techs dans le secteur financier: quels risques, quelles réponses réglementaires, October 2024.*

75 *Articles 31 et seq. of DORA.*

76 *ACPR, op. cit, Le développement des big techs dans le secteur financier: quels risques, quelles réponses réglementaires, p. 1.*

77 *Ibid.*

78 *Ibid.*

Beyond the consolidation aspects, other enhancements to the PSD framework could also be justified in the context of the development of Big Tech. These could include the application of additional capital requirements ("pillar II") and the introduction of liquidity requirements for payment and e-money institutions, as well as the supervision of X-Pay-type technical services (e.g. Apple Pay, Google Pay) and the provision of white-label services, notably by imposing greater transparency and measures to ensure the protection of customer funds.

The ACPR is also considering requiring mixed-activity groups to amalgamate their significant financial and ancillary activities within a dedicated structure, to enable consolidated supervision and, where appropriate, where the combined financial activities of the group present risks similar to those of a credit institution, the application of banking rules to the entire financial sub-group[79]. The ACPR notes that the complex structure of large technology conglomerates and, more generally, large mixed-activity groups, combined with the preponderance of non-financial activities, may prevent consolidated supervision under the current rules. The establishment of such a holding company would enable supervisors to gain a better understanding of the activities of each group, their interconnection with non-financial activities and, consequently, their systemic nature.

Lastly, the ACPR plans to make it possible for the supervisor to impose the application of banking prudential rules to the whole of a financial sub-group, where the combined financial activities of the group present risks similar in nature to those of a credit institution or where a risk to financial stability is identified as insufficiently covered by the applicable individual requirements, in order to take account of ongoing technological innovation.

[79] *Ibid.*

II. The AI Act for Financial Institutions

Financial Institutions were using AI tools long before the AI Act was introduced. These tools, some of which have been in place for years, will now have to adjust to the new regulations. On top of this, AIS providers will also have to maintain their systems in compliance throughout the period of use, which implies continuous monitoring and alert mechanisms. Faced with these new challenges, Financial Institutions, like all those to whom the AI Act applies, are benefiting from a staggered implementation of the AI Act, which will enable the authorities to educate the relevant stakeholders. For example, the provisions of the AI Act will only become applicable in their entirety starting from 2nd August 2026 (with the exception of the rules relating to high-risk AIS in Annex 1)[80].

In order to anticipate the impact of the AI Act, it is essential for financial stakeholders to understand precisely the scope of application for this industry, the content of the main obligations, and the role that would be devolved in this area to the sectoral supervisory authorities.

A. Clarifying the scope of AI in the financial sectors

The purpose of the AI Act is to regulate AI Systems with the primary aim of safeguarding the rights enshrined in the Charter of Fundamental Rights of the European Union. It therefore seems clear that this regulation should not apply to all AIS in the same way, but should instead aim to regulate AIS that may pose the greatest risks to fundamental rights.

Similarly, this new regulation is intended to define a general framework that is compatible with future technological developments. It has had to define the technical solutions it governs without relying solely on practices and techniques developed to date. To this end, the AI Act definition adopts the general approach of the OECD, and sets out precise criteria for characterising AIS, without targeting specific methods or techniques.

Financial Institutions will then be obliged to carry out case-by-case analyses to determine whether or not their AI solutions fall within the scope of the AI Act.

It should be noted at the outset that the AI Act also regulates the supply of general-purpose AI models[81]. However, insofar as Financial Institutions should, *a priori*, rarely be qualified as providers of such models, the provisions of the AI Act relating thereto will not be analysed in detail in this Report.

1. A definition focused on output generation

The AI Act adopts a specific definition of AI which aims to distinguish technologies capable of generating output from the input they receive from other types of software systems. The other fundamental elements of an AI System are: (i) the level of autonomy with which it operates (allowing

80 *CNIL, Entrée en vigueur du règlement européen sur l'AI: les premières questions-réponses de la CNIL, 12 July 2024.*

81 *Articles 51 et seq. of the AI Act.*

it to benefit from a "degree of independence of actions from human involvement and of capabilities to operate without human intervention") and (ii) its possible adaptability after deployment linked "to self-learning capabilities, allowing the system to change while in use[82]"[83]. This excludes simple prediction systems. For example, some automated systems for forecasting future share prices rely on methods that are too simplistic to be considered by the AI Act, in particular because of their limited ability to analyse trends and adjust their results autonomously[84]. The same reasoning applies to statistical estimation systems which predict, for example, an average customer service response time based on past data[85]. In the end, these two models are not sufficiently autonomous nor adaptable to be regulated.

The above-mentioned Commission guidelines also recall the other qualification criteria to be taken into account in characterising AI Systems within the meaning of the AI Act, namely: the automated nature of the system, the implicit or explicit objectives it pursues, the capacity for inference, the nature of these outputs and their capacity to influence their environment[86].

These guidelines specify the characteristics that systems must meet in order to be subject to the AI Act, with the Commission emphasising not only the broad spectrum of solutions that can potentially be captured, but also the need for a case-by-case and *in concreto* analysis to determine whether or not the AI Act is applicable. This assessment is particularly significant for financial stakeholders who had largely integrated this type of solution long before the AI Act was adopted. Ultimately, this definition centred on output generation provides an essential reference framework for determining which AI solutions fall within the scope of the AI Act, while clarifying the responsibilities of the stakeholders in these sectors.

2. Extraterritorial application

The territorial application of the AI Act is a fundamental feature of the regulation.

The AI Act applies to any AI System or model used in the European Union, regardless of where it was developed or provided. This means that foreign AI Systems producing outputs used in the EU will be subject to the requirements of the AI Act[87]. This will be the case, for example, of a French customer purchasing an AI System from a Canadian provider but using the AIS for its internal operations in France, or a company in China using an AIS to filter CVs and sending the filtered results to its Luxembourg subsidiary, which intends to use the AIS results for its activities in the European Union.

---

82 *Recital 12 of the AI Act.*

83 *These technical terms are to be clarified in a forthcoming publication by the European Commission following the results of the consultation on guidelines for the definition of prohibited SIA and AI. See European Commission releases analysis of stakeholder feedback on AI definitions and prohibited practices public consultations, 12 May 2025.*

84 *European Commission, Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), guidelines, 6 February 2025, para 50.*

85 *Ibid, para 51.*

86 *Ibid.*

87 *Article 2(1) of the AI Act.*

While the AI Act explicitly provides for its application to providers and deployers of AI Systems established or located in a third country where the output produced by the AI System is used in the Union[88], Recital 22 seems to introduce a criterion of intent. It specifies that the scope of the AI Act should include providers and deployers established in a third country, insofar as "the output produced by these systems is intended to be used in the Union". This provision could therefore justify third-country stakeholder not being subject to the AI Act, even if they are linked to an AI System whose outputs are used in the EU, if these systems were not intended for this purpose. However, to ensure full legal certainty for stakeholder, in the absence of clarification in the binding provisions of the AI Act, such a restriction of geographical scope based on the criterion of intent could be provided by the Commission on the criteria for extraterritorial application of the AI Act.

The extraterritorial nature of the AI Act could also complicate the use of solutions developed in jurisdictions not aligned with European standards, raising challenges for Financial Institutions wishing to adopt innovative AI Systems from abroad. These constraints will require contractual adjustments as well as thorough due diligence mechanisms to ensure compliance throughout the supply chain. In this regard, the European Commission has recently published model standard contractual clauses for AI procurement by public bodies. Although aimed at public bodies purchasing AI Systems developed or to be developed by an external provider, these buyer-friendly clauses can also be a source of inspiration for Financial Institutions[89].

3. Risk-based classification

The approach adopted by the AI Act is risk-based. The AI Act therefore provides for a progressive regime of obligations according to the degree of risk posed by the AI System to health, safety and fundamental rights.

AI Systems used by Financial Institutions will be categorised according to whether the risk is unacceptable, high, limited or minimal. A major mapping exercise of the AI solutions integrated into the organisations of Financial Institutions will have to be carried out to distinguish the levels of risk and the specific requirements applicable to them, depending on the uses considered.

(a) Unacceptable risk AI Systems

The AI Act contains a restrictive list of AI Systems that are prohibited because they pose a risk deemed unacceptable due to their nature[90].

There do not appear to be any specific cases of use in the banking and financial sector within this category. However, the implementation of certain categories of systems may prove tricky for the financial industry. In particular, the AI Act prohibits AI Systems that exploit potential vulnerabilities

88 *Article 2 of the AI Act.*
89 *European Commission, Procurement of AI, Updated EU AI model contractual clauses, 5 March 2025.*
90 *Article 5 of the AI Act.*

due to a person's age, disability or specific social or economic circumstances in a way that is reasonably likely to cause significant harm to that person[91].

In this respect, the European Commission guidelines published in February 2025[92] specify that AI Systems used to provide banking services, such as mortgages and loans, using the age or specific socio-economic situation of the customer, in compliance with EU legislation, do not constitute a prohibited practice "when they are designed to protect and support people identified as vulnerable due to their age, disability or specific socio-economic circumstances and are beneficial to those groups, also contributing to fairer and more sustainable financial services for those groups" .

On the other hand, an AI System that would target the elderly with insurance offers by exploiting their reduced cognitive capacity could fall within the scope of unacceptable practices prohibited by the AI Act[93].

Similarly, another practice prohibited by the AI Act concerns AI Systems based on collection of data on social behaviour or personal characteristics used for purposes unconnected with the context in which the data was collected (also known as "social scoring"), for example in the context of certain financial services. The integration of such data by an AI System could fall into the category of AI Systems with unacceptable risk if the system derives "prejudicial or unfavourable processing" in a context other than that in which the data was collected or if such processing is "prejudicial or unfavourable" in a disproportionate or unjustified manner[94]. While the AI Act points out that this provision is not intended to "affect lawful evaluation practices of natural persons that are carried out for a specific purpose in accordance with Union and national law"[95], the scope of the cases of use that will henceforth be prohibited is not precisely defined in the text. Clarification of the assessment of these situations referred to in articles 5(1)(c)(i) and (ii) of the AI Act would provide better visibility of the cases of use in the banking and financial sector that do or do not fall within their scope.

In this respect, the above-mentioned Commission guidelines provide useful clarifications. They indicate, for example, that the following should be prohibited on this basis:

- the use by an insurance company of an AI System recommending to refuse a contract or to set higher life insurance premiums for a person for whom the said company would have collected information on spendings and other financial information not related to the determination of the eligibility of this candidate for life insurance and the determination of the premium for this insurance[96]; and

---

91 *Article 5(1)(b) of the AI Act.*

92 *European Commission, Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), 4 February 2025, para 133.*

93 *Ibid, para 117.*

94 *Article 5(1)(c)(i) and (ii) of the AI Act.*

95 *Recital 31 of the AI Act.*

96 *European Commission, op. cit, Guidelines on prohibited artificial intelligence practices, para 170.*

– the use by credit institutions of an AI System to determine the creditworthiness of individuals and access to home loans on the basis of unrelated personal characteristics[97].

On the other hand, this provision of the AI Act does not call into question AI Systems enabling the evaluation of individuals for specific legitimate purposes resulting in potentially harmful or unfavourable processing if this is justified and proportionate and data from related social contexts are used[98].

Typically, information collected through telematic devices showing that a driver is not following safe driving practices could be used by the insurer to increase the premium for that policyholder because of the higher risk of an accident, provided that the increase in premium is proportionate to the driver's risky behaviour.

Despite the European Commission's clarifications, the use cases likely to be considered prohibited remain very broadly defined. A more restrictive approach to the provisions of the AI Act would not significantly hamper the ability of Financial Institutions to explore the opportunities that AI can generate in their sector.

(b) High-risk AI Systems

The AI Act provides an exhaustive list of AIS use cases that should be considered as high risk. Some of these use cases are specific to the financial sector. These potentially benefit from the exemption mechanism provided by the AI Act. Otherwise, they will have to comply with particularly stringent requirements.

(i) Credit scoring and underwriting systems in life and health insurance

Under a strict regime, the AI Act authorises the use of high-risk AI Systems, which are expressly defined in the text.

Two use cases in particular target stakeholders in the banking and financial sector:

– AI Systems for assessing the solvency of individuals or establishing their credit rating[99]

These AI Systems determine, among other things, individuals' access to financial resources or other essential services (housing, electricity and telecommunication services), which may lead to the creation or perpetuation of patterns of discrimination falling into the category of high-risk AI Systems[100].

The scope of application of the AI Act is not limited by a specific reference to the regulatory status of the stakeholder that is to deploy such solutions. The rules set out in the AI Act could therefore

97 *Ibid.*
98 *Ibid.*
99 *Article 5(b) Annex III of the AI Act.*
100 *Recital 58 of the AI Act.*

have to be complied with by credit institutions, but also by all stakeholders involved in granting credit to individuals and likely to incorporate this type of tool (whether lenders or any intermediary in the loan-granting chain, such as intermediaries in banking and payment services, or even potentially technology providers).

– For insurance, AI Systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance[101].

Because of their potentially significant impact on the living conditions of life and health insurance beneficiaries, the design, development and use of these AI Systems may infringe their fundamental rights, leading to risks of financial exclusion or discrimination, requiring increased vigilance by the regulator.

Note that in its "Factsheet" on the regulatory framework for AI in insurance, EIOPA points out that whilst the AI Act introduces additional requirements for providers or deployers of high-risk AI Systems, "insurance sector legislation continues to apply across all use cases, regardless of their qualification under the AI Act"[102].

It should be noted that the AI Act expressly provides that the European Commission may revise the list of cases of use of high-risk AI Systems where the AI System in question is intended to be used in one of the areas specified in Annex III to the AI Act[103]. Since credit scoring and underwriting in life and health insurance are indeed areas specified in Annex III of the AI Act, the Commission could potentially extend the list to other use cases that might emerge in the financial world and prove to be particularly risky, for example from the point of view of customer protection or market stability, should the Commission succeed in linking the latter notion to the protection of health, safety and fundamental rights[104].

(ii) Exemptions and the opt-out mechanism

Certain AI Systems, either because of their purpose or because they are already subject to specific supervision by other regulations, should in principle be excluded from the category of high-risk AI Systems under the AI Act, even though they could have been qualified as such under the AI Act. This is the case for AI Systems used to detect fraud in the provision of financial services and for prudential purposes to calculate the capital requirements of credit institutions and insurance companies, insofar as they are governed by EU law[105].

However, the exact scope of the exemption for the detection of financial fraud remains unclear[106]. In particular, it would be useful to know to what extent AI Systems are used for the purposes of

---

101 *Article 5(c) Annex III of the AI Act.*
102 *EIOPA, Regulatory framework applicable to AI systems in the insurance sector, July 2024.*
103 *Article 7(1) of the AI Act.*
104 *Article 1(1) of the AI Act.*
105 *Recital 58 of the AI Act.*
106 *Annex III of the AI Act lists the high-risk AI Systems referred to in Article 6(2) of the AI Act (subject to the exemption provided for in Article 6(3) of the AI Act or the opt-out mechanism). It provides in paragraph 5(b) that the following are considered*

combating money laundering and terrorist financing or for the prevention of market abuse benefiting from such an exemption. The scope of the exclusion of AI Systems used for prudential purposes to calculate the capital requirements of certain Financial Institutions provided for in Recital 58 of the AI Act also lacks clarity insofar as it is not clarified further by other provisions of the AI Act. Its relationship with the inclusion of "AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score" in the list of high-risk AI Systems provided for in Annex III of the AI Act also raises questions (see on this point paragraph 5 below relating to the relationship of the AI Act with prudential regulations).

Furthermore, through the opt-out mechanism, an AI System referred to in Annex III of the AI Act does not fall into the category of a high-risk AI System when it does not present significant risks of harm to the health, safety or fundamental rights of natural persons[107]. Whilst the conditions determining the application of the opt-out mechanism are clearly and restrictively listed, there is still uncertainty as to the concrete cases of use that can benefit from this exemption in the banking and financial sector.

Thus, in the case of a system enabling the assessment of a customer's creditworthiness by a credit institution's AI System, depending on the device into which it fits, it might not be content with performing a "narrow procedural task"[108] or "[improving] the result of a previously completed human activity"[109]. In this case, it could not be exempted on these grounds. On the other hand, if it is used solely to "perform a preparatory task"[110] to determine the customer's potential default risk, or to "detect decision-making patterns or deviations from prior decision-making pattern"[111] to establish a typical acceptable credit rating profile for the Financial Institution in question, then it would be exempt from the regime applicable to high-risk AI Systems. This assessment will have to be carried out in concreto according to the exact needs for which the AI System is used.

Hopefully the opt-out mechanism will soon be clarified so that the scope of high-risk AI Systems to be considered can be better assessed.

(iii) Specific constraints for high-risk AI Systems in the banking and financial sector

The use cases referred to above, considered to present a high risk, are among the only cases in which the developer of an AI System must carry out an impact assessment with regard to fundamental rights before deploying these systems for the first time[112]. It is interesting to note that only the banking and insurance sectors, out of all the use cases governed by the text and deployed

high-risk AI Systems: "AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud;". The exclusion of AI Systems used for the purpose of detecting financial fraud from the category of high-risk AI Systems contributes to maintaining the vagueness on the exact scope of the exclusion more than it clarifies it given the syntax of paragraph 5(b).

107 *Article 6(3) of the AI Act.*

108 *Article 6(3)(a) of the AI Act.*

109 *Article 6(3)(b) of the AI Act.*

110 *Article 6(3)(d) of the AI Act.*

111 *Article 6(3)(c) of the AI Act.*

112 *Article 27 of the AI Act.*

without any link to the public sector, have been subject to this obligation. We can certainly detect a particular vigilance on the part of the financial authorities regarding access to services provided by these industries.

(c) "Limited risk AI Systems" interacting directly with individuals

If they are not considered to present unacceptable or high risks, many use cases in the banking and financial sector will fall into the category of systems presenting a limited risk because they interact directly with natural persons or generate synthetic content[113]. It should be noted that the notion of a "Limited Risk AI System" is not defined as such in the AI Act but refers here to the category of systems that would not be captured by the unacceptable or high-risk use cases but still presents risks of identity theft or deception because of their direct interactions with the user[114]. Under the aegis of the AI Office, good practices could also be developed to comply with these requirements[115], for example at industry level via professional charters.

Financial Institutions deploying, for example, chatbots, language analysis systems or systems for analysing customer habits and improving the customer experience will have to inform the user, right from the product design stage, so that they understand that they are interacting with an AI System and/or that the information presented to them has been generated and manipulated by an AI System.

(d) AI Systems with minimal or no risk

Finally, the AI Act authorises the free use of AI with minimal risk. This is a residual category of AI Systems. It includes all those that do not fit into any other classification. These AIS do not need to comply with any specific requirements and represent most systems currently in use in the EU. They include video games and spam filters. Here again, best practice could also be developed at industry level via professional charters to help stakeholders to structure themselves.

B. Creation of new obligations linked to the use of AI

1. Four possible roles for Financial Institutions

The AI Act creates several categories to which different obligations are attached. An in-depth, case-by-case analysis will therefore be required to determine the status and related obligations. It defines four main stakeholders statuses[116]:

The AI provider is the first in the AIS value chain regulated by the AI Act. It is "a natural or legal person, a public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the

113 *Article 50 of the AI Act.*
114 *Recital 132 of the AI Act.*
115 *Article 50(4) of the AI Act.*
116 *Article 3 of the AI Act.*

market or puts the AI system into service under its own name or trademark, whether for payment or free of charge". It would seem that Financial Institutions, even if they do not primarily achieve this status since their main activity does not *a priori* consist of developing AI Systems, could quite easily fall into this category, for example if they have an AI System developed by a service provider in order to put it into service. In addition, a distributor, importer or deployer (as defined below) may be considered as a high-risk AI provider if it makes "a substantial modification to a high-risk AI system which has already been placed on the market or has already been put into service" or if it changes its intended use[117].

The AI deployer is "a natural or legal person, public authority, agency or other body using an AI system under its own authority [...]". In other words, it is the user using AI for professional purposes. Financial Institutions should fall more generally into this category, unless they more frequently choose to develop or have developed the AI System for bespoke use. For example, Financial Institutions will be deployers of their HR management tool if it is an AI System and they use it in their organisations to manage, for example, their payroll.

An AI importer is any person established in the EU who places on the market an AI System bearing the name or trademark of a person established outside the EU. It could be a French bank that buys AI software developed in China to put it on the European market.

The AI distributor is a natural or legal person who makes an AI System available in the supply chain, without modifying its properties. It may be a French company that buys and then distributes AI software already present in the EU to its branches. It makes the product available without modifying it. We could also consider that the parent company of a European financial group that acquires an AI System from a provider so that this AIS can be deployed by the group's European subsidiaries could qualify as a distributor.

As the various obligations contained in the AI Act depend, in part, on the category to which the AI operator belongs, qualification is important in order to determine the nature and extent of the requirements that must be met. The exercise of qualifying the role occupied by a Financial Institution must be carried out with precision, noting that the various categories mentioned above are not exclusive. For example, the same entity may be both a distributor and a deployer, if it makes an AI System available on the EU market and simultaneously uses it under its own authority. In this case, the requirements for each status should apply cumulatively. Beyond this, it should be noted that the AI Act does not introduce any derogation regime for the supply of AI Systems or models within the same group.

Thus, the use of AI solutions within a single financial group could lead to the characterisation of different statuses within the meaning of the AI Act for the group's entities, with a set of variable obligations depending on the status applicable to each entity.

---

[117] *Article 25(1)(b) and (c) of the AI Act.*

2. Specific obligations and liability regimes for each role

Transparency and AI Act compliance obligations must be observed by Financial Institutions when developing and supplying, importing or deploying AI.

The obligations are numerous and, as indicated above, depend on the qualification chosen for the Financial Institution concerned. The AI Act contains several provisions intended to integrate its obligations into the framework and obligations already provided for financial services institutions.

The obligations of providers and/or deployers of high-risk AI are set out in Articles 8 et seq. of the AI Act (control of AI, existence of a risk management system, requirements regarding the data used and the governance of said data, technical documentation, registration, transparency and provision of information to deployers, human control, accuracy, robustness and cybersecurity, etc., retention of documents, automatically generated logs, corrective measures and duty to inform, etc.).

The obligations defined for each role correspond to those imposed on the other categories of stakeholders in the AIS value chain defined in the AI Act. For example, whilst the prohibition of certain practices under Article 5 of the AI Act is clearly aimed at deployers, the European Commission's guidelines specify that providers are expected to take reasonable steps to ensure that their AIS, including general purpose AIS which can reasonably be expected to be used for a prohibited use case, cannot be deployed for such purposes[118].

Furthermore, any failure by one of the stakeholders in the AIS value chain to meet its obligations under the AI Act could have an impact on the ability of others involved in the development, marketing or deployment of the same AIS to meet theirs. The liability incurred for failure to meet the requirements of the AI Act (leading to penalties of up to 7% of annual worldwide sales or €35 million depending on the breach[119]) will, in this case, have to be coordinated with the contractual and extra-contractual liability that may be incurred by the stakeholder involved.

C. Recognition of existing supervisory authorities

A network of national and European competent authorities has been set up to ensure harmonised and effective implementation of the AI Act obligations.

1. The competent authorities under the AI Act

The AI Act itself provides for various public institutions, both national and European, to be responsible for implementing the new regulation.

The AI Act created two European bodies responsible for interpreting and implementing the AI Act, both with varying powers and authority.

---

118 *European Commission, op. cit, Guidelines on prohibited artificial intelligence practices, para 40.*

119 *Article 99(3) of the AI Act.*

- The European AI Office is a body depending from the European Commission. It contributes to the strategic, coherent and effective implementation of the AI Act and as such has a number of powers, including investigative powers[120], especially in terms of general-purpose AIS[121]. The AI Office will be assisted by the AI Act Service Desk, an information centre on the AI Act, enabling parties to seek help and receive tailored responses[122].

- The AI Board will provide recommendations on the application of the AI Act. It is made up of representatives from all the Member States. Its main task is to ensure that the application of the AI Act is harmonised across Europe.

The AI Act also requires each Member State to designate different national competent authorities[123], including the national supervisory authority, responsible for the general application of the AI Act and acting as a point of contact with the different national authorities; the market surveillance authority, responsible for verifying the conformity of AI Systems placed on the market; and the "notifying" authority, which plays a key role in the designation and notification of AI Systems' conformity assessment bodies.

The designation of these new powers must be consistent with the existing role of the sectoral authorities responsible for supervising the financial sector. For example, the European Central Bank retains its prudential supervisory functions over the risk management processes and internal control mechanisms of credit institutions[124].

One of the major challenges of this global framework and the different competences thus defined is the harmonisation of approaches between authorities with principal competence and those purely involved in the financial sector, at both national and European level. This is particularly critical for Financial Institutions, as divergences between regulators could complicate cross-border operations, and requirements specific to the AI Act must be integrated into sectoral regulations without creating conflicts or duplication.

2. The case of France

For the time being, France does not seem to have designated the competent authority or authorities to supervise the use of AI by Financial Institutions – see Recital 158 and Article 74(6) of the AI Act – In order to ensure consistency and compliance with the AI Act, the Member States will need to designate the competent authorities, within the limits of their respective powers, including for market surveillance activities[125]. In addition, explicit reference is made to the competent financial authorities under the Regulation on prudential requirements for credit institutions (CRR), and the Directives on credit agreements for consumers (2008/48/EC), access to the activity and prudential

---

120 *See Article 64 AI Act and Commission Decision, Decision establishing the European Artificial Intelligence Office C(2024) 390, 24 January 2024 for a more detailed view of the powers of the European AI Office.*

121 *Recital 163 and Article 75 of the AI Act.*

122 *Unveiled by the European Commission in its AI Continent Action Plan, 9 April 2025, p. 21.*

123 *Article 59 of the AI Act.*

124 *Considering 158 AI Act.*

125 *Ibid.*

supervision of credit institutions (CRD) and credit agreements consumers relating to residential immovable property (2014/17/EU).

The prerogatives of these authorities should include the power to carry out ex post-market surveillance activities which may be integrated, where appropriate, into their existing supervisory mechanisms and procedures under EU financial services law.

In addition, for high-risk AIS in the financial sector, "the market supervisor for the purposes of this Regulation shall be the national authority responsible for the financial supervision of such institutions"[126]. However, Member States may derogate from this provision and designate another competent authority[127].

To date, France seems to be opting for a division of powers between several existing authorities rather than creating a new one. The ACPR (the French Prudential Supervision and Resolution Authority) will be responsible for supervising the application of the AI Act to the financial sector, including large banking institutions. The ACPR is therefore preparing to develop *ad hoc* audit mechanisms for AIS[128].

One of the major objectives of the allocation of powers should be to reconcile the need for harmonisation of the authorities' approaches, as suggested above, with the imperative of not overly complicating the institutional framework accompanying the implementation of the AI Act for Financial Institutions. The priority should be to entrust the implementation of the AI Act by Financial Institutions to authorities with appropriate resources and technical skills, close to the specific challenges of the financial sector, and capable of responding quickly to the questions of stakeholders on issues that are often complex.

126 *Article 74(6) of the AI Act.*
127 *Article 74(7) of the AI Act.*
128 *ACPR, Artificial Intelligence: what impact for ACPR? ACPR Review, 5 July 2024.*

III. Coordinating the AI Act with other regulations governing the Financial Institutions

The European legislator, through the AI Act, aims to establish a harmonised legal framework at European level to promote the development, use and adoption of AI throughout the internal market[129]. However, this transversal legal framework is likely to overlap with existing regulations applicable to Financial Institutions in several respects. This results in a series of obstacles in the articulation and interaction between this new body of rules and pre-existing regulations, particularly those governing data (e.g. DORA, NIS 2, GDPR)[130], as well as rules specific to Financial Institutions.

A. Interactions between AI regulation and sector-specific regulations

1. A general approach to the complementarity of the AI Act with sector-specific regulations

In its text, the European legislator wishes to establish a coherent framework and an articulation of the AI Act with sectoral rules. More specifically, in recital 158 of the AI Act, the legislator states that, with regard to certain requirements of the AI Act, "it is […] appropriate to integrate some of the obligations [of the AI Act]", whilst, with regard to others, it calls to "avoid overlaps", in particular by introducing derogations[131].

This last recital refers specifically to the banking and financial sector, but the legislator's desire for consistency seems more general, since recital 64 of the AI Act envisages the hypothesis that this Regulation implies "a simultaneous and complementary application of the various legislative acts"[132]; while recital 81 refers to "complementarity between this Regulation and the sectoral Union law [which] should also be taken into account in future standardisation activities or guidance adopted by the Commission"[133].

This legislative approach will be also evident in the targeted consultation launched by the European Commission on AI in the financial sector. The European Commission expressly explains in its introduction that the AI Act is designed to complement the existing banking and financial services acquis – even though sector-specific regulation is not specifically intended to govern this technology – notably by laying down a framework for AI risk management and certain AI-specific requirements that Financial Institutions should take into account when exploiting this technology[134].

The approach adopted by the AI Act thus seems relatively clear to us: the cross-sector body of rules laid down by the AI Act must take account of the specific features of the banking and financial sector

---

129 *Recital 8 of the AI Act.*
130 *Please refer to paragraph III.BB of this Report.*
131 *Recital 158 of the AI Act.*
132 *Recital 64 of the AI Act.*
133 *Recital 81 of the AI Act.*
134 *European Commission, Consultation document – Targeted consultation on artificial intelligence in the financial sector, 18 June 2024, p. 3.*

when applying them to Financial Institutions. In other words, the AI Act complements the existing banking and financial legislative framework and is not intended to replace it.

2. Specific governance requirements to be integrated

From this approach of complementarity, we note that the AI Act either recognises the equivalence between its provisions and those of the sector-specific regulations, or specifies how to reconcile the obligation of the AI Act with those of the sector-specific regulations.

In other respects, the AI Act complements sector-specific regulations by imposing governance requirements.

(a) Recognition of equivalence or complementarity in terms of governance

(i) Forms of recognition of equivalence

The AI Act initiates recognition of equivalence between certain of its requirements and the rules established by sectoral regulations. In a number of similar provisions and terms, the AI Act provides, by means of a double condition, that if the providers/deployers are (i) "Financial Institutions" and (ii) as such, they are "subject to requirements regarding their internal governance, arrangements or processes under Union financial services law", then compliance with the latter set of sector-specific rules "shall be deemed to be fulfilled by complying with the [obligation]" laid down by the AI Act.

This recognition of equivalence calls for two preliminary remarks:

- On the definition of "Financial Institution": at first sight, some might consider that the qualification of "Financial Institution" refers directly to that set out in Article 4(1)(26) of the CRR. However, it does not seem to us that class 1 credit institutions and investment firms are excluded from the scope of this recognition of equivalence. This would contradict the philosophy of harmonisation and complementarity intended by the European legislator which, more importantly, directly targets this idea of recognition of equivalence in Recital 158, which states that the AI Act should allow "limited derogations" for credit institutions and other Financial Institutions;

- On the interpretation given to "Union legislation on financial services": the expression used by the AI Act of "Union legislation on financial services" should not be interpreted as excluding banking services, for the same reasons given above.

Consequently, it seems to us that the meaning of the provisions on recognition of equivalence should allow a Financial Institution which is already subject to a certain number of rules of governance, systems or internal processes under the terms of its regulatory status to be deemed to comply with the provisions referred to in the AI Act.

It should also be pointed out that the AI Act does seem to allow equivalence to be recognised by these provisions and not subordination to them. In fact, to admit that the provisions allow the AI Act to be subordinated to the sectoral rules would be tantamount to completely disregarding certain specific rules of the AI Act. This does not seem to be the case here, because even if the sectoral regulatory framework allows Financial Institutions to comply favourably with the requirements of the AI Act, it does not replace them. Financial Institutions will have to take this into account when meeting the requirements of their own sectoral regulations which are deemed to be equivalent. In other words, the adage *specialia generalibus derogant*, whereby special laws (i.e. sector-specific regulations) derogate from general laws (i.e. the AI Act) should not apply directly.

Full recognition of equivalence is thus notable with regard to the obligation to monitor the operation of the high-risk AI System on the basis of the instruction manual[135]. The obligation to provide information in the event of a serious incident[136] during the use of this AI System could be fulfilled by the notification of major operational incidents to the ACPR by the effective managers[137], subject to notifying the other persons covered by the provision of the AI Act.

(ii) Recognition of the complementary nature of the rules

With regard to the complementarity of the rules of the AI Act with those of the sectoral regulations, the AI Act recognises this firstly with regard to the retention of documents. Financial Institutions providing high-risk AI Systems can therefore rely on their existing systems to meet their document retention obligations under the AI Act. As such, Financial Institutions will need to keep their AI technical documentation up to date[138]. For credit institutions, this technical documentation could be incorporated into the procedures manuals describing the entity's activities[139].

For these same entities, the AI Act also recognises the complementarity of sector-specific regulations concerning automatically generated logs[140], monitoring systems and post-marketing surveillance plans[141].

(iii) Recognition of partial equivalence

Article 17 of the AI Act stipulates that providers of high-risk AI Systems must implement quality management systems, involving the drafting of precise policies and procedures in order to comply with the prescriptions of the AI Act. However, Financial Institutions providing such a system benefit from a recognition of equivalence of their sectoral regulations, with the exception of the requirements developed in points g), h) and i) of paragraph 1 of Article 17. The recognition of equivalence is then only partial.

---

135 *Article 26(5) of the AI Act.*
136 *Ibid.*
137 *Article 249(1) of the Order of 3 November 2014 and Article L. 521-10 of the French Financial Code .*
138 *Article 18(3) of the AI Act.*
139 *Article 254 of the Order of 3 November 2014.*
140 *Article 19(2) of the AI Act.*
141 *Article 72(4) of the AI Act.*

Thus, with regard to the risk management system[142], the development, implementation and operation of post-marketing surveillance systems[143] (it being specified that, as previously explained, the article relating to this obligation allows Financial Institutions to integrate the obligations relating to pre-marketing surveillance into the entity's existing systems and plans, provided that they present an equivalent level of protection) and the serious incident procedures[144] (it should be noted that Article 73(9) of the AI Act stipulates that for high-risk systems referred to in Annex III placed on the market by a supplier subject to an equivalent reporting obligation, only the breach of an obligation intended to protect fundamental rights must be reported), the Financial Institutions will have to put them in place as the recognition of equivalence is only partial[145].

(b) New AI Act obligations to complement sector-specific regulations for Financial Institutions

In addition to the provisions of the AI Act recognising equivalence or complementarity with sector-specific regulations, the Regulation introduces new obligations for Financial Institutions, depending on their role as explained in paragraph II.B.1, and the classification of the AI System, as detailed in paragraph II.A.3.

As such, and in the spirit of the AI Act, it seems to us that these AI-specific obligations should not contradict those of sector-specific regulations, but rather complement them.

Financial Institutions will thus be required to meet non-exhaustive obligations in terms of data governance[146], the preparation of technical documentation[147], recording[148] and preparation of an automated log system[149] and human control[150]. These requirements will be in addition to those already established by the sector-specific regulations in force and will be integrated into them in a coherent manner.

3. Refining the management of the risks inherent in the use of AI

The AI Act adopts a risk-based approach, conceptually close to that which traditionally prevails in banking and financial regulation (although the frame of reference is different)[151]. This approach implies that Financial Institutions must carry out a double identification and qualification process: on the one hand, the qualification of the AI model or System (e.g. prohibited, high risk, general use, etc.) and, on the other hand, the qualification of the stakeholders involved (e.g. supplier, deployer, etc.), in addition to a risk-mapping process.

---

142 *Article 17(1)(g) of the AI Act.*
143 *Article 17(1)(h) of the AI Act.*
144 *Article 17(1)(i) of the AI Act.*
145 *Please refer to paragraph III.A.3 of this Report.*
146 *Article 10 of the AI Act.*
147 *Article 11 of the AI Act.*
148 *Article 12 of the AI Act.*
149 *Article 19 of the AI Act.*
150 *Article 14 of the AI Act.*
151 *This has been highlighted by B. Bréhier, L'application du règlement européen sur l'intelligence artificielle (IA Act) aux activités bancaires et financières, RDBF n°6, nov.-déc. 2024, §20.*

At the same time, Article 9(1)(i) of the AI Act provides for the implementation of a risk management system for high-risk AI Systems. No recognition of equivalence has been accepted for these provisions (see paragraph 2(a)(iii) above). However, it is necessary to address the question of the possible overlap or imbrication of this system with the existing regulatory framework for Financial Institutions.

Although there is no formal recognition of equivalence in the AI Act, it is clear that the risk management system provided for in the AI Act will not be able to prevail; it will have to be complemented by banking and financial regulations, as set out in Article 17(4) of the AI Act. In our view, it is inevitable that the two systems will be linked.

Indeed, it seems important to note that the risk management system in place in Financial Institutions responds to the particularities of the sector by taking into account multiple aspects and issues that are not considered in the AI Act, which only aims to preserve fundamental rights. The risk management system established under sector regulation also benefits from authorisation by the competent supervisory authority, which is well established in the European regulatory landscape, whereas the system established by the AI Act is still in its infancy.

Finally, the rules established by sector regulation are designed to be flexible and neutral, so the integration of a new technology such as AI should not create obstacles for Financial Institutions. They will, however, have to adapt their risk management systems to meet the new risks created by this technology.

As a result, the AI Act risk management system should naturally be integrated into the existing system for Financial Institutions. However, these institutions will not be exempt from having to make certain adjustments to meet the specific requirements of the AI Act.

4. Unclear articulation of the rules of good conduct

The AI Act does not expressly provide for an equivalence mechanism between the rules of good conduct to be implemented with regard to clients benefiting from a regulated service using AI and the rules of good conduct arising from the sectoral rules.

It will in fact be up to each Financial Institution to comply with the rules of good conduct for each regulated service in order to take into account the effects or risks attached to the AI that would be used for their service. For example, Article 50 of the AI Act stipulates that providers must ensure that AI Systems intended to interact directly with natural persons are designed and developed in such a way that these persons are informed that they are interacting with an AI System, unless it appears from the point of view of such persons, who are normally informed, reasonably attentive and aware, that they are interacting with such an AI System. This transparency obligation should be included in the rules of good conduct imposed on Financial Institutions.

Nevertheless, the qualitative and quantitative level of information to be given to clients/investors upstream and downstream of the provision of the regulated service relating to the use of AI and the associated risks will be a matter for the internal policy of each Financial Institution.

5. Relationship with prudential regulation

The link between the AI Act and prudential regulation is based on Recital 58 of the AI Act, which establishes a principle of exclusion in this area, the exact scope of which remains uncertain.

According to Recital 58, "AI systems provided for by Union law [...] for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under this Regulation". In other words, AI Systems used for prudential purposes by Financial Institutions which are already subject to sector-specific regulation (such as CRR for credit institutions or Solvency II as supplemented by Delegated Regulation (EU) 2015/35 for insurance companies) should not, in principle, be subject to the requirements set out in the AI Act for high-risk AI Systems, insofar as Recital 58 excludes *a priori* this qualification with regard to these systems – unlike AI Systems intended to be used to assess the creditworthiness of natural persons or to establish their credit score (credit scoring) which, for their part, are expressly categorised as high-risk AI Systems (in accordance with Annex III point 5(b) of the AI Act).

However, the exact scope of this exclusion is uncertain. Prudential regulations governing the use by Financial Institutions of AI Systems integrated into their internal models for the purposes of calculating their capital requirements do not completely disregard the role played by the internal ratings assigned by these models in approving loans granted – including to natural persons.

This is the case, for example, in Article 144(1)(b) of the CRR, which makes authorisation to use the internal model approach subject to the demonstration by credit institutions[152] that "internal ratings and default and loss estimates used in the calculation of own funds requirements and associated systems and processes play an essential role [...] in the decision-making process and in the credit approval functions [...]".

This assessment of the essential role played by the internal rating assigned by the credit institution's system in the decision to grant credit is known as the "use-test"[153]. Could an internal model incorporating an AI System for assessing the creditworthiness of individuals with a view to assigning them an internal rating and assigning them to a credit step[154] for the purposes of calculating capital requirements be considered to include a credit scoring system falling within the scope of high-risk AI Systems (by virtue of Annex III, point 5(b)) and thereby trigger, to a certain extent, the application

---

152 *To the satisfaction of the competent authority.*

153 *Julien Uri (ACPR) and François Guebs (Banque Nationale de Belgique), presentation "AI Act et réglementation sectorielle: interactions et conséquences sur la supervision" – available here: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.telecom-paris.fr/wp-content-EvDsK19/uploads/2024/12/lundi-ia-finance-11-supervision-f-guebs-j-uri.pdf.*

154 *In accordance with Articles 172 and 173 of the CRR.*

of the rules laid down by the AI Act for high-risk AI Systems? The question remains open, as the competent authorities have not yet provided any clarification in this respect.

Thus, although Recital 58 of the AI Act establishes a principle of exclusion of AI Systems used for prudential purposes to calculate capital requirements from the category of high-risk AI Systems, the requirements of the AI Act will probably have an impact on the development of internal models and the evaluation of the criteria governing their use by the competent authorities, insofar as these systems participate in the evaluation of the creditworthiness of natural persons and imply the attribution of an "internal" credit rating with a view to granting credit to these natural persons.

It should also be noted that this exclusion from the scope of high-risk AI Systems of AI Systems used for prudential purposes to calculate the capital requirements of credit institutions and insurance companies (already governed by existing sector-specific regulations) is not repeated (or otherwise specified) in the body of the AI Act itself.

Clarification of the relationship between the AI Act and prudential regulation (in particular the exclusion provided for in Recital 58) would certainly be beneficial in order to allow Financial Institutions for which EU law provides the possibility of using an internal models-based approach to calculate their capital requirements to clearly identify the rules applicable to them depending on the use they make of AI in relation to their internal models.

In addition, it should be noted that the principle of excluding AI Systems used for prudential purposes to calculate capital requirements from the category of high-risk AI Systems under the AI Act set out in Recital 58 only concerns two categories of Financial Institutions, namely credit institutions and insurance companies, precisely those for which EU law currently allows the use of AI Systems for prudential purposes, in particular the context of use of internal models.

However, as indicated above (see paragraph I.E.2), other types of Financial Institutions could consider using AI for prudential purposes to calculate their capital requirements, for example investment firms determining their capital on the basis of K-factors or portfolio management companies subject to additional capital requirements under the AIFM Directive. If so, Recital 58 of the AI Act, as currently drafted, would not allow AI Systems set up by these Financial Institutions for the purpose of calculating their capital requirements to benefit from the principled exclusion from the category of high-risk AI Systems that it provides for under the AI Act (and this, *a priori*, regardless of whether Union law provides[155] or does not provide[156] for any specific framework for the use that these Financial Institutions might have of AI for prudential purposes).

---

155 *As the IFD/IFR regulation refers to the CRD/CRR regulation for the calculation of the K factor reflecting the net position risk (K-NPR), investment firms are a priori authorised to use internal models to calculate the related capital requirements under EU law. However, investment firms are not mentioned among the Financial Institutions referred to in Recital 58 of the AI Act as benefiting from the principled exclusion that it lays down, with regard to the AI Systems used for the purposes of calculating the capital requirements that they use.*

156 *The regulations governing the determination of additional capital requirements for portfolio management companies subject to the AIFM directive do not include provisions on the use of AI for this purpose.*

AI Systems used by Financial Institutions other than credit institutions or insurance companies, for prudential purposes to calculate their capital requirements, could therefore be qualified as high-risk AI Systems, even though they pursue a similar objective, should the conditions of Article 6 of the AI Act be met. Clarification as to the interpretation of the scope of the exclusion principle set out in Recital 58 as regards the Financial Institutions likely to benefit from it (in particular on the basis of the objectives which presided over its inclusion in the AI Act) could also prove beneficial, in order to provide legal certainty as to the use which could be made by other Financial Institutions of AI for prudential purposes.

6. Relationship with sector-specific outsourcing rules

The AI Act does not lay down any specific rules on outsourcing[157] which could overlap or pose difficulties of articulation with pre-existing rules in banking and financial regulation (see paragraph I.G.1). However, although such an overlap is not explicitly observed, scenarios where a Financial Institution would alternatively take on the role of AI provider or AI deployer remain ambiguous.

Does the Financial Institution's status as a supplier or deployer within the meaning of the AI Act mean that it is an outsourcing entity or that it provides an outsourced service?

The roles of provider and deployer defined by the AI Act are based on the relationship of each stakeholder with the AI System, rather than on the relationship between the stakeholders themselves, as is the case for outsourcing, which qualifies a relationship between a Financial Institution and a third-party provider. Consequently, the role of the stakeholder within the meaning of the AI Act does not immediately constitute a relevant activity within the meaning of the sector regulation on outsourcing. In our view, the AI Act and sector regulation statuses are neither antinomic nor incompatible and must be analysed separately.

Thus, the fact of entrusting a third party with an activity or service that the Financial Institution would itself have carried out (or that it would be reasonable to imagine it would have carried out) seems to be the first criterion for assessing a possible outsourcing relationship, without the role defined by the AI Act for each stakeholder interfering.

By putting the concepts of AI Act and outsourcing into perspective, several scenarios can be distinguished to assess a possible outsourcing relationship. Firstly, if a Financial Institution calls on a third party to design its AI System, then it would not be carrying out an outsourcing operation as such, as this operation would fall outside the scope of its services and activities arising from its status. However, if a Financial Institution, an AI System supplier, entrusts a third party deployer with the use of its system for the provision of a service or activity that it would have performed, or if a Financial Institution calls upon a third party, acting as supplier or deployer, for the provision of an

---

157 *As a reminder, outsourcing is defined by sector regulation as the fact that a Financial Institution decides that an activity or service that it would itself have performed (or that it would be reasonable to conceive that it would have performed) be performed by a third party (Cf. paragraph 26 of the "EBA Guidelines on outsourcing arrangements", EBA/GL/2019/02, 25 February 2019).*

activity or service that the entity would itself have performed or provided, then an outsourcing scheme with regard to the activity entrusted to the third party would need to be considered.

The use of any AI service provision will merit particular attention, especially when the Financial Institution, acting as a deployer, uses an AI tool provided by a third party, to carry out a regulated activity. This hypothesis might not be considered as outsourcing, as the Financial Institution would retain its function internally and would only call on a third party under a service provision contract. However, this approach needs to be qualified by an analysis of the AI System, its operation, development, deployment and purposes. In fact, this provision of service could be assimilated to outsourcing if it proves to be "critical", i.e. whose anomaly or failure could seriously harm the activity, the provision of regulated services, the continuity or the solidity of the Financial Institution.

Generally speaking, as ESMA points out[158], Financial Institutions must scrutinise any relationship with third-party AI service providers to identify any outsourcing qualification, and *a fortiori* for the provision of a PSEE leading to the application of additional obligations that could call into question the scheme envisaged by the Financial Institution.

B. Coordinating the AI Act with other European data regulations

The AI Act does not always clearly specify its relationship with other European regulations relating to data, whether they are general in scope such as the GDPR (which is often cited by the AI Act) or NIS 2, or sector-specific such as DORA (whereas the AI Act includes a number of provisions specific to financial entities).

However, these texts aim to make stakeholder more accountable, not only by imposing strict obligations, but also by forcing them to document and demonstrate their compliance with these obligations.

Nevertheless, both DORA and the GDPR can be allies in strengthening data protection, thereby strengthening the assets of Financial Institutions. Financial Institutions need to manage their assets made up of or using data, assess risks and ensure transparency to comply with DORA, GDPR and AI Act, especially when deploying high-risk AI solutions.

1. DORA

DORA, which came into force on 17 January 2025, aims to consolidate and harmonise ICT risk requirements in relation to operational risk, which until now have been spread across various EU legal acts.

---

158 *ESMA, Public Statement On the use of Artificial Intelligence (AI) in the provision of retail investment services, ESMA35-335435667-5924, 30 May 2024, "The deployment of AI tools in various steps of the provision of investment services can be based on the acquisition of solutions developed by third-party service providers. In such instances, firms are reminded of the applicable MiFID II requirements regarding outsourcing of critical and important operational functions aimed at ensuring an adequate level of due diligence in the selection process of such providers along the value chain and the implantation of adequate controls."*

The aim of the AI Act is also to establish a uniform legal framework for AI Systems to promote the adoption of AI while ensuring a high level of protection of fundamental rights and supporting innovation. In the financial sector, the objectives of these regulations are intrinsically linked, provided that the underlying communication technology is based on AI, or the AI System in question constitutes an ICT. In other words, some Financial Institutions may frequently have to apply both regulations in parallel to the same product or service provider. By way of example, AI Systems should be considered as "ICT assets" within the meaning of DORA, triggering the application of the rules relating to such assets. In particular, this should trigger the inclusion of these AI Systems in the risk management framework set out in Article 6 of DORA.

However, these regulations are not always perfectly aligned due to their different purpose and scope. For example, DORA requires the implementation of audits of third-party ICT service providers and of the Financial Institution's own ICT, whereas the AI Act requires, with regard to high-risk AI Systems, that they allow "effective control by natural persons during their period of use". Two levels of control should therefore be able to apply to certain ICTs based on high-risk AI Systems, at the risk of creating redundancies or gaps in the controls carried out. Financial Institutions should therefore ensure that their policies and procedures for the control of these systems are perfectly articulated to meet regulatory requirements, while in practice limiting duplication in terms of the scope of controls, their frequency, remedial actions, etc.

DORA and the AI Act also both impose documentation obligations, albeit in different fields. DORA's obligations logically focus on ICTs, in particular the "business" functions, the roles and responsibilities that rely on ICTs, the information assets and ICT assets that support these functions, and their roles and dependencies with regard to ICT-related risk. The obligations arising from the AI Act relate in particular to the technical documentation of high-risk AI Systems – which may overlap with the ICT obligations. Financial Institutions will therefore need to have policies and procedures in place to comply with both sets of documentation obligations and identify redundancies.

Innovation is the crux of the challenges posed by the AI Act and DORA, which provisions aim to control risks and apply an ethical compliance as well as an operational security framework. The AI Systems put in place by Financial Institutions will therefore have to comply with these requirements. Their main challenge will be pursuing their innovative projects whilst respecting this framework.

One of the pillars of DORA, and of the regulations applicable to Financial Institutions in general, is the control of risks arising from the use of external service providers. As a general rule, the use of external service providers must be subject to precise decision-making processes, regular controls, and so on. In addition to the regulations applicable to outsourcing, third-party service providers may now also be subject to two other layers of obligations: those imposed on Financial Institutions by DORA and the AI Act, each of which imposes obligations in terms of documentation, AI System bias management, operational resilience and cybersecurity, etc., within their own scope of application.

It should be noted that alongside DORA and the AI Act, other texts apply to cybersecurity of AI Systems. Whilst Article 15 of the AI Act is devoted to the cybersecurity of high-risk AI Systems, we

need to look to another regulation for a comprehensive approach to this issue. This is the Cyber Resilience Act Regulation 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products incorporating digital elements. The purpose of this text is to provide European cybersecurity certification for products, hardware or software containing digital components (in particular the Internet of Things) made available on the market "whose intended or reasonably foreseeable use includes a direct or indirect logical or physical connection to a device or network". The aim is to protect consumers and businesses from risks during the design, development, production and making available-on-the-market stages.

This regulation should be read in conjunction with the EUCC Scheme[159], the first European cybersecurity certification scheme based on common criteria, particularly for the evaluation and certification of software used in the internal market. Based on a voluntary basis, the EUCC enables ICT suppliers to go through an evaluation process commonly accepted by the EU to certify ICT products such as software[160].

This scheme complements the SOG-IS[161] certification, which aims to protect users against the cybersecurity risks associated with IT products.

2. GDPR

(a) A delicate interplay with the AI Act

The AI Act explicitly provides for its articulation with the GDPR, even though certain concepts do not always have the same scope or field of application.

In the field of AI, data acts like the fuel that powers the engine of the algorithms. The quality and quantity of the data therefore have a direct influence on the AI's ability to learn and make decisions.

When the data in question is personal data, including pseudonymised data, the GDPR is intended to apply automatically. Personal data is central to many AI Systems implemented in the financial sector. At each stage in the development and deployment of an AI System, personal data may be included and processed, particularly in training data, validation data, test data, input data and output data. It is even possible for an AI System to infer personal data from input data that does not contain any personal data. This would theoretically be the case when an AI System can infer a person's unique identity from non-personal data provided to it. In addition, large language model (LLM) training requires information relating to individuals to refine the model by exploiting contextual information.

---

159 *Implementing Regulation 2024/482 of 31 January 2024 laying down detailed rules for the implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Union Common Criteria Cybersecurity Certification Scheme (EUCC).*

160 *This regulation was supplemented by a second regulation 2024/482 of 31 January 2024 laying down detailed rules for the implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European cybersecurity certification scheme based on common criteria (EUCC).*

161 *The SOG-IS agreement was created in response to the decision of the Council of the European Communities of 31 March 1992 on the security of information systems (92/242/EEC) and Council Recommendation 1995/144/EC of 7 April 1995 on common information technology security evaluation criteria. https://www.sogis.eu/index_fr.html.*

The processing of personal data in AI Systems therefore requires heightened vigilance and rigorous compliance with the GDPR in order to protect the rights of individuals at every stage of the development and deployment of these technologies. It is crucial to consider the privacy implications, even when the initial data is explicitly not personal.

The GDPR therefore applies simultaneously to the AI Act. The two regulations are supplementary to one another: the AI Act does not replace the GDPR.

The GDPR is based on an accountability principle and technology-neutral rules, requiring operators to ensure the processing of personal data is lawful and proportionate. In contrast, the AI Act operates on a risk-based approach, similar to the approach in the Defective Products Regulations, whereby certain types of AI Systems are simply prohibited or presumed to pose a high risk and can only be deployed in certain circumstances and under certain conditions.

Despite these fundamental differences, the two sets of regulations share a common objective: the protection of individuals. This approach is achieved through the liability of the stakeholders involved. The GDPR, which focuses on the processing and protection of personal data, guarantees individuals control over their information. It introduces rights such as the right of access, the right of rectification, the right to erasure, and the right to object to data processing, particularly where such processing is automated. Under the GDPR, data controllers and processors must put in place technical and organisational measures to ensure the compliance of their processing operations.

At the same time, the AI Act adopts a specific approach to AI Systems, imposing particular requirements to avoid violations of fundamental rights. This involves, for example, imposing transparency criteria and more generally ensuring that high-risk systems do not compromise the rights to human dignity, data protection or non-discrimination. AI stakeholders must also prove their compliance with strict standards, including documentation and impact assessment obligations. For example, both the AI Act and the GDPR aim to protect the rights of individuals in the case of automated procedures by incorporating the concept of human intervention. The GDPR grants data subjects the right not to be subject to a decision based solely on automated processing (including profiling) which produces legal effects concerning them or significantly affects them (Article 22 GDPR). The AI Act requires high-risk systems to incorporate a human guarantee to minimise risks and ensure the reliability of the AIS (Article 14 AI Act). It should be noted that a decision taken exclusively by an AI System could thus fall within the scope of the GDPR in accordance with the aforementioned article 22. By way of illustration, the CJEU has held that the evaluation of credit scoring is an automated decision, provided that the score had a decisive influence in the decision[162]. The AI Act, for its part, allows data subjects who are the subject of a decision taken by a deployer on the basis of the output of an AI System (high risk mentioned in Annex III) to obtain explanations on the role of the AIS in the decision-making procedure and on the main elements of the decision taken, in accordance with Article 86 of the AI Act.

[162] *CJEU, C-634/21, OQ v SCHUFA Holding AG, 7 December 2023.*

Together, these texts aim to protect individual rights against the undesirable effects of digital technologies while promoting innovation, particularly in terms of data circulation. Ultimately, these texts aim to develop innovations that respect the rights of individuals.

That said, the AI Act and the GDPR may lead to differences in the implementation of the principle of privacy by design. As a reminder, it involves incorporating the protection of personal data right from the design stage of systems, ensuring that security measures are proactively taken into account throughout the data lifecycle. Under the GDPR, systems that process personal data must be designed from the outset to incorporate data protection mechanisms. This may include the principles of data minimisation, purpose limitation and data security by default.

The principle of minimisation of data is a direct translation of the principle of privacy by design in AIS, the application of which can sometimes prove tricky, particularly when it comes to processing large quantities of data to train AI Systems or guaranteeing the transparency and explainability of complex models. Machine-learning algorithms do require large quantities of data to train their models. However, to improve performance and reduce bias, it is sometimes necessary to use redundant datasets or to include non-essential information. The principle of minimisation must therefore be borne in mind when incorporating these large databases, and the AIS needs to be assessed in terms of data protection. Certain weightings will therefore be essential, especially when training models on large databases in the face of a reduction in the number of data items, which could have an impact on the quality of the AIS. In other words, only the minimum amount of data, strictly necessary to maintain the quality of an AIS, should be processed[163].

In addition, the GDPR also introduces obligations to limit data retention periods. AI models often require historical datasets to be re-trained and kept up to date, which needs to be articulated with the GDPR obligation to limit data retention time. In order to comply with this obligation, the CNIL encourages providers to set a data retention limit proportionate to their uses. Although data may be kept for product maintenance or system improvement purposes, it must be subject to enhanced security measures[164]. Similarly, the obligation to trace decisions taken by automated systems, which often requires longer data retention to be able to verify and explain algorithmic decisions at a later date, means that data must be retained for a longer period.

To mitigate the impact on privacy while maintaining compliance with the principle of minimisation, it is common practice to pseudonymise or anonymise the data used to train AI Systems. However, pseudonymisation does not completely solve the problem, insofar as the data can be re-identified, in which case it is still considered to be personal and therefore subject to the protection of the GDPR. As for anonymisation, this practice can make data less reliable or reduce the performance of algorithms.

---

163 *CNIL, AI: Tenir compte de la protection des données dans la conception du système, Recommendation, 08 April 2024.*

164 *Ibid.*

Another consideration to be considered concerns the purposes of processing, a key principle of the GDPR[165]. According to the latter, data should be collected for a specified and legitimate purpose and not further processed in a way incompatible with that original purpose. However, AIS have a constant need for data to improve over time through continuous learning. This means that data initially collected for a specific purpose can be re-used for other purposes to improve the model. To encourage healthy re-use of data, consistent with the GDPR, financial stakeholders will soon be able to turn to the European Digital Governance Act (**DGA**). It is a regulation adopted in 2022, which promotes rules for the exchange and re-use of data between all stakeholders in the common market. In addition, the European Union plans to adopt another text focusing specifically on the exchange of financial data (Financial Data Access Regulation (**FiDA**))[166]. Furthermore, the CNIL mentions that the re-use of databases to drive AIS is possible provided that the data has not been collected in a "manifestly illicit" manner and that the re-use is compatible with the initial collection[167].

Faced with this need for coordination, the CNIL has issued recommendations for providers, whether they are acting as data controllers or data processors[168]. These AI operators must comply with a number of steps to ensure the proper use of personal data in AI Systems. First of all, they will have to define the purpose of the processing when they set up a personal database. This means clearly defining the purpose of their system, drawing up specifications that minimise the impact on data subjects. This includes defining the expected results, performance indicators and contexts of use[169], in order to avoid excessive data collection. Techniques must also be chosen to ensure that no more data is processed than is necessary in application of the data minimisation principle. Furthermore, the processing must be lawful: the legal basis for the processing of personal data must be clearly defined by the AI System, ensuring that it is both relevant and valid. A Data Protection Impact Assessment (**DPIA**) prior to the deployment of an AI System, particularly for high-risk systems, may be necessary to minimise risks. It may also be necessary to have the choices made validated by pilot studies or to obtain the opinion of a multidisciplinary and independent ethical committee, to ensure the technical and ethical relevance of the data and methods used. Operators will have to transparently inform data subjects about the use of their data by the AI System and about their rights under the GDPR. Finally, downstream, operators will have to guarantee the security of the AIS, in particular by putting in place regular control and audit mechanisms to ensure the ongoing compliance of the AI System and the data processed.

The future application and interpretation of the principles of the AI Act and the GDPR should lead regulators to deliver continuous educational efforts towards the professionals..

---

165 *Article 5 of the GDPR.*

166 *Proposal for a Regulation on a Framework for Financial Data Access, European Commission (2 December 2024) (link).*

167 *CNIL, AI and GDPR: the CNIL publishes its new recommendations to support responsible innovation, Recommendation, 7 February 2025.*

168 *See CNIL, IA factsheets, Recommendations.*

169 *However, the re-use of data for purposes not initially intended is and remains possible, subject to additional steps being taken, such as a compatibility test. In this respect, the CNIL specifies that the re-use of data to improve models is not, prima facie, a purpose that is "incompatible" with the initial purpose. See CNIL, Réutilisation de bases de données: les vérifications nécessaires pour respecter la loi, 23 January 2025.*

(b) Sources of conflict between the key principles of the GDPR and the purposes of AI

As mentioned above (see below), compliance with the essential principles of the GDPR at all stages of the development and deployment of an AI System can be complex. For example, the GDPR requires that principles such as minimisation, purpose limitation or accuracy be respected by the provider and the deployer when collecting data for training the AI System, using it for training, using it as output data, or when reintegrating the data into the system in order to improve it. By way of illustration, the principle of accuracy should apply when data is collected; as such, this would require the data controller to check that all personal data intended for training its model is accurate. However, as this data is generally collected by scraping data that is freely available online, carrying out an accuracy verification operation would in practice be complex, despite the existence of initial solutions[170]. The same principle of accuracy applies to output data. So, assuming that the training data was accurate, the provider would also need to ensure the accuracy of the data generated by the AI System. This would require an additional verification step that could prove complex due to the lack of certified input data to validate the accuracy of the output data. In this regard, in April 2024, NOYB, a data rights advocacy group filed a complaint against OpenAI with the Austrian Data Protection Authority arguing that ChatGPT provided inaccurate output data in response to a prompt.

(i) Tension over transparency

The exception to the obligation to provide information set out in Article 14(5)(b) of the GDPR, which states that this exception applies if the provision of information proves impossible or would require a disproportionate effort, is tricky to implement, depending on the context in which the data is collected. This exception applies to processing for archival purposes in the public interest, for scientific, historical or statistical research purposes, but also in cases where bodies that are not, or are no longer, in contact with the data subjects do not have at their disposal the information that would enable them to provide individual information. In practice, data protection authorities ask data controllers to assess and document the disproportionate nature of individual communication to data subjects in relation to the actual invasion of their privacy in the absence of such individual information[171]. Thus, the authorities recognise that informing data subjects individually may in some cases require disproportionate efforts on the part of the controller. In such cases, the controller could provide general information on its website, supplemented where necessary by appropriate additional measures[172].

---

170 *These solutions involve, for example, excluding certain sites from the sources of personal data collection by default, or limiting data collection to data that is freely accessible.*

171 *A large number of factors may be taken into account (absence of information enabling the data subjects to be contacted, age of the data used by the data controller, large number of data subjects concerned by the information to be provided, whether or not the processing envisaged is intrusive, whether or not there are particular risks to the data subjects associated with the implementation of the processing, the type of data subjects concerned by the individual information, etc.).*

172 *CNIL, AI: Informing the people concerned, Recommendation, 7 February 2025.*

(ii) Tension over exercising the rights of data subjects

Under the GDPR, data subjects have various rights they can exercise towards data controllers (e.g. right of access, erasure, rectification, etc.). However, it may prove difficult for a data controller who processes personal data for purposes related to an AI System to comply with some of these requests; such a situation may even require the data controller to update the organisation of its operational processes. For example, if an individual identifies that output data contains personal data associated with him or her, he or she must be able to request its deletion or modification in accordance with the rights guaranteed by the GDPR. However, this means that the data used to drive the system must be identified as relating to the data subject, which is not always immediately possible for the data controller. In many cases, this could even lead the controller to carry out additional processing for the purpose of identifying the data subject. However, the GDPR stipulates that the data controller is not obliged to process additional information or retain personal data for the sole purpose of complying with the Regulation or responding to requests from data subjects. However, the situation can be simplified when the data subject himself provides information that enables him to be identified: by inviting him to proceed in this way, the data controller can reconcile seemingly contradictory imperatives. Finally, it is also possible that the data in question was generated by the AIS. In practice, responding to these requests would therefore require data to be classified (possibly by means of metadata) so that, in the event of a request from a data subject, it would be possible to link the individual to the data concerning him or her among those processed. In this respect, at the European Data Protection Committee's "Stakeholder event on AI models" on 5 November 2024, several stakeholders stressed the fact that, once trained, an AI model did not constitute a database within which it is possible to easily search for data associated with a particular person. Considering that such a search is not impossible, the CNIL recommends that, in response to this analysis, an internal procedure should be established consisting of interrogating the model to check what data it might have stored concerning the person concerned[173]. Once the request has been processed, the data controller must ensure that this decision is reflected in the AI System (e.g. for a rectification request, that its system generates output data in line with the requested modification and that obsolete data is no longer processed, by re-training the model without the disputed data, for example).

It should be noted that cost, impossibility or practical difficulties may sometimes justify a refusal to such requests; when the right must be guaranteed, the CNIL will take into account the reasonable solutions available to the creator of the model and the timeframe conditions may be adjusted. Scientific research is evolving rapidly in this field, and the stakeholders involved must keep abreast of developments in the state of the art in order to protect people's rights as effectively as possible.

(iii) Tension over legal basis

The GDPR provides that any processing of personal data must be founded on an appropriate legal basis. With regard to the processing of personal data in the context of the development and

[173] *CNIL, AI: Respecting and facilitating the exercise of data subjects' rights, 7 February 2025.*

deployment of AI Systems, the CNIL has pointed out that legitimate interest is likely to be the legal basis most frequently used by professionals. It provides support to professionals wishing to base their processing on this legal basis, in particular by putting forward safeguards which, implemented according to the risks presented by the processing, would ensure a fair balance between the various interests involved[174]. However, the GDPR provides that where processing is based on legitimate interest, the data subject may exercise his or her right to object, thereby obliging the controller to cease processing the information concerning him or her. As mentioned above, the implementation of this right is particularly complex in the case of an AI System, but it is possible, in certain cases, to justify a refusal or to arrange the conditions for following it up[175].

(iv) Tension over the application of the two regulations

Finally, the authorities responsible for applying the AI Act could be different from those responsible for applying the GDPR (where the AI Act does not prescribe the competence of the data protection authorities). In this respect, cooperation between the authorities concerned will be necessary to avoid divergences in the interpretation of the applicable principles.

3. AI Act, DORA and NIS 2

Although they have distinct objectives, the AI Act and Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a common high level of cybersecurity throughout the Union (Network and Information Security) (**NIS 2**) may interact in a residual manner. In fact, the DORA regulation acts as a *lex specialis* in relation to NIS 2[176]. The two texts specify that the Member States must first apply DORA to Financial Institutions, in line with the broader European cybersecurity framework[177]. While the relationship between these two texts and the AI Act depends on the transposition of NIS 2 into national law, several observations can be made.

With regard to the cybersecurity of AI Systems, the AI Act imposes strict robustness and security requirements on high-risk AI Systems, while NIS 2 strengthens organisations' cybersecurity obligations, including the protection of critical systems using AI. For example, an AI System used to detect fraud in banking transactions will have to simultaneously meet the security standards of the AI Act and the cybersecurity requirements set by NIS 2, assuming they exceed the DORA framework. It should be noted that the Cyber Resilience Act[178] (**CRA**) should also be taken into consideration as a complementary text to NIS 2 covering "products with digital elements", i.e.:

- "A software or hardware product and its remote data processing solutions, including separately marketed software or hardware components"[179]; and of which

---

174 *AI: Mobilising the legal basis of legitimate interest to develop an AI system, CNIL, 10 June 2024.*

175 *CNIL, AI: Respecting and facilitating the exercise of data subjects' rights, 07 Feb. 2025.*

176 *It should be noted that the bill on the resilience of critical infrastructures and the strengthening of cybersecurity adopted by the Senate on 13 March 2025 limits the predominance of the lex specialis DORA to risk management, incident reporting and supervision (art. 62A).*

177 *Recital 28 of NIS 2 and recital 16 of DORA.*

178 *Regulation 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital components.*

179 *Article 3(1) of the CRA.*

– the "intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network"[180].

This scope covers "smart" objects[181] beyond the scope of high-risk AI.

In terms of incident management, NIS 2 requires rapid notification of cybersecurity incidents that have a significant impact. If an AI System is involved in an incident, such as an attack exploiting a vulnerability in that system, this may require a double analysis to ensure compliance with both regulatory frameworks (not forgetting the notification imposed by the GDPR)[182].

The two texts also provide for regular audits and compliance mechanisms. Entities using AI Systems in critical sectors must therefore coordinate their efforts to comply with the requirements of both regimes.

C. Environmental sustainability rules in the context of AI/AI Act use

1. Sustainability, a strategic challenge for the banking and financial sector

For several years, the sustainability framework has been a strategic issue aimed at working towards sustainable development through a transition to low-carbon economies that respect the environment, use resources efficiently and promote equity and social justice[183].

In the banking and financial sector, environmental, social and governance sustainability issues are no longer just a trend but a general framework that incorporates strategic thinking on financing economic transition. This is demonstrated by the European work undertaken following the publication in March 2018[184] of the action plan for financing sustainable growth, renewed in 2021 in the form of a strategy for financing the objectives of the Green Pact for Europe, namely, "a society that is climate-neutral by 2050, efficient in its use of environmental resources and supportive of the regions and people particularly affected by this transition"[185].

The European action plan on sustainable finance has led to significant changes, with the banking and financial sector identified as being key to facilitating part of the financing of economic

---

180 *Article 2(1) of the CRA*

181 *Appendices III and IV of the CRA.*

182 *Cf. also the provisions of the DORA regulation, with the proviso that the provisions of the latter, as lex specialis, take precedence over those of NIS 2.*

183 *The term "sustainable development" first appeared in 1980 in the* ***World Conservation Strategy****, a publication of the International Union for Conservation of Nature (IUCN). The concept was taken up again in 1987 in the report of the* ***World Commission on Environment and Development, Our Common Future*** *(also known as the Brundtland Report). It is from this report that the definition recognised today is taken: "Development that meets the needs of the present without compromising the ability of future generations to meet their own needs".*

184 *Communication from the Commission to the European Parliament, the European Council, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, Action Plan: Financing Sustainable Growth, 8.3.2018 COM (2018) 97 final.*

185 *Communication from the Commission to the European Parliament, the European Council, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, Financing the transition to a sustainable economy, 6.7.2021 COM (2021) 390 final.*

transition. With the adoption of stringent legal and regulatory requirements[186] and increased stakeholder awareness, Financial Institutions have gradually adopted environmental sustainability criteria, integrating them into the various aspects of their banking and financial activities: investment strategies and decisions, project and asset financing, risk management framework, sustainability publications, etc.

As part of the implementation of the new environmental sustainability obligations, Financial Institutions have identified that a wide range of issues need to be addressed alongside other more traditional risks.

These questions and issues concern, in particular, the evaluation and comparison of the environmental sustainability performance of different investments when reliable, standardised ESG data is rare or non-existent. Adapting to a legal and regulatory framework for environmental sustainability that is evolving rapidly and varies considerably from one jurisdiction to another can also prove complex. Another major challenge is integrating environmental sustainability criteria into existing financial models and decision-making processes, while taking adequate account of ESG risks and opportunities.

These new issues require changes and technical adjustments that can be complex and resource-intensive.

AI's ability to analyse large datasets efficiently and accurately can be a key asset in managing environmental sustainability. For example, AI could process and interpret large-scale environmental data, enabling Financial Institutions to assess climate-related financial risks more accurately and prudently.

From this perspective, AI could become an essential tool for navigating the complex interplay between financial activities and environmental sustainability objectives.

However, while the sudden rise of AI promises to successfully transform the integration of sustainability into the financial sector, it also presents new complexities for those involved in sustainable finance.

One of the impacts directly linked to the objective of sustainable development defined in 1987 in the Brundtland Report as “development that meets the needs of the present without compromising the ability of future generations to meet their own needs” concerns the environmental damage that would be caused by the indiscriminate use of AI in the financial sector.

Admittedly, the transposition of the CSRD directive into French law and duty of vigilance would require a large number of entities in the financial sector to ensure that the environment was

---

186 *See in particular, Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27 November 2019 on the publication of sustainability information in the financial services sector, Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020 on the establishment of a framework to promote sustainable investment and amending Regulation (EU) 2019/2088, the information to be published under Article 449 of Regulation No 575/2013 on prudential requirements for credit institutions.*

respected and to disclose their environmental impact. But these texts do not impose specific environmental requirements relating to the creation and use of AI.

Does this mean that other texts govern the impact of AI and digital technology on the environment?

2. The role of the environment in the AI Act

The AI Act contains a number of provisions that explicitly address the environment and aim to improve transparency on the impact of AI in this area (cf: Recital 27: "AI systems are developed and used in a sustainable and environmentally friendly manner"; Recital 48: "The fundamental right to a high level of protection of the environment, enshrined in the Charter and implemented in the policies of the Union, should also be taken into account when assessing the seriousness of the harm that an AI system may cause"; Recital No 165: "Providers and, as appropriate, deployers of all AI systems, high-risk or not, and AI models should also be encouraged to apply on a voluntary basis additional requirements related, for example, to the elements of the Union's Ethics Guidelines for Trustworthy AI, environmental sustainability (...)"; Article 95(2)(b): "The AI Office and the Member States shall facilitate the drawing up of codes of conduct concerning the voluntary application, including by deployers, of specific requirements to all AI systems, on the basis of clear objectives and key performance indicators to measure the achievement of those objectives, including elements such as, but not limited to: […] assessing and minimising the impact of AI systems on environmental sustainability, including as regards energy-efficient programming and techniques for the efficient design, training and use of AI;").

With regard to the environmental impact of AI, European regulations do not define sustainability standards for AI Systems as such, leaving the responsibility for such a definition to the Member States[187]. The AI Act must therefore be mirrored in French domestic law, to consider in particular the possible legal consequences of the transparency of the environmental impact of AI Systems.

3. The carbon footprint of digital technology in French law

Caught between conflicting injunctions to promote a digital-friendly economy while at the same time embracing a policy to combat climate change and carbon emissions, the French legislature has struck a balance with Law 2021-1485 of 15 November 2021 aimed at reducing the environmental footprint of digital in France (known as the REEN Law). The aim of this law is to make the hidden ecological costs of digital technology visible, by encouraging businesses to adopt more responsible digital practices, with an emphasis on awareness-raising, eco-design, sustainable equipment management and the energy efficiency of infrastructures. However, during the parliamentary debates, a provision aimed at including the environmental impact of digital technology in the extra-financial performance declaration of companies was proposed before being deleted at the end of the parliamentary process. It is remarkable that the legislature should have envisaged transparency of the environmental footprint of digital technology as part of the information published under company law. Although the proposal has not been adopted at this stage, it reveals a very clear trend

187 *Senate Report No. 379, 2024-2025, AI and the future of public service, p. 37.*

towards making the environmental footprint a new "indicator" or at least an element of corporate accountability[188]. We must therefore be vigilant about how this environmental transparency is received by investors, and consider the possible legal implications of this information with regard to the requirement for "accurate, precise and fair" information (article 223(1), RG AMF). In addition to the need for environmental transparency, the impact of the use of digital technology and AI Systems could be subject to a cost-benefit analysis by Financial Institutions. This would enable them to weigh up the benefits of using AI against the energy costs that this technology could generate, particularly when it is used to perform certain tasks in place of existing technologies[189].

D. The relationship between intellectual property protection and the AI Act

1. The Directive on copyright and related rights in the digital market and the AI Act

In Europe, the Directive on copyright and related rights in the digital market (**Directive (EU) 2019/790 of 17 April 2019**) introduced an exception for text and data mining (TDM), allowing protected content to be used for research and innovation purposes.

Under these rules, rights holders can choose to reserve their rights in their works and other protected subject matter to prevent text and data mining, unless this is done for scientific research purposes. Where the reservation of rights has been expressly made in an appropriate manner, providers of general-purpose AI models must obtain permission from rights holders if they wish to carry out text and data mining on these works (Recital 105 of the AI Act).

There are few references to intellectual property in the AI Act, nevertheless Article 53 of the AI Act incorporates obligations on this subject: "1. Providers of general-purpose AI models shall: [...] (c) put in place a policy to comply with Union law on copyright and related rights, and in particular to identify and comply with, including through state-of-the-art technologies, a reservation of rights expressed pursuant to Article 4(3) of Directive (EU) 2019/790;".

Nevertheless, putting these provisions into practice still raises many questions, not only for suppliers but also for AI deployers or users.

2. AI users and intellectual property rights

The data used to draft prompts or to feed AI Systems may contain information protected by intellectual property rights but also sensitive information protected by laws relating to trade secrets or banking secrets. AI users may not be aware that the data they are exploiting could infringe intellectual property or trade secrets or breach confidentiality obligations.

---

188 *Marina Telller, De la RSE à la RNE: la petite lettre qui change tout, Mélanges AEDBF, vol.8, Revue Banque, 2022, (hal-03480269).*

189 *ESMA, Institut Louis Bachelier, The Alan Turing Institute, Leveraging Large Language Models in Finance: Pathways to Responsible Adoption, Working papers, 2025, p. 24.*

It is essential that users are trained and informed about the legal implications of using data of this type, as well as the risks associated with exploiting information that is potentially protected by specific rights such as trade secrets.

A good practice guide for users can reduce this type of risk linked to their input, in particular by asking them to:

- not to use data protected by intellectual property or confidential data/commercial/professional secrets of the user's company when using the AI tool;
- check that the results of prompts made on the tool do not infringe the obligation to protect certain data through searches on Google or other search engines;
- study the conditions and terms of use of the AI tool with regard to the use made of the data provided.

3. Providers and their AI training model and deployers confronted with intellectual property rights

The data used to train AI models may include works protected by intellectual property rights, such as texts, images or sound recordings.

The AI Act sets out requirements for the activities of suppliers and deployers, although references to intellectual property in the AI Act are limited.

Article 53 of the AI Act states that providers of general-purpose AI models must put in place measures to ensure compliance with copyright, in accordance with Directive (EU) 2019/790 of 17 April 2019. Among these measures, providers are required to create and make publicly available "a sufficiently detailed summary" of the data used to train the AI model.

This requirement for transparency of sources should enable holders of copyright and related rights to ensure that the conditions for access to and use of their works have been complied with, and, where appropriate, to exercise their right to object to any use of their data, i.e. their "opt-out". This obligation will take effect twelve months after the regulation comes into force, i.e. on 2 August 2025. The AI Office, established by a decision of the European Commission on 24 January 2024, will be responsible for devising a clear and effective model for summarising the training data used by AIs. The obligation to respect copyright and provide this summary will apply to AI providers offering models within the EU, regardless of where these models were trained.

In the third version of the draft code of practice for general-purpose AI models (GPAI) published by the AI Office on 11 March 2025, it is mentioned that providers who sign this code acknowledge that any use of copyright-protected content requires the permission of the relevant rights holder(s), unless exceptions and limitations to copyright apply (cf. recital no. 105 of the AI Act).

The copyright section of the Code of Practice sets out commitments that suppliers of general-purpose AI models must meet in order to comply with EU legislation. This draft aims to simplify and clarify the obligations compared to previous versions, while maintaining the essential elements.

The third draft Code of Practice for General Purpose AI includes a section on copyright, setting out commitments for providers of AI models. This section aims to ensure compliance with EU copyright law, in accordance with Article 53(1)(c) of the AI Act.

The main points are as follows:

(a) Compliance policy: signatories must develop, update and implement a copyright policy, which includes specific commitments to respect copyright and related rights.

(b) Specific measures: signatories must also develop a copyright policy that is documented and supervised within the organisation. They will ensure that only legally accessible content is reproduced or extracted during web browsing. They will have to identify and respect reservations of rights during exploration, obtain adequate information about unexplored protected content, mitigate the risks of AI models generating results that infringe copyright, and designate a point of contact for communication with rights holders and establish a complaints mechanism.

(c) Proportionality: the commitments must be adapted to the size and capacities of the signatories, taking into account small and medium-sized businesses.

(d) Respect for copyright: the section does not diminish the application of existing copyright laws and commercial agreements between signatories and rights holders.

This code aims to establish a clear framework for suppliers of AI models to respect copyright, while incorporating communication and accountability mechanisms.

4. AI-generated creations

The emergence of AI also raises important questions about the works it generates. The ownership of copyright in these creations is a subject of significant legal debate.

(a) Ownership of copyright

The question of who becomes the owner of the rights to creations generated by AI is a complex one. In many cases, the general terms and conditions of use (GTCU) of AI tools stipulate that rights can be assigned to users. However, it is crucial to question the clarity of these assignments and the rights that are actually transferred.

Two scenarios need to be distinguished: that of **autonomously generated creations**. When AI produces content without human intervention, the ownership of rights may be unclear and will depend on contractual stipulations. In these cases, there will be a risk in using this type of work, since it could be copied if it is not protected by intellectual property rights (subject to cases of

parasitism, etc.). And a second scenario of **AI-assisted creations**: when the user modifies the content generated by the AI, this could strengthen the user's claim to copyright, especially if he or she makes a significant creative contribution.

(b) Risks associated with exploiting AI-generated content

Exploiting content generated by AI also entails legal risks, particularly in terms of counterfeiting. If AI generates content that is similar or identical to a protected work, two scenarios may arise. On the one hand, the supplier will have to pay compensation: some AI tool suppliers offer compensation in the event of infringement in their general terms and conditions, provided that the user is not at fault and with certain limits on the amount or limits on certain guarantees for the image of the goods or people represented. This protects users to a certain extent, but they still need to be diligent in using the tools. On the other hand, the user may be held liable in other cases where the provider declines all liability, and the user must take full liability for the exploitation of the content generated. This poses challenges for users who may not be fully aware of the legal implications of their choices.

IV. Liability at stake for Financial Institutions

A. Full liability of Financial Institutions towards their clients/investors and the supervisory authorities

The AI Act and sector-specific European provisions, such as MiCA and DORA, are *ex ante* rules defining obligations for operators[190]. These rules constitute the essential part of the applicable legal framework, but do not contain, rules relating to the liability of operators. They usually provide for sanctions in the event of breaches of the obligations they impose, but their purpose is not to compensate for the losses suffered by potential victims and caused by the operators' activities. As regards the ex-post treatment of damage caused by the use of IT technologies, and AI in particular, the legal framework, both European and national, is still relatively uncertain, particularly following the withdrawal of the proposed directive of 28 September 2022 on the adaptation of the rules on non-contractual civil liability rules to AI. This withdrawal is regrettable at this stage if we consider the risk of damage, of varying kinds, caused by the frequent and increasing use of AI Systems. The new risk of damage is linked to the characteristics of the technologies used, namely their complexity, opacity, autonomy, unpredictability, openness to the outside world, dependence on data and vulnerability.

The risks generated by AI Systems and other IT technologies are particularly significant in sectors such as financial services, where the malfunctioning of AI Systems is likely to have a major impact both on the protection of individuals (e.g. a robo-adviser causing errors that could cause serious economic damage to an individual investor) and on market stability.

The main assumptions relating to the use of the technologies in question that could give rise to damage and therefore liability are: credit scoring, the use of robo-advisers, high-frequency trading, the internal organisation of institutions and compliance and risk management. As for the characteristics of AI technologies that give rise to an increased risk of liability, these are mainly:

- the training of models/algorithms on the basis of data that are insufficiently relevant, unrepresentative, inadequate and that reproduce existing biases in society;
- interconnection with other systems or data sources (particularly in credit scoring or high-frequency trading) that may disadvantage borrowers or hinder the proper functioning of the trading algorithm;
- the use of external data, making the development of self-learning systems unpredictable, vulnerability to cyber-attacks and leaks of personal and confidential data. The resulting liability risks apply not only to the developers and suppliers of the technologies in question, but also to those who use them.

190 *These sector-specific rules may refer to the rules of civil liability, most often national, in the event of damage caused by breaches of the obligations they contain, but without further details as to the content of the rules, the basis of liability and its regime.*

Indeed, the more Financial Institutions use AI Systems and applications, the closer the link between the legal rules applicable to financial markets, on the one hand, and liability rules, on the other, is likely to become[191]. The relationship between these two bodies of rules must therefore be analysed precisely and progressively, given the evolving legislative context in this area. At the same time, it becomes more complex to assess liability and compliance with applicable legislation without highly structured governance[192]. Liability rules (current or future, specifically applicable to AI), particularly those in Europe, will therefore have a greater impact on Financial Institutions to the extent that they use AI and other IT technologies in the design and delivery of the regulated services concerned. The liability rules will, in a way, make the obligations arising from the *ex ante* rules applicable to Financial Institutions (AI Act and sector-specific regulation) more effective.

The liabilities that Financial Institutions are likely to assume as a result of the use of AI Systems may therefore be multiple. These liabilities may vary according to the Financial Institution's more or less significant contribution to the development of the AI System which will be at issue in the violation of imperative standards and/or in the production of harm. The wider the category of operators, the wider the field of liability[193]. Depending on the circumstances, it will be necessary to identify the most relevant event giving rise to liability (design or use and modification of the system) and to designate the most appropriate person responsible.

As for relationships with clients/investors, it will be appropriate to consider classic contractual breaches involving an AI System (e.g. bad advice...), for which the use of AI Systems should not radically change the way liability is envisaged compared to the current situation, except that the hypotheses of lack of sufficient human supervision could be more numerous. The damage that is likely to be caused in this case and the liability (both contractual and extra-contractual) arising from it are, on the whole, classic. As far as professional customers are concerned, conventional contractual limitation or exemption clauses, slightly adapted to the use of AI Systems, should make it possible to maintain exposure to liability at levels comparable to those currently in force. Such an approach will be more complex in the case of customers, who are then considered to be consumers, and who may rely in particular on the law relating to unfair terms (e.g. terms limiting or exonerating liability considered to be unfair), the arsenal relating to contractual formalism and the duty to inform, the applicable rules of good conduct, or even the law relating to unfair commercial practices. Particular care must therefore be taken when using AI Systems with customers who are consumers.

Conversely, damage of a partly new nature must also be considered. Indeed, AI Systems, due in particular to insufficient input data or data of approximate quality, but also to biases likely to interfere in the machine learning mechanisms, generate damages that largely fall within the field of extrapatrimonial damages (e.g. injury to dignity, discrimination, etc.), the scale of which may be

---

191 *The bodies of sector-specific rules and the AI Act, on the one hand, and the liability rules, on the other, are intended to be more closely integrated (e.g. the obligation to supervise Financial Institutions is equivalent to the deployer's obligations under article 26 AI Act).*

192 *ESMA, Artificial Intelligence in EU securities markets, (2023) https://www.esma.europa.eu/sites/default/files/library/ESMA50-164-6247-AI_in_securities_markets.pdf.*

193 *See article 3(8) AI Act: "operator" means a supplier, product manufacturer, deployer, agent, importer or distributor.*

particularly significant. These new types of damage will have to be examined in greater detail because they are inherent in the use of AI Systems.

Directive (EU) 2020/1828 of 25 November 2020 on representative actions may also be a point of attention. The AI Act is one of the texts covered by this directive, which opens the way to representative actions for breaches of EU law by professionals. This directive has probably not yet been transposed into French law, but it could lead to a significant change in liability exposure, particularly if we take into account the development of third-party funding.

B. A nascent extracontractual liability regime

The rules on civil liability for AI at European level are fairly limited for the time being, at least until the new “defective products” directive comes into force. This directive dated of 23 October 2024 must be transposed into the laws of the Member States within two years of its publication. Thus, for the time being, damage arising from the use of AI Systems will be compensated on the basis of national rules of extra-contractual and/or contractual liability (or even on the basis of national rules specific to damage caused by AI). It should be noted that the European legislator has introduced liability rules specific to the financial markets, such as those for credit rating agencies (e.g. CRAR), investment firms or, more recently, issuers of digital assets (MiCA), which will be applied in parallel with the liability rules that are partially specific to AI.

Liability for defective products applies to products and not to services, the latter being generally based on fault. The system of liability for defective products is known as no-fault liability because the basis of this liability is the defectiveness of the product. If this defect causes damage, then the producer/manufacturer will be liable. The new directive has a broader scope than its predecessor. It applies beyond the category of producers in the strictest sense (all the “economic operators” mentioned in Article 8). In this respect, it should be noted that an economic operator may be subject to liability for defective products and therefore considered to be a manufacturer when he “substantially modifies a product outside the manufacturer's control and then makes it available on the market or puts it into service”. In the future, it will be necessary to determine whether deployers of AI Systems or users of computer technologies will be treated as manufacturers, and subject to this liability regime, because they have substantially modified this type of product, for example through local training of systems.

This is all the truer given that, in terms of its material scope, the new directive on liability for defective products formally includes software in the product category. So if a Financial Institution develops a programme/algorithm locally, e.g. for credit scoring, whether or not the programme incorporates AI, it could in theory be considered a producer within the meaning of the new directive on defective products. Making these products available to customers could then be considered as putting the product into circulation or placing it on the market, which would trigger the risk of liability.

It should be noted that the “defective products” directive only covers material damage, but not non-material damage (for this kind of damage, it will be necessary to refer to national law, which will be the case, for example and in all likelihood, for cases of discrimination, loss of opportunity, anxiety loss, etc.), or pure economic loss.

The proposal for a directive of 28 September 2022 on the adaptation of the rules on non-contractual civil liability rules to AI, withdrawn from the European Commission's legislative programme in February 2025, aimed to establish a regime essentially based on fault, which could arise in particular from non-compliance with ex ante provisions, such as the AI Act. Its main contribution was to be in the area of access to information held by the defendant (disclosure), on the one hand, and in the establishment of presumptions (fault and causality between the fault and the output of an AI causing damage) benefiting the plaintiff, on the other. The provisions of the proposed directive focused essentially on high-risk AI Systems. Despite its imperfections, this proposal for a directive had the merit of introducing a link between the body of ex ante rules (AI Act) and the body of ex post rules (directive on extra-contractual liability for damage caused by AI).

At this stage, the relationship will most likely be with national liability rules, on the one hand, and the rules of the directive on liability for defective products, on the other. Pending a specific civil liability regime for damage caused by AI, there seems to be nothing to prevent breaches of the various obligations arising from the AI Act and sectoral rules from characterising fault-triggering liability. Even if, for the time being, the rules on access to documents and presumptions contained in the proposal for a directive on extra-contractual liability for damage caused by AI are no longer relevant, it seems important to emphasise the training of staff deploying AI Systems, as well as the monitoring and documentation of the use of these systems.

C. Contractual liability of AI providers to be negotiated

The different positions occupied by Financial Institutions must be considered. As clients, Financial Institutions using AI Systems service providers will have to ensure that any limitation or exoneration clauses proposed by the said providers are not excessively broad, as the liability risks for the AI Systems deployer are quite significant. On the other hand, Financial Institutions may wish to stipulate clauses under which damages suffered as a result of the use of the AI Systems provided, such as damage to reputation, will be compensated by the co-contractor.

As deployers of AI Systems, Financial Institutions will take care to stipulate clauses limiting or exonerating their liability for damage caused by the use of AI Systems, which will only be possible in relation to professional clients.

If Financial Institutions are considered to be suppliers or producers of AI Systems, the liability regime incurred being in particular that based on liability for defective products, the limiting or exonerating liability clauses cannot be invoked insofar as this liability regime is extra-contractual.

CONCLUSION

The use of AI by Financial Institutions is subject not only to well-established sector-specific regulations, but also to an abundance of specific regulations that are open to interpretation[194].

The task of coordinating the various sets of regulations needs sometimes to be balanced with a degree of risk involved.

Three levels of uncertainty were particularly highlighted:

- the supervisory authority for Financial Institutions for the application of the AI Act has not yet been formally designated in France – once it has been designated, it will be necessary to determine how the supervision of the implementation of the AI Act and the disciplinary regimes that already apply to Financial Institutions will work together in the future.

  An additional challenge also arises in terms of European coordination. If other Member States were to follow the French example and divide up the prerogatives linked to the application of the AI Act between several authorities, the harmonisation of practices could be affected and differences of interpretation could arise. In addition, there is a risk that certain Member States will opt out – voluntarily or otherwise – creating disparities in the application of the AI Act, which could encourage certain stakeholders to set up in one country rather than another. To compensate for these discrepancies, it might be appropriate to establish an authority in each Member State responsible for liaising with the European authorities. In this way, both national and European authorities will have to cooperate in order to work together on coherent educational work, upon the initiative in particular of the AI Office and the European Commission;

- the integration of the new AI Act obligations into the normative field of Financial Institutions, the mechanisms of equivalence or complementarity of the AI Act rules with sectoral regulations remaining largely open to interpretation; and

- the link between the AI Act and other cross-sector regulations already governing Financial Institutions, in particular the GDPR and DORA, adds a further level of complexity.

While the use of AI undeniably presents the means for development and efficiency for Financial Institutions, the additional regulatory burden involved will weigh heavily on the decision to use it. The AI Act based on the protection of fundamental rights also opens up unusual territory for Financial Institutions with their own specific liability issues.

---

194 *As highlighted in the report published by ESMA, the Institut Louis Bachelier and the Alan Turing Institute, the vast majority of jurisdictions consulted by the OECD indicated that they had adopted an AI policy covering, at least in part, the banking and financial sector (ESMA, Institut Louis Bachelier, The Alan Turing Institute, Leveraging Large Language Models in Finance: Pathways to Responsible Adoption, Working papers, 2025, p. 28).*

The impact of the application of the AI Act on the competitiveness of European Financial Institutions is also a concern, making it imperative for the European Union to be able to enforce it extraterritorially. Note that in his report "The Future of European Competitiveness" (9 September 2024), Mario Draghi stated that the regulatory burdens weighing on AI researchers and developers in Europe are a real roadblocking to the development of AI projects by European industry stakeholders and could ultimately encourage them to develop their AIS outside the EU. In this regard, the European Commission is currently considering two consultations to ease the burden of AI Act compliance on SMEs[195]. Simplifying the implementation of the AI Act is also being considered by postponing its application to extend the compliance deadlines[196].

This pyramid of overlapping texts governing the use of AI has naturally led the working group not to propose other texts[197] or even amendments to existing texts, but rather to carry out this coordinating analysis work.

All the initiatives were welcomed, in particular those taken by the European Commission[198] to clarify the links between the regulations applying to the use of AI by Financial Institutions.

In line with the European AI action plan[199], the working group calls on the supervisory authorities and legislators to respond as effectively as possible to the requests for simplification and clarification from Financial Institutions, with a view to promoting genuine consistency between sectoral and cross-sectoral regulations and those governing AI specifically.

---

195 *See European Commission releases analysis of stakeholder feedback on AI definitions and prohibited practices public consultations, 12 May 2025 and Commission launches public consultation and call for evidence on the Apply AI Strategy, 9 April 2025.*

196 *The simplification would be based on the 'Stop-the-clock' directive, which is part of the 'Omnibus I' package (or "Suspensive" directive) that entered into force on 17 April 2025 and would allow the application dates of certain AI Act obligations to be postponed.*

197 *This position is in line with that of the ECON draft report dated 14 May 2025: "[The European Parliament] warns against the adoption of new sectoral legislation to regulate AI in financial services, as there are already established sectoral rules that cover AI deployment; believes that this would create additional layers of complexity and uncertainty and ultimately deprive the sector of the benefits of AI use; strongly advises the Commission and the Member States to coordinate to avoid gold-plating relevant legislation and to prevent the creation of new barriers in cross-border markets; [...].*
"The alternative is to take a restrictive approach to AI deployment in finance, with new legislation out of fear of the unknown effects, or because status quo is comfortable. Such a policy would deprive the financial services sector of the opportunity to use AI. [...]. Such a route should be off the table considering the global race for AI, the stark geopolitical realities underpinning it, and the fact that the EU is already lagging behind." (European Parliament, ECON, Draft report on impact of artificial intelligence on the financial sector (2025/202565INI)), 14 May 2025.

198 *European Commission, Consultation document – Target consultation on artificial intelligence in the financial sector, 18 June 2024.*

199 *European Commission, Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions – AI Continent Action Plan, 9 April 2025, p. 3: "Fifth, the EU's large single market is a significant asset, with one set of clear rules, including the AI Act, preventing market fragmentation and enhancing trust and security in the use of AI technologies. Nevertheless, there is a need to facilitate compliance with the AI Act, particularly for smaller innovators"; p. 22: "The Commission will continue to work with the AI Board of Member States, which assists in providing guidance on the application of the AI Act, including within the context of sectoral legislation." and p. 23: "[...] we should first gain experience in applying these new horizontal rules and evaluate their effect before any possible new legislation on AI can be considered.".*

ANNEX 1 – PARTICIPANTS IN THE WORKING GROUP "THE LEGAL AND REGULATORY IMPACTS OF ARTIFICIAL INTELLIGENCE IN BANKING, FINANCIAL AND INSURANCE MATTERS"

PRESIDENT:

Brice HENRY, Partner, Allen Overy Shearman Sterling LLP

VICE-PRESIDENT:

Laurie-Anne ANCENYS, Partner, Allen Overy Shearman Sterling LLP

REPORTERS:

Maxence KIEKEN, Associate, Allen Overy Shearman Sterling LLP

Constantin BEYTOUT, Senior Associate, Allen Overy Shearman Sterling LLP

Pascal MOLINELLI, Counsel, Allen Overy Shearman Sterling LLP

Morgane-Aude ROUSSEL, Senior Associate, Allen Overy Shearman Sterling LLP

HCJP REPRESENTATIVES:

Jean-Guillaume DE TOCQUEVILLE, Secrétaire Général, Haut Comité Juridique de la Place Financière de Paris

Gérard GARDELLA, Ancien Secrétaire Général, Haut Comité Juridique de la Place Financière de Paris

AMF REPRESENTATIVES:

Maxence DELORME, Directeur des affaires juridiques

Clément SAUDO, Directeur, Division Marchés financiers et services sur crypto-actifs, Direction des affaires juridiques

Olivier BROCHAND, Senior Policy Officer, Division Innovation et Finance Digitale, Direction de la régulation et des affaires internationales

Juliette LE DROGOU, Policy Officer, Division Innovation et Finance Digitale, Direction de la régulation et des affaires internationales

Charles MOUSSY, Directeur, Division Innovation et Finance Digitale, Direction de la régulation et des affaires internationales

Marc WOLFENSTEIN, Juriste, Division Marchés financiers et services sur crypto-actifs, Direction des affaires juridiques

ACPR REPRESENTATIVES:

Barbara SOUVERAIN-DEZ, Directrice juridique

Beatrice PASSERA, Cheffe de la Cellule de Conseil en Droit européen, Direction des Affaires juridiques

Reda ROSTANE, Expert juridique affaires européennes, Direction des Affaires juridiques

REPRESENTATIVES OF THE FRENCH TREASURY:

Paul ABADIE, Adjoint au Chef de Pôle Affaires internationales et enjeux technologiques du secteur financier

Axelle BLANCHARD, Adjointe aux affaires européennes à la cheffe du pôle des affaires internationales, européennes et technologiques

Arthur FRAPPEREAU, Adjoint au Chef de Pôle Affaires internationales et enjeux technologiques du secteur financier

Florent JOILAN, Adjoint au chef de bureau lutte contre la criminalité financière

Romain LOISEAU, Adjoint à la cheffe de bureau entreprises et intermédiaires d'assurance

Victor MAUJEAN, Adjoint au chef du bureau FINENT3, chargé du droit des sociétés et gouvernance des entreprises

Victor MILLARD, Adjoint à la cheffe du bureau des entreprises et intermédiaires d'assurance

Alexis MINE, Adjoint aux affaires internationales à la cheffe du pôle des affaires internationales, européennes et technologiques

REPRESENTATIVES OF THE BANQUE DE FRANCE:

Christophe ARNAUD, Directeur des services juridiques

Céline GARIN-PIAT-DESVIAL, Responsable innovation et digitalisation, Direction des services juridiques

REPRESENTATIVE OF THE MINISTRY OF JUSTICE:

Julien GOLDSZLAGIER, Chef du Bureau du droit des sociétés et de l'audit, Direction des affaires civiles et du Sceau du Ministère de la Justice

Martin GUESDON, Chargé des fonctions de sous-directeur du droit économique, Direction des affaires civiles et du sceau

MEMBERS OF THE WORKING GROUP:

Ahmed BALADI, Partner, Gibson Dunn

François BARRIERE, Professeur de Droit, Université Lumière Lyon 2, French Counsel, Skadden Arps Slate Meagher & Flom LLP

Celestine BARTHOUT, Associate, Norton Rose Fulbright

Sébastien BONFILS, Directeur Juridique, Crédit Mutuel Arkéa

Michel CANNARSA, Professeur des Universités Catholiques, Doyen de la Faculté de Droit de l'Université catholique de Lyon

Thomas CAVIGLIOLI, Directeur Juridique Corporate, BPI France

Agnès CHATELLIER, Responsable juridique – Regulatory Digital, BNP Paribas

Asmaa CHEIKH, Responsable de la coordination du pôle de Règlementation bancaire et financière, Direction des affaires juridiques, Groupe Société Générale

Thiebald CREMERS, Directeur Juridique, AMAFI

Katia CZARNOTTA, Juriste, Natixis

Thomas DAUTIEU, Directeur de l'accompagnement juridique, CNIL

Marie-Mathilde DELDICQUE, Juriste référent coordinateur IP & Communication, Ambassadeur IA, BPCE

Louis DE MENEVAL, Legal Head of Digital, Commercial contracts & Litigation, AXA IM

Pierre-Yves DEVRIERE, Head of Digital Transformation / Managing Director, Ardian

Muriel FAURE, Chairman of the AFG Technology Innovation Commission

Philippe GOUTAY, Partner, Jones Day

Clara HAINSDORF, Partner, White and Case LLP

Emmanuel JOUFFIN, Responsable Référentiel SSI et Veille Réglementaire, La Banque Postale

Lara KIRDAR, Legal Counsel in Digital & AI, Qonto

Nathalie LANERET, VP Government Affairs and Public Policy, Criteo

Yves Marie LECOCQ, Juriste Digital & Data, BNP Paribas

Loïc LEGOUET, Directeur juridique, Amundi

Caroline LOUVEAUX, Chief Privacy and Data Responsibility Officer, Mastercard

Matthieu LUCCHESI, Counsel, Gide Loyrette Nouel AARPI

Catherine MARTIN, Responsable Juridique Digital, AXA France

Matthieu MAZARE, Juriste, CNIL

Julien NIVOT, Chargé de mission au sein du département Marché et Innovation Numérique, ESMA

Luke O'LEARY, Head of Legal & Compliance, Capi Money

Jerôme PEDRIZZETTI, Juriste, Crédit Agricole S.A

Sébastien PRAICHEUX, Partner, Norton Rose Fulbright

Albane RICHARD, Juriste, BNP Paribas

Dibril SAKO, Direction Juridique, AXA Group

Marina TELLER, Professeure de Droit, Université Nice Côte d'Azur