UNIWERSYTET ZIELONOGÓRSKI

DYSKURS PRAWNICZY I ADMINISTRACYJNY 2/2026 ISSN 2657-926X

Johan Schweigl
Faculty of Law, Masaryk University, Czech Republic
ORCID: 0009-0001-7866-5542
Johan.Schweigl@law.muni.cz

From Internal Standards to the AI Act: Reshaping Financial Processes for the Era of Algorithmic Accountability

Keywords: EU AI Act, Algorithmic Hygiene, Duty of Care, Financial Regulation, Agentic AI

Summary. This paper looks at how internal governance in financial institutions changes as the sector moves from voluntary standards to the mandatory EU AI Act. It traces the path from the traditional "duty of care" to what could be called "algorithmic accountability". The argument is that as Agentic AI takes over cognitive workflows such as AML monitoring and risk management, the traditional focus on human behaviour becomes less relevant. The paper proposes the concept of "Algorithmic Hygiene" as a way of describing the continuous oversight of how software is configured and how it performs. The conclusion is that institutional stability now depends ongoing beyond formal "tick-the-box" compliance toward a real technical audit of an institution's "algorithmic DNA".

Od standardów wewnętrznych do aktu o AI: przekształcanie procesów finansowych na potrzeby ery algorytmicznej odpowiedzialności

Słowa kluczowe: unijny AI Act, higiena algorytmiczna, należyta staranność, regulacja finansowa, Agentic AI.

Streszczenie. Niniejszy artykuł analizuje transformację wewnętrznego ładu instytucji finansowych w okresie przejścia od dobrowolnych standardów do obowiązkowego unijnego AI Act. Przedstawia ewolucję tradycyjnej zasady „należytej staranności" w sformalizowane ramy „odpowiedzialności algorytmicznej". W oparciu o metodę analityczną wzbogaconą o praktyczne obserwacje z sektora bankowego, autor wskazuje na zasadniczą zmianę w obszarze kontroli wewnętrznej: w miarę jak Agentic AI automatyzuje procesy poznawcze, takie jak monitorowanie AML czy zarządzanie ryzykiem, tradycyjny nadzór nad zachowaniem człowieka staje się drugorzędny. Autor wprowadza pojęcie „higieny algorytmicznej" jako proaktywnego procesu skupionego na technicznej integralności i konfiguracji oprogramowania. W konkluzji artykuł stwierdza, że stabilność instytucjonalna zależy obecnie od wyjścia poza formalne podejście „tick-the-box" w kierunku rzeczywistego technicznego audytu „algorytmicznego DNA" instytucji.

1. Introduction: The Role of AI in the Financial Services Ecosystem

Discussions about the integration of Artificial Intelligence (AI) into the financial sector usually focus on technological innovation or on its broad macroeconomic impact. The most important changes, however, take place inside financial institutions themselves, where new technology meets established legal principles and strict regulatory expectations. This paper looks beyond the general development of AI as a tool for efficiency, and focuses on how this shift reshapes internal processes, control mechanisms, and questions of organisational responsibility.

2. Background and Context

In theoretical terms, this paper combines two areas of law: financial law and an emerging field that is now often referred to as AI law. Although the focus is on banking and payment regulation, the underlying logic – how legal systems set rules for autonomous technologies – has a much wider reach. As AI is entering all areas of human activity, AI law will likely develop into an independent legal field, with cross-cutting principles applicable to many sectors. Financial regulation is simply among the first areas where these principles must be tested in practice.

AI has been reshaping the global economy over the last several years, and is sometimes compared to a new "industrial revolution". Recent studies show that AI may transform labour markets and economic production across all sectors. In advanced economies, around 60% of jobs are already exposed to AI in some way, which gives a sense of the scale of the shift[1]. Some studies suggest that, unlike previous waves of technology, the current adoption of Generative AI will hit highly skilled professions where cognitive tasks dominate. By 2030, it may be possible to automate more than 50% of the cognitive skills needed across many jobs. Even managers and experts in finance now face a much higher level of automation than was expected before the arrival of Generative AI[2].

Findings of a study by the McKinsey Global Institute[3] show a major shift in how automation works. Earlier waves of technology mostly replaced physical and

[1] M. Cazzaniga, F. Jaumotte, L. Li, G. Melina, J. A. Panton, C. Pizzinelli, E. Rockall, M. M. Tavares, *Gen-AI: Artificial Intelligence and the Future of Work*, IMF Staff Discussion Note SDN/2024/001, International Monetary Fund, January 2024, p. 2, available at: https://www.imf.org/-/media/files/publications/sdn/2024/english/sdnea2024001.pdf [accessed on: 01.05.2026].

[2] Technologické centrum Praha, *Policy Brief: Dopady generativní umělé inteligence na společnost v ČR*, Policy Brief M2, 2024, available at: https://stratin.tc.cas.cz/vystupy/2024/M2/Policy%20Brief_DopadyGenAI_2024_final.pdf [accessed on: 01.05.2026].

[3] McKinsey Global Institute, *The economic potential of generative AI: The next productivity frontier*, McKinsey & Company, June 2023, available at: https://www.mckinsey.com/capabilities/mck-

repetitive tasks. Generative AI now affects high-wage "knowledge workers" whose roles were previously seen as safe from automation. The financial sector relies heavily on professional expertise and is therefore among the first to face these changes. According to Bloomberg's analysis of the McKinsey data, banks alone could see a productivity boost of around $200 to $340 billion per year, which could mean a 9% to 15% jump in operating profits[4].

The EU AI Act[5] is a major piece of legislation that aims to address the main challenges posed by AI in different areas of human activity. For highly regulated entities, however, the AI Act is not a completely new start. Businesses, and not only financial institutions, are already required to operate under a strict "duty of care" (fiduciary duty). This principle, which is part of the legal orders of the EU Member States, requires financial institutions to manage risks and protect client assets even without specific AI legislation.

The financial sector is relatively unique compared to other industries for several reasons:

– Management of Third-Party Assets: financial firms manage money that belongs to their clients, which creates a higher level of responsibility;
– Systemic Importance: the failure of a major bank can have consequences for the stability of the entire financial system;
– Public Trust: financial services depend on the trust of the public.

Regulated financial institutions had, to some extent, already adapted their internal rules for the use of AI before the AI Act came into force. The new legal requirements therefore mostly formalise and unify what already existed in internal standards, rather than introducing entirely new rules.

3. Problem Statement and Research Goal

The AI Act takes the rules that previously sat under the general principle of "good faith" and turns them into a mandatory "legal minimum". The risk is that compliance becomes a "tick-the-box" exercise, where the principles set by law are reflected in internal processes only on paper, without proper controls and audits. For example,

insey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier [accessed on: 01.05.2026].

[4] B. Baschuk, *Biggest Losers of AI Boom Are Knowledge Workers, McKinsey Says*, Bloomberg News, 14 June 2023, available at: https://www.bloomberg.com/news/articles/2023-06-14/biggest-losers-of-ai-boom-are-knowledge-workers-mckinsey-says [accessed on: 01.05.2026].

[5] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 12 July 2024.

when an employee approves a decision made by an AI system, that person should actually understand how the result was reached, not just sign off.

Another challenge is that financial institutions need to balance the major laws applying to them. They have to follow the AI Act and at the same time respect the GDPR[6] (for privacy) and DORA[7] (for digital security). Balancing these three areas is not easy for any compliance department.

The goal of this paper is to look at how internal controls in financial institutions are changing in the era of AI. The paper first describes how firms managed technology risks in the past under the duty of care. It then sets out the basic principles of the EU AI Act and explains how they create a new mandatory standard for the industry. Finally, it discusses where internal governance is heading, with a focus on what the paper calls "Algorithmic Hygiene" – a state where compliance and audits look directly at the technical health of the algorithms.

4. Methodology and Paper Structure

The paper combines several methods. The analytical method is used to review the requirements of the EU AI Act, DORA and the GDPR, and to identify how these regulations overlap and what specific obligations they impose on financial institutions. The comparative method is used to compare the "pre-regulatory" era based on the duty of care with the new mandatory standards of the AI Act. The case-based approach also plays a part, since the paper draws on the author's experience and observations from the banking and payment industry.

Section 5 covers the "pre-regulatory" era and the duty of care. Section 6 analyses the core principles of the EU AI Act. Section 7 looks at where internal governance is heading, with a focus on "Algorithmic Hygiene" and the new role of internal controls. Section 8 summarises the findings and reflects on supervisory implications.

This paper aims to address three research questions:

RQ1: How does the AI Act change the way financial institutions manage internal risks, compared to the previous era,based on the duty of care?

RQ2: What new internal control mechanisms become necessary when AI agents take over tasks previously performed by humans?

---

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016, p. 1.

[7] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, OJ L 333, 27 December 2022, p. 1.

RQ3: Can the traditional Three Lines of Defence model still work in the era of agentic AI, or does it need to be rebuilt?

The research has several limitations. First, the AI Act has only recently been adopted and there is almost no case law that would clarify how the rules will be applied in practice. Second, sectoral guidance such as the BaFin document is national-level soft law, and similar guidance from other Member States may differ. Third, the concept of "Algorithmic Hygiene" introduced here is a normative proposal of the author and has not yet been empirically tested across institutions. The paper is therefore meant to open a discussion rather than to present a finished framework.

5. Governance Before the AI Act: Internal Risk Management Practices

The financial services sector has long been among the leaders in digital transformation.[8] However, the adoption of new technology has not been uniform across the industry. Large banks have moved more slowly because their systems are usually more complex, with more legacy and a more rigid corporate culture. This opened space for fintech companies and neobanks. Many of these new players were originally built as technology firms and used automation as the core of their business model, not just as a side tool.

The shift toward automation was driven by the need for operational efficiency and competitive pressure. Because no specific AI legislation existed at the time, the sector relied on internal standards and guidelines. Internal governance was not about following an AI law but about keeping the business stable and managing risk. Financial institutions understood that internal processes which were left unregulated could cause serious financial and reputational damage, and so they started to integrate technology risks into their existing risk management frameworks.

5.1. Duty of Care and Risk Management

The fundamental legal principle of the "Duty of Care" and its corporate equivalent, "Prudent Management" (known in the Czech legal system as *péče řádného hospodáře*), is rather universal across the legal orders of the EU Member States. Despite some variations in terminology, it is one of the basic pillars on which corporate law stands. Corporate law theory and case law have developed this principle in detail, and the AI Act now translates parts of that established theory into concrete

[8] M. Fernández, N. Charnay, *AI and banking: Leaders will soon pull away from the pack*, S&P Global Ratings, 28 October 2024, available at: https://www.spglobal.com/ratings/en/research/articles/241028-ai-and-banking-leaders-will-soon-pull-away-from-the-pack-13354388 [accessed on: 01.05. 2026].

obligations for the use of AI systems. In the financial sector, the statutory bodies of financial firms have a fiduciary obligation to act in the best interests of their clients and to keep the institution stable[9]. Failing to do so properly, they would face consequences.

In the financial sector, a duty of care is understood as an obligation for providers to avoid conflicts of interest, act with loyalty, and protect the customer's interests[10] .As S&P Global notes, the banking sector has been a "pioneer" of machine learning and deep learning for over a decade[11]. Even during this "pre-regulatory" period, the move from rule-based systems to more autonomous models was guided by the general principle that firms must act honestly and professionally. Any new technology had to be assessed in terms of risk management to make sure it would not cause unreasonable harm or loss to the customer. The internal governance of technology, including AI, was therefore already part of professional conduct standards, long before the current unified regulation. The internal approaches taken by individual institutions, however, varied widely in quality and depth.

5.2. Early Limitations

When trying to gain efficiency through automation, the early adoption of AI in the financial sector faced several barriers. These were not only technical but also legal and ethical, and they made institutions cautious. The first major issue was data privacy and the risk of "data leakage". Under the GDPR, businesses including financial firms have a strict duty to protect their clients' personal data. In the early stages of the AI boom, many institutions were rightly worried that putting sensitive information into external AI models could mean a loss of control over banking secrecy. For a payment institution or a bank, any unauthorised exposure of client data is a red line, with consequences ranging from heavy fines to a loss of public trust.

Another important issue was the so-called "Black Box" effect. Many advanced AI models, in particular those used in banking, are designed to solve complex tasks. As a result, it is hard to understand exactly how they reach a specific result[12].In

[9] O.O. Cherednychenko, C. Busch (eds.), *A Bank's Duty of Care: Perspectives from European and Comparative Law*, European Review of Private Law, 2017, p. 397, available at: https://pure.eur.nl/en/publications/a-banks-duty-of-care-perspectives-from-european-and-comparative-l-2/[accessed on: 01.05.2026].

[10] Financial Services Consumer Panel, *Incorporating a Duty of Care into the Financial Services & Markets Act*, FSCP Position Paper, June 2015, available at: https://www.fca.org.uk/panels-assets/consumer-panel/publication/fscp_position_paper_on_duty_of_care_2015.pdf[accessed on: 01.05. 2026].

[11] M. Fernández, N. Charnay, *op. cit*.

[12] W. Knight, *The Dark Secret at the Heart of AI*, MIT Technology Review, 11 April 2017, available at: https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/ [accessed on: 01.05.2026].

a heavily regulated environment, this lack of transparency is a serious problem. For example, when a model rejects a loan application, the compliance department, internal audit and the regulator all need to know the specific reasons. Without explainability, such models had to be limited to back-office tasks and were rarely used for critical, client-facing decisions.

There were also technical and operational risks, sometimes described as human-machine misalignment. There was a real concern that AI agents could optimise their goals in ways that ignore human values[13]. In addition, older banks often struggled with legacy systems and poor data quality, which made it difficult to integrate modern AI tools. Shneiderman argues that, given these risks, the focus needs to shift from autonomous agents to Human-Centred AI. According to him, the answer lies in designing systems that allow a high level of automation while keeping a high level of human control. For the financial sector, this means treating AI not as a replacement for human judgement but as a tool that supports human expertise and is reliable and safe to use[14].

6. The AI Act as a Legal Minimum and Process Transformation

The entry into force of the AI Act marks a shift for the financial services sector, although it is not a paradigm shift. The earlier era based on the duty of care and on voluntary best practices has now been replaced by mandatory regulatory principles. For highly regulated entities such as banks and payment institutions, the AI Act does not replace existing responsibilities. It formalises them into a strict and unified legal minimum.

Banks now have to make sure that their automated processes follow the core AI Act principles and that they are transparent and traceable. Institutions are moving from a "best effort" regime to enforceable compliance, where every algorithmic decision is subject to oversight. The change covers the full lifecycle of AI systems – from the initial design and the choice of training data, through automated pre-decisions, to ongoing supervision. This creates room for a new standard of integrity, where technical reliability matters as much as financial stability.

6.1. Standardisation of Rules: Core Principles of the AI Act

The aim of the AI legislation framework, as set out in its introductory recitals, is to create a unified EU market for safe and trustworthy AI. The framework should

[13] M. Fernández, N. Charnay, *op. cit*.

[14] B. Shneiderman, *Human-Centered Artificial Intelligence: Reliable, Safe & Trustworthy*, arXiv:2002.04087 [cs.HC], 2020, available at: https://doi.org/10.48550/arXiv.2002.04087 [accessed on: 01.05.2026].

support innovation while keeping a high level of protection for fundamental rights, safety, and democratic values. It complements existing Union laws such as the GDPR and consumer protection law by adding specific obligations on transparency, technical documentation, and a human-centred approach. For financial institutions, the AI Act turns internal best practices into a standardised, mandatory legal floor. The following principles describe what firms must now incorporate into their internal control systems.

Risk Management System (Article 9). The Act requires a continuous process of risk management throughout the lifecycle of a high-risk AI system. AI-specific risks therefore need to be considered as part of the standard risk assessment. Risk management is essential for the stability of an institution, and AI risks have to be properly assessed and, where necessary, mitigated. This systemic approach is further developed in sectoral guidance, such as the recent BaFin Guidance on ICT Risks in the Use of AI (2026) in Germany. BaFin states that AI systems must be fully integrated into the existing ICT risk management framework under DORA.[15]

Data Governance and Quality (Article 10). To prevent algorithmic bias, in particular in credit scoring, the Act requires the use of high-quality training, validation and testing data. Article 10 says that these data sets must be relevant, representative, and as free of errors as possible.

Transparency and Provision of Information (Article 13). This principle is the legal answer to the "Black Box" problem described above. High-risk AI systems must be designed in a way that allows users to understand the system's output, or at least the process by which the result was reached. Firms must provide detailed technical documentation and "instructions for use" so that the algorithm is not a mystery to those who operate it[16]. The BaFin guideline mentioned above also addresses this point. It stresses that the management body has a strategic responsibility and must have enough AI literacy to understand how algorithmic decisions affect the firm's risk profile and capital stability[17].

Human Oversight (Article 14). One of the most important principles for the financial sector is the requirement of meaningful human oversight. The aim is to prevent automation bias, where human operators stop questioning the machine. According to Constantino, meaningful human oversight requires that the persons

[15] BaFin (*Bundesanstalt für Finanzdienstleistungsaufsicht), Guidance on ICT Risks in the Use of AI at Financial Entities*, version of 23 January 2026, pp. 9–11, available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Meldung/2025/neu/meldung_2025_12_18_orientierungshilfe_ikt_risiken_en.html [accessed on: 01.05. 2026].

[16] W. Knight, *op. cit*.

[17] BaFin, *op. cit*.

in charge have the necessary competence and authority to intervene, override or even shut the system down when it deviates from its intended path[18].

Accuracy, Robustness, and Cybersecurity (Article 15). High-risk systems must be resilient against errors and against attempts to alter their performance, such as "data poisoning". In the financial context, this principle overlaps with DORA, since AI is increasingly treated as a key part of a firm's ICT systems.

6.2. Data Governance and the Shield of Banking Secrecy

The practical use of AI in financial institutions faces a basic dilemma: AI models need a lot of data to work well, but banks are bound by the strictest standards of banking secrecy and data protection (the GDPR). In the past, this often led to a zero-trust approach, where real client data was almost never used in AI systems and only general or anonymised data was used instead. With the AI Act, in particular Article 10, the focus moves toward a more practical approach. Any system that processes or has access to client data must go through a serious technical and legal due diligence. If the system passes, new options for the use of AI become available. The process should normally include:

– Data Minimisation and Localisation: ensuring that only necessary data is processed and, where possible, kept within the institution's secure infrastructure to prevent data leakage to public models or third-party cloud providers;
– Purpose Limitation: under the GDPR and banking laws, client data can only be used for specific, authorised purposes (*e.g.,* fraud prevention or credit scoring). Using this data to train a general-purpose AI without explicit consent or legal basis would constitute a major breach of requirements on data privacy;
– Vetting of AI Vendors: if an institution uses an external AI provider (*e.g.,* via API), the onboarding must confirm that the vendor does not use the institution's input data to train its own models, as it would constitute a direct violation of banking secrecy.

As pointed out in the BaFin guideline[19], data security in AI is not just about encryption – it is about the integrity of the entire data pipeline.

6.3. Regulatory Interactions

Another aspect connected with the AI Act is the interaction between the AI Act, the GDPR and DORA. The GDPR has been in force for almost a decade, and

[18] J. Constantino, *Exploring Article 14 of the EU AI proposal: accountability challenges of the human in the loop when supervising high-risk AI systems in public administration*, SSRN, 2022, pp. 31, 43, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4254940 [accessed on: 01.05.2026].

[19] BaFin, *op. cit.*

DORA for the last couple of years. These two regulations are two important pillars of financial regulation, although their reach goes well beyond the financial sector. The AI Act will now complete the trio. Although these are often seen as three separate regulatory areas, the current trend, driven by the European Commission's "Digital Omnibus" package[20], is moving toward radical simplification. The goal is to reduce the administrative burden on firms by up to 25% by 2029 by removing overlapping requirements.

These three areas are inextricably intertwined and the process of bringing them together will raise some difficult questions. The trend toward simplification, however, is clear.

7. The Future Perspective: Algorithmic Hygiene and Internal Controls

The rapid progress of AI automation is not just an upgrade of existing tools – it changes the way institutions operate at a fundamental level. As AI systems become more advanced, they are increasingly moving from supporting roles to taking over entire workflows previously handled by human staff. The clearest examples can be found in high-volume areas such as customer service, complaint handling, routine risk management tasks, the updating of contractual terms, back-office administration and parts of client onboarding and AML (Anti-Money Laundering) monitoring.

The wide integration of AI across the banking business leads to a complete change of internal processes. In this new setting, the traditional focus of internal control, namely the supervision of human behaviour and manual data entry, becomes less central in some areas. The key factor for the safety and stability of the institution is now how the AI is configured and how it functions internally. When a human is removed from a process, the "control" must be built directly into the way the algorithm is set up. A new approach to institutional health is therefore needed, which the paper calls Algorithmic Hygiene – a continuous effort to keep the institution's automated processes clean, transparent and compliant.

7.1. The Need for Algorithmic Hygiene

With the arrival of Agentic AI, the focus of internal controls has to shift from supervising human behaviour to direct oversight of the integrity and functioning

[20] European Commission, *Commission proposes Digital Omnibus to simplify EU digital rules*, IP/25/2718, Brussels, November 2025, available at: https://ec.europa.eu/commission/presscorner/ [accessed on: 01.05. 2026].

of the software. We are moving beyond simple automation of isolated tasks toward the deployment of autonomous assistants that can make decisions with a direct impact on clients and on the stability of the institution, although still within the limits set by the human-in-the-loop principle. Algorithmic Hygiene therefore becomes a central element of regulatory compliance.

Algorithmic hygiene is not a one-off audit but a continuous process of keeping "software health". In practice, it will probably focus on:

- System Integration and ICT Interaction: monitoring how the AI agent is embedded within the institution's IT systems and ensuring its interactions with other ICT systems do not create vulnerabilities;
- Output Measurement and Error Statistics: implementing rigorous, real-time evaluation of the agent's performance. Statistical deviation from expected results would serve as the primary red flag for internal control intervention;
- Quality Control of "Pre-fixed" Solutions: given the high costs of custom AI development, financial institutions will largely rely on purchasing pre-fixed, certified solutions tailored to specific use cases. Algorithmic hygiene here acts as a continuous quality assurance mechanism for these external modules.

A new element of internal controls will be the testing of agents through non-standard tasks. Instead of just monitoring routine operations, control departments will likely confront agentic assistants with specific, unusual or edge-case scenarios. The way the agent handles such challenges, and whether it stays within legal and ethical limits, will probably become part of modern controls and audits.

7.2. Redefining the Three Lines of Defence for the Agentic Era

The arrival of Agentic AI does not call for a radical restructuring of internal organisational frameworks, but rather for a targeted update of the Three Lines of Defence (3LoD) model. The focus of control shifts to the software itself: how it is configured, how it is integrated into the institution, and how it performs in real conditions. The evaluation has two key phases: tool onboarding (the pre-production phase) and ongoing control (the production phase), and both phases run across all three lines.

The First Line (Business & IT Operations). Responsibility starts at the selection and onboarding of the AI solution. Since institutions will increasingly rely on pre-fixed external solutions, the first line must check that the configuration of the tool fits the specific needs of the given process, such as AML monitoring or client onboarding. During the operational phase, the focus moves to continuous hygiene: monitoring how the software functions and analysing error statistics. The first line is responsible for making sure that the algorithm's outputs meet the agreed KPIs and do not show dangerous deviations.

The Second Line (Risk & Compliance). The second line carries out an independent assessment at the onboarding stage and verifies that the setup follows both the relevant legislation (the AI Act, the GDPR) and the internal risk appetite. During periodic controls, it uses methods such as the assignment of non-standard tasks. By looking at how the AI agent deals with unusual situations, the second line checks the underlying logic of the software. This line will also benefit from the simplifications brought by the Digital Omnibus, which should allow more efficient reporting and cross-regulatory monitoring.

The Third Line (Internal Audit). Internal audit completes the system by periodically reviewing how well the whole algorithmic hygiene framework works. The audit focus will likely shift from tracking individual human actions to auditing the software as a whole. Internal audit will check whether the onboarding and ongoing control processes in the first and second lines are working properly and whether the reported error statistics are credible. Auditing the integrity of the algorithm and its integration into the institution will likely become the way of confirming that the institution is acting with a duty of care.

8. Conclusion: New Trends in Financial Governance and Supervision

The move toward broad AI automation marks an important turning point in the internal governance of financial institutions. As this paper has shown, the implementation of the AI Act and DORA is not just additional bureaucracy. It is a logical continuation of the traditional "duty of care". In a setting where the human factor is gradually moving out of critical processes, accountability does not disappear. It changes shape and becomes "algorithmic accountability".

Recent legislative developments show a clear trend toward simpler and more harmonised rules. This gives institutions more space for effective risk management and is an important condition for the practical use of "algorithmic hygiene". Instead of being buried in formal administrative tasks, institutions can focus on the actual health and configuration of the software and on how it is set up within their internal processes.

Algorithmic accountability is gradually becoming the standard against which professional financial management will be measured. Institutions that combine technological progress with the integrity of the algorithms they use will be the ones best placed for the future.

8. Policy Implications

For supervisory practice, one risk in particular deserves attention. The human-in-the-loop principle, which is central to Article 14 of the AI Act, can easily turn into a "tick-the-box" exercise. A human formally approves a decision produced by an AI

system without understanding how the system reached it. Supervisory authorities should therefore look not only at whether human oversight exists on paper, but also at whether the persons in charge have the competence and time to challenge the algorithm's output. Without this, human oversight is only a formality.

8.2. Open Questions and Future Research

Several questions remain open and would deserve further work. First, the concept of Algorithmic Hygiene needs to be tested in practice across institutions of different size and type. Second, the relationship between the AI Act and sectoral regulation, such as the CRR and CRD for banks, is not yet fully clear and may lead to overlaps that future case law or supervisory practice will have to deal with. Third, the role of supervisory authorities (the EBA, national regulators) in the technical audit of algorithms is still an open question – it is not yet settled whether supervisors will themselves carry out algorithmic audits or rely on internal and external auditors. These questions go beyond the scope of this paper and should be addressed in follow-up research.

References

Baschuk B., *Biggest Losers of AI Boom Are Knowledge Workers, McKinsey Says*, Bloomberg News, 14 June 2023, https://www.bloomberg.com/news/articles/2023-06-14/biggest-losers-of-ai-boom-are-knowledge-workers-mckinsey-says [accessed on: 01.05.2026].

BaFin (*Bundesanstalt für Finanzdienstleistungsaufsicht*), *Guidance on ICT Risks in the Use of AI at Financial Entities*, version of 23 January 2026, https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Meldung/2025/neu/meldung_2025_12_18_orientierungshilfe_ikt_risiken_en.html [accessed on: 01.05.2026].

Cazzaniga M., Jaumotte F., Li L., Melina G., Panton J. A., Pizzinelli C., Rockall E., Tavares M.M., *Gen-AI: Artificial Intelligence and the Future of Work*, IMF Staff Discussion Note SDN/2024/001, International Monetary Fund, January 2024, https://www.imf.org/-/media/files/publications/sdn/2024/english/sdnea2024001.pdf [accessed on: 01.05.2026].

Cherednychenko O.O., Busch C. (eds.), *A Bank's Duty of Care: Perspectives from European and Comparative Law*, European Review of Private Law, 2017, https://pure.eur.nl/en/publications/a-banks-duty-of-care-perspectives-from-european-and-comparative-l-2/ [accessed on: 01.05.2026].

Constantino J., *Exploring Article 14 of the EU AI proposal: accountability challenges of the human in the loop when supervising high-risk AI systems in public administration*, SSRN, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4254940 [accessed on: 01.05.2026].

European Commission, *Commission proposes Digital Omnibus to simplify EU digital rules*, IP/25/2718, Brussels, November 2025.

Fernández M., Charnay N., *AI and banking: Leaders will soon pull away from the pack*, S&P Global Ratings, 28 October 2024, https://www.spglobal.com/ratings/en/research/articles/241028-ai-and-banking-leaders-will-soon-pull-away-from-the-pack-13354388 [accessed on: 01.05.2026].

Financial Services Consumer Panel, *Incorporating a Duty of Care into the Financial Services & Markets Act*, FSCP Position Paper, June 2015, https://www.fca.org.uk/panels-assets/consumer-panel/publication/fscp_position_paper_on_duty_of_care_2015.pdf [accessed on: 01.05.2026].

Knight W., *The Dark Secret at the Heart of AI*, MIT Technology Review, 11 April 2017, https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/ [accessed on: 01.05.2026].
McKinsey Global Institute, *The economic potential of generative AI: The next productivity frontier*, McKinsey & Company, June 2023, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier [accessed on: 01.05.2026].
Shneiderman B., *Human-Centered Artificial Intelligence: Reliable, Safe & Trustworthy*, arXiv:2002.04087 [cs.HC], 2020, https://doi.org/10.48550/arXiv.2002.04087.
Technologické centrum Praha, *Policy Brief: Dopady generativní umělé inteligence na společnost v ČR*, Policy Brief M2, 2024, https://stratin.tc.cas.cz/vystupy/2024/M2/Policy%20Brief_DopadyGenAI_2024_final.pdf [accessed on: 01.05.2026].

Legal sources

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119, 4 May 2016.
Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA), OJ L 333, 27 December 2022.
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act), OJ L, 12 July 2024.

AI Use Disclosure

The author used an artificial intelligence language model to assist with linguistic editing, translation refinement, and the structural organisation of this paper. While the AI was employed to enhance the clarity and stylistic quality of the text, all conceptual ideas, legal analyses, original terminology (including the concept of "Algorithmic Hygiene"), and final conclusions remain the sole responsibility of the author.