In data we trust? Emerging policy and supervisory approaches to AI data use in financial services[1]

Executive summary

Artificial intelligence (AI) is transforming the financial sector while further amplifying the critical role of data within it. Advanced forms of AI, such as generative (gen) AI, depend on vast and diverse amounts of data across all stages of their life cycle. Data are essential for training gen AI models, assessing performance, identifying biases and refining outputs, and therefore shape their capabilities, limitations and evolution. As these systems become more embedded in core financial institutions' activities, such as deposit-taking, credit and insurance underwriting, and payments, sound data management becomes essential not only for ensuring reliable and trustworthy AI applications but also for preserving trust and confidence in the financial system.

Although data management challenges are not new, the financial sector consistently identifies them as significant barriers to the broader adoption of gen AI. A long-standing issue is the incompatibility of the sector's numerous data sources, which often contain rich but fragmented information. This has historically resulted in inconsistent data quality, hindering analytics and automation efforts. The scaling of gen AI amplifies these weaknesses while introducing new challenges, including those related to the growing use of synthetic and alternative data. Among the most pressing concerns are those relating to data privacy, quality and security, all of which are exacerbated by third-party dependencies. Taken together, these shortcomings can heighten consumer protection risks as well as micro- and macroprudential vulnerabilities. If left unaddressed, they have the potential to erode the anticipated benefits of gen AI in the financial sector.

Data protection has received considerable attention, even before the advent of AI, including at the international level. Although data protection is widely regulated across jurisdictions, its scope varies, and applying data protection principles to AI remains a challenge as their interplay continues to evolve. In response, some data protection authorities have started issuing cross-sectoral guidance on how data requirements apply to AI practices. This guidance, combined with cross-sectoral data protection frameworks, forms the foundation for addressing AI-related data risks in the financial sector.

Data protection frameworks place particular emphasis on data privacy, understood as individuals' ability to control their personal data. However, advanced AI systems, which rely on extensive volumes of personal data, can undermine individuals' ability to determine how their data are collected, processed and shared. Upholding core data privacy principles – such as lawful basis, meaningful consent, purpose limitation, data minimisation and retention limitation – becomes particularly challenging in the context of AI. Other principles, including fairness and transparency, also present complexities in AI.

Data quality is equally central. Data protection frameworks emphasise data accuracy, completeness and representativeness to prevent the spread of false information and reduce the likelihood of decisions based on inaccurate data. Similarly, AI frameworks attach critical importance to this area as poor data quality can lead to biased or harmful outputs. While both frameworks align in their emphasis

[1] Juan Carlos Crisanto (Juan-Carlos.Crisanto@bis.org), Johannes Ehrentraud (Johannes.Ehrentraud@bis.org), Adrien Currat (Adrien.Currat@bis.org), Bank for International Settlements; and Wenguang Wu (wwenguang@pbc.gov.cn), People's Bank of China. The authors are grateful to Elisabeth Noble, Jermy Prenio, Jeffery Yong, Jon Frost, Alain Otaegui, Timothy Shakesby, Musa Parmakisz, Joe Perry, Shunsuke Tani, Giuseppe Bianco and Lucia Russo. Charlotte Gardini provided valuable administrative support.

on data quality, they differ in approach: statistical accuracy in AI is based on likelihoods and predictions, whereas accuracy in data protection requires personal data to be correct and complete.

Data security – encompassing confidentiality, integrity and availability – is another core aspect of data protection frameworks. Organisations are required to implement robust security measures to safeguard data within information and communication technology (ICT) systems, which is especially important in AI settings given the scale and potential sensitivity of the data processed. Data breaches in such contexts can result in financial losses, reputational damage and legal repercussions. Furthermore, strong data security measures are essential for maintaining operational resilience.

Sound data governance forms the backbone of managing the complexities of data in AI, providing a strong foundation to support data quality, privacy and security. It establishes clear roles, responsibilities, processes and policies necessary to manage data effectively while ensuring compliance with regulatory requirements. A key aspect of data governance is accountability, a fundamental principle that requires organisations to take responsibility for how data are sourced, processed and used.

While relying on cross-sectoral data protection frameworks, financial authorities address AI data risks through a combination of approaches, often using established and largely non-prescriptive guidance. In addition to AI-related legislation and industry standards, international standards such as the Basel Committee on Banking Supervision's (BCBS) Principles for effective risk data aggregation and risk reporting (BCBS 239) serve as a key reference for robust data management. Building on these, authorities commonly rely on established supervisory and regulatory guidance for general data management, model risk management (MRM) and operational resilience, which includes cyber security, outsourcing and third-party risk management. They also frequently employ non-prescriptive approaches, such as thematic reviews and information papers, to highlight emerging good practices for managing data in AI. While specific supervisory expectations for AI data usage are not yet fully consistent, early signs of convergence are emerging in key areas, including data privacy, quality, security and governance.

Nonetheless, important challenges remain within the current policy framework for addressing AI data risks. Tensions persist between technological capabilities and existing data protection requirements, in particular in their practical application across different stages of the AI life cycle. Although data protection authorities are providing guidance, some requirements place demands that current AI technologies are not yet fully equipped to meet. Existing regulatory and supervisory frameworks designed for traditional data-related uses or earlier forms of AI might not fully capture the complexity of gen AI ecosystems. Third-party dependencies further complicate oversight due to limited data visibility across the AI supply chain, often compounded by market concentration among key providers.

To address AI data-related challenges, financial authorities could issue tailored guidance on data governance, quality, security and third-party dependencies. This may involve clarifying supervisory expectations for robust data governance frameworks and the application of data protection principles throughout the AI life cycle. Guidance on data quality could focus on strong data management processes, continuous quality assurance and clear standards for key data quality dimensions such as accuracy and completeness. Data security measures might emphasise the importance of effective incident response plans and integration of cyber security with data protection controls in AI environments. Supervisors could also strengthen expectations regarding third-party dependencies in AI ecosystems, including enhanced transparency on data lineage and monitoring of third-party providers. Additionally, authorities could foster industry understanding through thematic reviews and best practices. Over time, developing a comprehensive policy framework tailored to AI data issues would be particularly beneficial.

Enhanced collaboration between financial authorities and data protection authorities is vital given the cross-cutting and rapidly evolving nature of AI data challenges. Structured cooperation can promote regulatory consistency, reduce uncertainty and help mitigate the risk of cross-border fragmentation. Continued dialogue with industry stakeholders will also be key. The overall objective is to ensure that AI adoption in financial services supports innovation while reinforcing trust, resilience and financial stability.