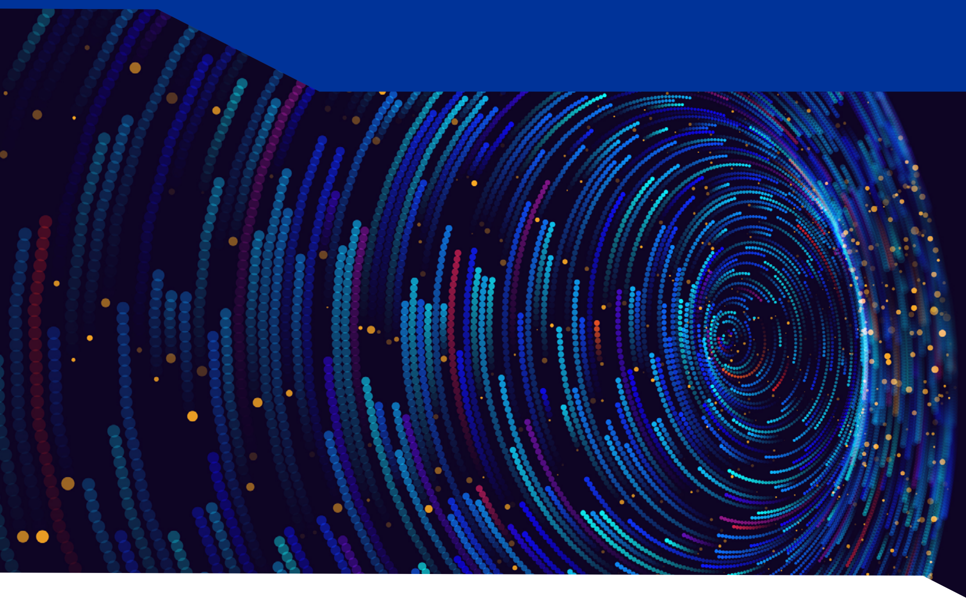
EU Supervisory
Digital Finance
Academy

Digital Finance in the EU: Navigating new technological trends and the AI revolution

Editors

Lorenzo Moretti, Laura Rinaldi, Pierre Schlosser



Funded by
the European Union

European Commission

EUI EUROPEAN UNIVERSITY INSTITUTE

eba European Banking Authority

eiopa EUROPEAN INSURANCE

ESMA European Securities and Markets Authority

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

This e-book has received funding from the EU TSI Programme in the framework of the EU Supervisory Digital Finance Academy (EU-SDFA) project, grant agreement number 101092497.

Published by
European University Institute (EUI)
Via dei Roccettini 9, I-50014
San Domenico di Fiesole (FI)
Italy

ISBN:978-92-9466-637-6
doi:10.2870/8600400
QN:QM-01-24-186-EN-N

Funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.
This e-book has received funding from the EU TSI Programme in the framework of EU-SDFA project, grant agreement number 101092497

Digital Finance in the EU: Navigating New Technological Trends and the AI Revolution

The EU Supervisory Digital Finance Academy's Second Year e-Book

EDITED BY

Lorenzo Moretti, Florence School of Banking and Finance, European University Institute

Laura Rinaldi, European Commission DG REFORM

Pierre Schlosser, Florence School of Banking and Finance, European University Institute

European University Institute, Florence, Italy

Table of Contents

1. Foreword

Nathalie Berger

Director for Structural Reform Support, European Commission DG REFORM

In recent years the financial sector has witnessed a surge in the implementation of AI-based solutions and tools. This rapid escalation in conjunction with the emergence of generative capabilities mirrors the broader economic landscape, in which AI innovation is gaining significant traction at an unprecedented scale. This has led to substantial investments and heightened user expectations. While the implementation of AI-based solutions in the financial sector has primarily focused on support functions, there is growing recognition of its potential to expand into new domains in the near future. This expansion is accompanied by significant benefits but also the emergence of new risks, which make it necessary for regulatory and supervisory authorities to enhance their capacity to address these challenges.

This e-book takes stock of the second year of one of the most ambitious and transformative technical support projects launched by the European Commission (DG REFORM) in the financial sector and access to finance policy domain: the EU Supervisory Digital Finance Academy (EU-SDFA). In the past two years the EU-SDFA has rapidly established itself as a renowned entity in the landscape of capacity-building activities for financial supervisory authorities. It is a unique cross-sectoral EU-wide initiative that aims to overcome sectoral barriers, foster a common culture and understanding of digital finance issues and build an inclusive community of financial sector experts capable of managing the disruptive challenges of digitalisation.

The EU-SDFA is a comprehensive policy-oriented training programme in Digital Finance. It combines foundational and advanced training weeks, online learning modules, workshops and other dissemination events. These are open to the EU financial supervisory community.The Academy format contributes to fostering a common shared culture among supervisors. It provides a space for them to openly discuss and learn from each others' experiences and practices. This consolidated platform is grounded on the contribution of various key partners, and notably the European University Institute, Florence School of Banking and Finance (EUI-FBF) and the three European Supervisory Authorities (ESAs).

The EU-SDFA capacity-building programme is founded on three principal conceptual pillars. The first pillar pertains to technologies and their applications. EU-SDFA activities expose participants to the primary technologies utilised in the domain of digital finance, thereby equipping them with a comprehensive understanding of their operational mechanisms, the challenges and risks emanating from utilising them and the novel opportunities they might engender. The second pillar focuses on policymaking and policy implementation, and supervisors can ensure the proper management of risks brought by digitalisation and understand the implications for daily supervisory activities by diving deeply into the rationale, functioning and implementation of the regulatory initiatives underpinning the Digital Finance Strategy. The third pillar focuses on developing practical skills. Through case studies and other practical group exercises, the EU-SDFA offers participants opportunities to develop the skills necessary to supervise digital finance activities and to learn how to use related technologies.

In the context of the Academy, and in particular in the last few months, there has been a notable increase in the focus on AI applications and reflections on their impact on the financial system. Numerous residential and online sessions for financial supervisors across Europe have been meticulously organised, with a focus on exploring the primary domains of AI application, identifying opportunities for financial entities and users stemming from the utilisation of this technology and understanding its anticipated transformation of financial intermediation activities. Contributions have also enabled staff of the EU-SDFA participating National Competent Authorities (NCAs) to initiate exploration of the concrete functionality of these technologies and how the risks they can pose can be effectively mitigated. This exploration has involved reflection on the impact of the AI Act on the financial industry and supervisory activities.

The success of the second year of the Academy and its impact on the EU supervisory landscape would not have been possible without the collaboration of the European University Institute, Florence School of Banking and Finance, and the support of the three European Supervisory Authorities (ESAs). The

Institute's recognised academic expertise in the area of financial regulation, along with its historical ties with the EU institutions, agencies, and Member States, has been essential for the successful delivery and continuation of the programme. Concurrently, the EU-SDFA is complementary to the ESAs' initiatives aimed at aiding the development of a resilient, innovative and competitive financial system in the EU. Input from the financial and technology industries have also been instrumental in facilitating an open dialogue on the challenges posed by the dynamic evolution of digital finance. This e-book is further evidence of the commitment and coordination among the project partners and of their joint effort to achieve a common long-term goal: to establish and nurture a community of financial supervisors proficient in digital technologies.

Introduction

Lorenzo Moretti
Florence School of Banking and Finance, European University Institute

This second EU-Supervisory Digital Finance Academy e-book is being published two years after the launch of the EU-SDFA project. It follows the first e-book (Beck, Giani, and Sciascia, 2023) and shares its twofold objectives. First, it aims to provide the participants in the Academy with a complementary source of knowledge, analysis, and reflection. The content is inspired by the key courses and topics covered in the past 12 months of the EU-SDFA. Second, however, the e-book aims to extend the intellectual community of the Academy by offering a source of knowledge – and hopefully inspiration for debate – to an audience beyond the participants. Although all the authors are also important contributors to the EU-SDFA, in writing these chapters they are speaking to the broader policy-making and financial service industry community that is interested in understanding more about the deep impact digitalisation is having on the sector and the shaping role of regulation.

Because of its nature, this e-book is also highly interdisciplinary. Readers will find contributions by economists, lawyers, political scientists and authors deeply involved in the policymaking and regulatory activities concerning digital finance in Europe. Our hope is that this unique blend of perspectives will allow this publication to speak to as broad an audience as possible. We hope it will foster much needed dialogue on the future of European innovation in the financial sector.

This year's e-book is structured in two main sections. The first builds on last year's edition and provides an update and reflections on the main technological and regulatory developments relevant to digital finance in Europe. Chapter 1.1 provides a picture of technological and business trends that have revolutionised financial services in recent years together with the geopolitical implications of cloud computing, distributed ledger technologies, AI, and the role of big techs. Chapter 1.2 complements this view with a summary of the relevant European regulatory landscape. In this section, the regulatory-driven nature of the European innovation ecosystem clearly emerges (Majone 1994, Thatcher 2014). In Europe, regulation does not arise simply as a reaction to private-led technological initiatives. Instead, it aims to be a proactive force promoting innovation. Its aim is to provide clear rules of the game for all actors to follow, a logic which is a key ingredient in what has been referred to as the "Brussels effect" (Bradford, 2020). Importantly, the section also provides supervisors and financial service industry professionals with an up-to-date overview of relevant regulations and their evolution.

The second section dives into the latest and arguably most defining trend in the past couple of years: the rise of Artificial Intelligence (AI). The section offers a unique interdisciplinary perspective on this topic, with original reflections on the implications for regulators and supervisors. With contributions from different academic disciplines and all the partners of the EU-SDFA, including DG Reform and the European Supervisory Agencies, the section offers readers a balanced view of how AI can improve financial services and the risks to which consumers, investors, and supervisors must be alert.

Chapter 2.1 starts by looking at how AI is being utilised in the financial sector today and its broader future potential. It explains why financial services represent a high-potential field for the application of AI and focuses on use cases such as credit risk management, sustainable finance, and asset management. It also shows how in several of these areas AI is not necessarily introducing entirely new activities but instead accelerating trends that were already underway in the past decade. Therefore, the chapter partially offers a reassuring note for regulators and supervisors, implying that not all challenges posed by AI are novel and that existing regulatory tools can go a long way to mitigate AI risks. Chapters 2.2 and 2.3 build on this by shifting the focus to the risks associated with widespread AI adoption in financial services. They cover both direct risks to financial stability and indirect risks related to environmental, social and governance (ESG) factors. The discussion encompasses the potential for AI-driven market volatility, cybersecurity threats, the intensity of energy and data demands of AI models, and the ethical implications of AI decision-making in financial contexts. Chapter 2.4 introduces the perspective of supervisors. While supervisors will need to manage the challenges arising from regulating the use of AI in this complex industry, the chapter explains how AI can be used to the advantage of supervisors and offers original data on their current use of it.[1] An analysis of regulatory approaches to AI follows. Chapter 2.5 broadens the perspective by offering a cross-country view of how the rest of the world is addressing the complex issue of AI regulation. Chapter 2.6 focuses on Europe's approach and explains the genesis and legal approach behind the EU's pioneering AI Act. Chapter 2.7 concludes the section with reflections on the trade-offs between the potential benefits of AI in financial services and the new risks this technology may introduce.

Certainly, each of the topics this e-book covers is complex and multifaced. The goal of the publication is not to provide a comprehensive view of each one. Instead, it aims to be a helpful handbook, for supervisors and regulators in particular, to navigate the fast-changing world of digital finance, interpret new and ongoing developments, and discuss possible implications for the future.

References

Beck T., Giani L. and Sciascia G. (2023). Digital Finance in the EU: Drivers, Risks, Opportunities. San Domenico di Fiesole: European University Institute, 2023, EU Supervisory Digital Finance Academy (EU-SDFA) - 101092497. Available here.

Bradford A. (2020). The Brussels Effect: How the European Union Rules the World. *Faculty Books*. 232.

Cambridge SupTech Lab. (2024). State of SupTech Report 2024. Cambridge.

Majone G. (1994). The rise of the regulatory state in Europe. *West European Politics,* 17(3), 77-101.

Thatcher M. (2014). From old to new industrial policy via economic regulation. *Rivista Della Regolazione Dei Mercati*, 2, 6-22.

1 The data in this chapter are a subset of the data presented in the latest version of the State of SupTech Report by the Cambridge SupTech Lab.

Section 1

Digital Finance Macro Trends

1. Market developments based on digital technologies

Nico Lauridsen

Florence School of Banking and Finance, European University Institute

Nikolas Passos

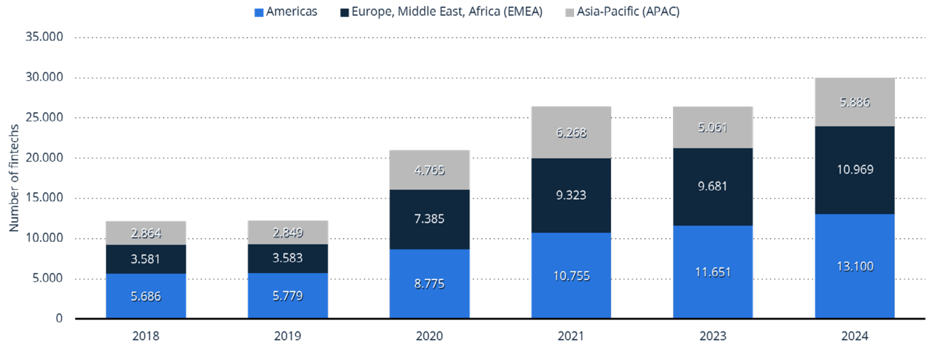
Florence School of Banking and Finance, European University Institute

1. The Outlook for the FinTech Market: Global and European Trends and Projections

This chapter aims to provide an overview of the recent trajectory of the FinTech market by identifying and critically examining the crucial factors that have shaped its evolution at the global and European levels. Particular attention is given to technological advances and the implementation of new regulatory frameworks, both of which have been instrumental in driving innovation in the sector (Financial Stability Board, 2019; Boot et al., 2021; Beck at al., 2022). The chapter explores two main aspects of FinTech growth. First, it covers the increase in market participants and the growing volume of financial transactions due to improved access to funding. Second, it analyses the ongoing consolidation of the industry driven by recent macroeconomic shifts and considers the broader implications for market structure and competition (Propson et al., 2024). By focusing on these two areas, the chapter aims to provide a descriptive analysis of how the market is responding to current global challenges such as geopolitical risks and inflation. It also explores the policy considerations surrounding the adoption and enforcement of new regulatory frameworks in the realm of digital finance. Indeed, the evolution of the FinTech market has taken place in a historical moment of favourable macro conditions and non-dedicated regulatory regimes. To discuss the outlook for the FinTech market and its development it is essential to analyse current shifts in global trends. The analysis of market trends considers a time horizon of five years, both prior to and following the present. This approach is necessary due to the high volatility of the macroeconomic environment, which complicates discussion of potential implications for market structure in the medium to long term.

The graph in Figure 1 shows the growth in the total number of FinTech companies worldwide from 2018 to 2024 by region in total numbers. It shows a significant increase in the number of FinTechs in different parts of the world. Particularly due to the innovation market in the United States and the increasing use of digital financial services in Latin America, the Americas have experienced the most substantial growth. In 2023 alone, nearly 1,500 new companies were added in this region. On the other hand, the European, Middle East, Africa (EMEA), and Asia-Pacific (APAC) regions grew at a slower pace, mainly due to varying market conditions, regulations, and levels of digital infrastructure. The strong increase in the Americas results from the region's key role in shaping global FinTech trends, with its environment supporting ongoing innovation and investment (Bakker et al., 2023). The contraction between 2021 and 2023 in APAC and the slow increase in EMEA and the Americas suggest that the pandemic shock and the geopolitical tension that caused a change in macroeconomic and monetary policy had an impact on the overall growth of the FinTech market (Ziegler et al., 2022; Jimenez et al., 2022).

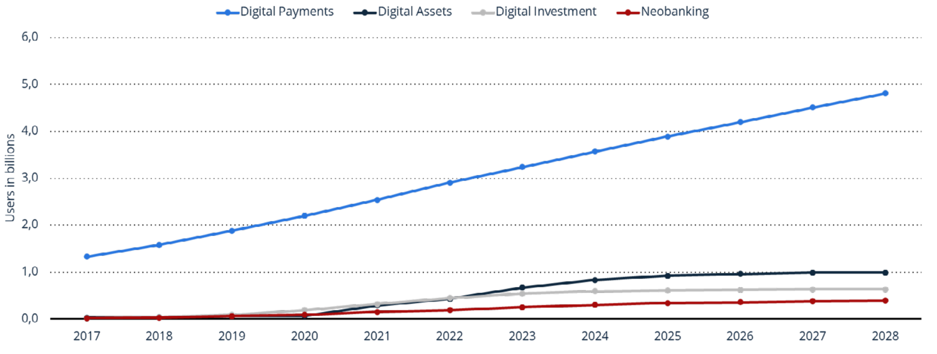
Figure 1. Numbers of FinTechs worldwide from 2018 to 2024, by region



As of January 2024, the Americas (North America, South America, Central America and the Caribbean) were the region with the largest number of FinTechs globally. There were approximately 13,100 FinTechs in the Americas, almost 1,500 more than a year before. In comparison, there were 10,969 FinTechs in the EMEA region (Europe, the Middle East and Africa) and 5,886 in the Asia Pacific region. In 2023, the United States ranked first in terms of the number of FinTech unicorns globally. Note(s): 2018 to 2024. Source(s): BCG; CrunchBase; Statista

Moving forward in our discussion, Figure 2 shows the number of FinTech users worldwide from 2017 to 2023 and forecasts up to 2028 by sector. It highlights major trends in user adoption in different FinTech sectors. Digital payments stand out as the dominant sector, with projections indicating a rise to 4.81 billion users by 2028. This reflects the status of digital payments as the most accessible and widespread entry point for consumers engaging with FinTech services. While other sectors are also growing, they remain significantly below this level, reflecting the continued importance of payments in the broader FinTech ecosystem. The data also show the economic disruption caused by the Russia-Ukraine war, which is likely to have led to the observable fluctuations in user adoption patterns during this period, further shaping the trajectory of the global FinTech landscape. Indeed, this evidence reveals the crucial role of payments as a fundamental data source of growth of the platform business model, such as open banking models (Berg et al., 2022; Dinçkol et al., 2023; Cornelli et al.,2023).

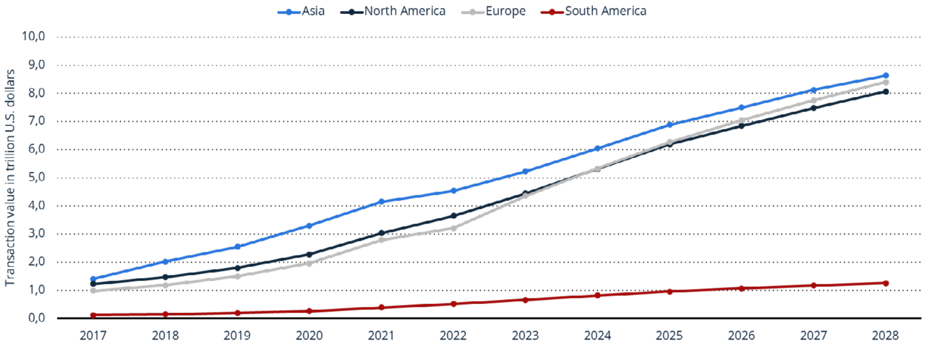
Figure 2. Numbers of FinTech users worldwide from 2017 to 2023, with forecasts from 2024 to 2028, by sector (in billions)



Over the period until 2028, the number of FinTech users is forecast to exhibit fluctuations among the four observed sectors. The number of digital payment users is forecast to grow gradually and reach 4.81 billion in 2028. According to Statista Market Insights, all other sectors are forecast to increase their user base too, although they are estimated to remain well below the number of digital payment users. Note(s): Worldwide, 2017 to 2023; the data shown use current exchange rates and reflect the impact on the market of the Russia-Ukraine war. Source(s): Statista Digital Market Insights

This initial evidence is expanded in Figure 3, which shows global trends and illustrates the transaction value of the FinTech industry worldwide from 2017 to 2023, with projections extending to 2028 and broken down by region. Asia experienced the most significant growth in transaction value, surpassing North America and Europe between 2019 and 2023. Asia is projected to maintain its leadership in transaction volumes until 2028, which reflects the region's rapid adoption of FinTech services and the expansion of its digital economy. North America and Europe continue to show steady growth, albeit at a slower rate than Asia. Despite showing an upward trend, South America remains significantly behind in terms of transaction value.

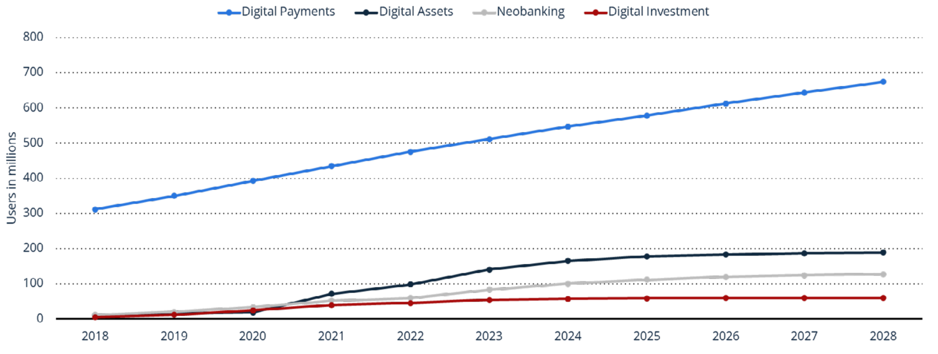
Figure 3. The transaction value of the FinTech industry worldwide from 2017 to 2023, with forecasts from 2024 to 2028, by region (in trillion USD)



The transaction value of the FinTech industry is forecast to notably increase between 2023 and 2028 in all the observed regions. The region with the highest transaction value between 2019 and 2023 was Asia, followed by North America and Europe. Asia is expected to hold its leading position in terms of transaction value in the coming years too. Further information and methodological notes can be found in Statista's Digital Market Insights. Note(s): North America, Asia, Europe, Central and South America, 2017 to 2023; the data shown use current exchange rates and reflect the impact on the market of the Russia-Ukraine war. Source(s): Statista Digital Market Insights.

Moving forward to an analysis of the outlook for FinTech, Figure 4 focuses on the European FinTech sector, which experienced significant and steady growth from 2018 to 2023. The number of users in all sectors rose consistently in line with the global trend, with the digital payments sector standing out as a critical driver. It is projected that the number of users in this sector will reach 674.62 million by 2028. This growth can be attributed in part to the evolution of open banking regulatory frameworks, the revision of the Payment Services Directive 2 (PSD2) to PSD3, and the design of open finance through financial data access and payments (FiDA). These developments have facilitated greater FinTech adoption across the continent, which promotes business models such as banking as a service and finance as a service (Babina et al., 2024; He et al., 2023; OECD, 2023).

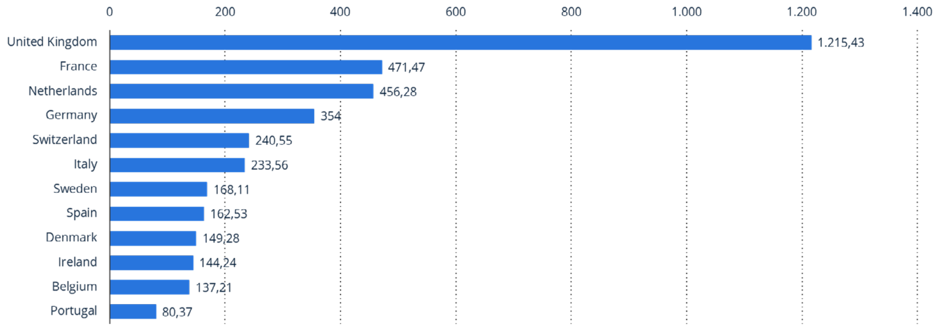
Figure 4. The number of FinTech users in Europe from 2018 to 2028, by sector (in millions)



The number of users is forecast to significantly increase in all sectors. The trend from 2018 to 2028 remains consistent throughout the entire forecast period. There is a continual increase in all sectors. Notably, the digital payments segment achieves the highest value of 674.62 million users in 2028. Note(s): Europe, 2018 to 2028; the data shown use current exchange rates and reflect the impact on the market of the Russia-Ukraine war. Source(s): Statista Digital Market Insights.

Figure 5 shows the volume of transactions in 2023. It shows that the UK is one of the most advanced markets globally, with transaction values surpassing 1.2 trillion USD. France and the Netherlands also have significant transaction volumes. The transaction values of these countries exceed those of other European countries, with France at 471.47 billion USD and the Netherlands at 456.28 billion USD ranking second and third respectively. The UK's dominant position in FinTech nearly three times higher than those of these major players shows its unparalleled market strength. Germany follows with a transaction value of 354.09 billion USD, significantly trailing the UK and revealing a gap between the UK FinTech ecosystem and the rest of Europe. Switzerland, Italy and Sweden display competitive but smaller transaction volumes, revealing the UK's apparent advantage. The maturity of the UK market underscores the continued relevance to FinTech of access to capital. It is necessary to address the complexity of EU regulatory frameworks to facilitate innovation and attract capital to Europe.

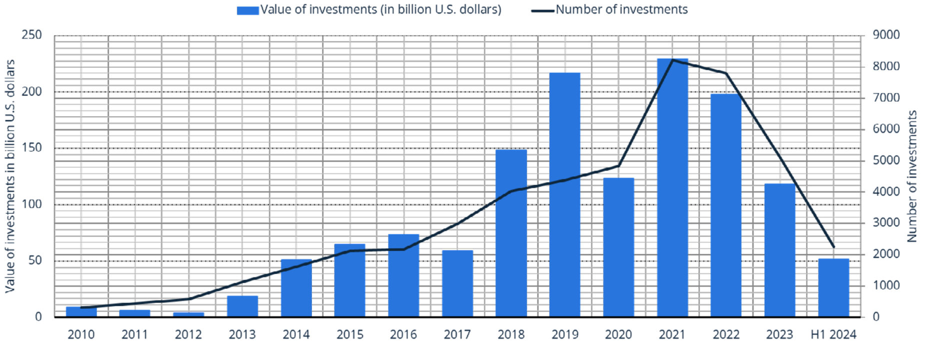
Figure 5. The FinTech transaction value in Europe in 2023, by country (in billion USD)



In 2023 the value of FinTech transactions exceeded 1.2 trillion USD in the United Kingdom, making it the European market with the highest FinTech transaction value generated. The United Kingdom was followed by France and the Netherlands with roughly 471.5 and 456.3 billion USD respectively. Further information and methodological notes can be found in Statista's Digital Market Insights. Note(s): Belgium, Denmark, France, Germany, Ireland, Italy, Netherlands, Portugal, Spain, Sweden, Switzerland and the United Kingdom, 2023; the data shown use current exchange rates and reflect the impact on the market of the Russia-Ukraine war. Source(s): Statista Digital Market Insights.

The analysis continues with the global evolution of the value of FinTech investments (in billion USD) and the number of investments from 2010 to the first half of 2024, as Figure 6 depicts. Following consistent growth since 2010, investments reached a peak of 216.8 billion USD in 2019. However, 2020 saw a significant decline due to the impact of the COVID-19 pandemic, with investments dropping to 124 billion USD. A strong recovery ensued in 2021, surpassing 229 billion USD in investments. Nevertheless, from 2022 onwards, the FinTech sector encountered renewed challenges, including the 'VC winter' with decreased venture capital funding and higher investor risk aversion. This downturn was further exacerbated by inflationary pressures resulting from geopolitical tensions, particularly the war in Ukraine, which disrupted global markets and heightened economic uncertainty, leading to a change in monetary policy with an increase in interest rates. The collapse of Silicon Valley Bank in early 2023 further rattled confidence in the sector, leading to concerns about liquidity and tighter capital flows (Bellavitis et al., 2023; Ma and Zimmermann, 2023). Despite these hindrances, the FinTech industry still managed to attract 118.2 billion USD in global funding in 2023, although the trend continued to decline in the first half of 2024. The ongoing volatility shows the susceptibility of the FinTech market to external macroeconomic factors, with the Americas remaining the most attractive region for capital inflows.

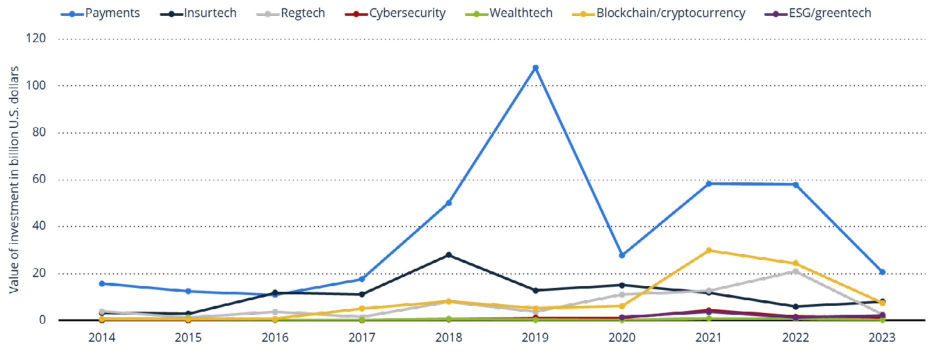
Figure 6. The value and number of investments in FinTech worldwide from 2010 to the first half of 2024



Global FinTech investments saw a dramatic rise from 2010 to 2019, peaking at 216.8 billion USD. In 2020 investments dropped sharply to below 124 billion USD, but rebounded in 2021 to over 229 billion USD. 2022 experienced another decline although not as severe as in 2020. The downward trend continued in 2023, with global funding reaching 118.2 billion USD. Throughout these fluctuations the Americas was the region that attracted the most investments. Note(s): Worldwide, 2010 to H1 2024. Source(s): KPMG; PitchBook.

Figure 7 provides a detailed analysis of access to VC funding in the FinTech market. The graph illustrates global FinTech investments in different sectors from 2014 to 2023. The payments sector consistently attracted the highest levels of investment, reaching over 100 billion USD in 2019 before experiencing a significant decline. In 2023, investments in payments amounted to 20.7 billion USD, a sharp drop from previous years. This evidence suggests a consolidatory trend for payment neobanks, which are extending their platforms to other market sectors and leveraging data network effects. Most other sectors, including Insurtech, RegTech, Wealthtech and blockchain/cryptocurrency, also followed a similar downward trend, reflecting broader challenges in the FinTech space. However, two sectors – cybersecurity and ESG/GreenTech – stood out in 2023 with increased investment compared to 2022 due to the emerging risks in the geopolitical situation and climate change. This reflects a growing interest in sustainability and security in financial technology. Overall, the data indicate a shift in priorities in FinTech investments as market conditions evolve.

Figure 7. The value of investment in FinTech worldwide from 2014 to 2023 in selected sectors (in billion USD)



The payments sector of the global FinTech industry attracted the highest investment value worldwide between 2014 and 2023. In 2023 the value of investment in this sector amounted to 20.7 billion USD, which was a sharp decrease compared to the previous years. Almost every other sector experienced a similar drop in investments in 2023. There were, however, two FinTech sectors that attracted more investment in 2023 than in 2022: insurtech and ESG/GreenTech. Note(s): Worldwide, 2014 to 2023; figures include venture capital, private equity and mergers and acquisitions deals. Source(s): KPMG; PitchBook.

In conclusion, the global FinTech market has seen significant regional variations. The Americas have experienced the most growth, primarily due to the U.S. and the increased adoption of digital financial services in Latin America. However, EMEA and APAC faced slower growth due to regulatory and market challenges. Despite these differences, digital payments continue to be the dominant FinTech segment globally, influencing user adoption trends. While Asia has surpassed other regions in transaction volumes, the European market, particularly the UK, remains strong and is supported by advances in open banking and regulatory frameworks. However, the sector is encountering challenges, such as reduced investment flows and external macroeconomic pressures, which are influencing the future direction of the market.

2. Regulatory considerations

Discussion on the outlook for the FinTech market continues to highlight the structural disparities between market-driven and regulatory-driven ecosystems. These differing approaches are deeply rooted in a geopolitical landscape marked by heightened uncertainty and rapid technological progress. Recent advances in generative AI have sparked concerns about the potential impact of growing inequality in artificial intelligence, reflecting the highly concentrated market and supply chain, which could amplify socioeconomic disparities within and across countries (Acemoglu, 2024). At the same time, ongoing efforts to enhance the coherence of the European Union have refocused attention on the debate surrounding over-regulated economic systems that may stifle innovation (EC, 2024). However, regulations continue to play a pivotal role in financial systems to maintain financial stability and foster financial innovation, which is endogenous to economic growth (Laeven et al., 2015; Cevik, 2024). The design of the regulatory framework in the European Union digital finance strategy illustrates the EU shift from a 'same risk, same rules' approach to a more function-based regulation addressing emerging risks stemming from financial innovation, such as cyber risk and exposure to crypto-assets (Borio et al., 2022). Furthermore, open banking and finance frameworks advocate consumer-centric utilisation of data to access financial services, fostering financial innovation and enhancing market competition (OECD, 2023). In addition, to reduce pressure on the market and promote financial innovation, regulators and supervisors have created innovation hubs and sandboxes, designing spaces where technology can be safely tested and developed (Feyen, 2021). The effectiveness of innovation facilitators has been limited in the FinTech market due to the varying levels of maturity in the ecosystem and fragmented regulatory enforcement (Cornelli et al., 2024). It is crucial to enforce and implement the European Union digital finance strategy to reduce regulatory arbitrage both within and outside the EU, and to support financial innovation (Buchak et al., 2018). To address these challenges, new regulatory enforcement should be accompanied by policies that facilitate innovation, empower consumer data and promote financial literacy as fundamental pillars of digital finance. As a result, the EU will continue to be a highly regulated and rigid market, but it will also be more resilient and less susceptible to external shocks with overall stronger consumer protection. In the end, the enforcement of digital finance regulatory frameworks should be considered a harmonisation of the rules in the EU FinTech market, and this process should be supported by an active policy to empower customers in the use of emerging technologies in financial services.

3. SupTech

As the financial intermediary market undergoes a digital transformation, regulators and supervisors are also leveraging technologies to enhance the efficiency of their day-to-day oversight activities. The use of 'innovative' technologies in financial supervision, often called SupTech, is becoming widespread among National Competition Authorities (NCAs). However, the definition of SupTech is still developing as technologies evolve. This is aligned with the digital transformation of NCAs, which involves improving and automating supervisory technology. Technology neutrality allows supervisors to harness the same data-driven applications used in the market to design supervisory tools. SupTech utilises the same data and information that the market generates to enhance microprudential and macroprudential activities (Di Castri et al., 2019). Adoption of this technology is revolutionising supervisor practices, prompting a structure change in their authority in the current European supervisory architecture. Indeed, this NCA technological change is fundamental for supervisors to continue to fulfil their mandate to maintain financial stability and market integrity by trying to keep up with the speed of technological change in the market. This digital transformation of NCAs follows heterogeneous paths depending on the specific characteristics of the country and organisations. However, some common trends and development areas in which NCAs are focusing their resources and capacity (Di Castri et al., 2023; Prenio, 2024) are listed below.

- **Prudential Supervision**. NCAs use SupTech solutions to collect, validate and manage supervisory data. This includes using API-based prudential reporting platforms, electronic data warehouses and automated regulatory reporting processes.

- **Supervision of Consumer Protection and Market Conduct.** SupTech solutions are used to enhance complaint management and analysis, and also to analyse sentiment in web content and social media.

- **Anti-Money Laundering/Counter-Terrorism Financing and Counter Proliferation Financing (AML/CFT/CPF)**. SupTech solutions are employed to improve AML supervision by enabling advanced data analytics to assess risks and control the frameworks of supervised entities. Examples include using network analysis to track fund transfers to high-risk jurisdictions and machine learning tools to examine the internal control frameworks of banks.

- **Misconduct Analysis**. NCAs use big data architecture and AI tools for analysis of misconduct, including in the fight against financial crime.
- **Data Management**. SupTech solutions are used to improve data management, including storage, organisation, querying and data analysis.
- **Financial Risk Assessment**. NCAs are developing SupTech tools to support financial risk assessments, although this is an area where successful development and implementation can be challenging.
- **Macro Forecasting.** NCAs employ SupTech tools for macro forecasting to predict market trends and systemic risks. These tools leverage big data and machine learning to produce forecasts of economic conditions, asset bubbles and other indicators critical to maintain market stability.

Development of SupTech is still in its early stages, and significant efforts are needed to effectively integrate emerging technologies in NCAs and improve supervision practices. To achieve this, NCAs must address challenges related to user accessibility, data integration, capacity building and change management. Furthermore, common internal and external barriers such as organisational structures are hindering the widespread adoption of SupTech by NCAs, which limits the scalability and full potential of these innovative technologies (Di Castri et al., 2023; Prenio, 2024). Below is a summary of these fundamental barriers and challenges.

- **Budget constraints and costs of development.** The development and implementation of SupTech solutions require a significant investment in infrastructure, software and training personnel over the lifecycle of the tools, which requires direct budget lines involving several NCA units.
- **Legacy systems vs. migration to the cloud.** NCAs still rely on outdated IT systems that are not designed to handle the large volumes of complex data that SupTech solutions require. Integrating new technologies in legacy systems can be complex, expensive and risky. However, adopting cloud computing facilitates the development of SupTech, even though increased reliance on technology also increases vulnerability to cyberattacks and data breaches. NCAs need to implement effective security measures to protect sensitive data and ensure the integrity of SupTech systems with a dedicated cloud strategy.

- **The procurement process.** NCAs rely on external vendors to develop and maintain SupTech solutions. This reliance on third parties can lead to risks related to data security, business continuity and solution flexibility that is not aligned with the lifecycle of the solution.

- **Lack of human resources and skills.** The rapid evolution of SupTech technologies requires specific IT and data analysis skills that are in short supply in many NCAs. A lack of adequately trained personnel is a significant obstacle to the effective implementation and management of SupTech solutions.

- **Lack of strategy and resistance to change.** Adopting SupTech often involves significant changes to operational processes and organisational culture. Staff resistance to change can hinder the implementation of new technologies and undermine their effectiveness.

- **Lack of cross-border coordination.** Access to comprehensive data is crucial for SupTech development. However, many NCAs face difficulties coordinating with other agencies to gain access to the necessary data. A lack of data sharing and standardisation can limit the ability of SupTech solutions to provide complete and accurate insights.

- **Legal and procedural frameworks.** Existing regulations regarding data protection, privacy and information security can pose obstacles to the adoption of SupTech. NCAs must ensure that SupTech solutions comply with legal requirements and that sensitive data are adequately protected both within and outside NCA organisations. Cloud adoption should reduce this barrier to SupTech and provide secure infrastructure for data sharing and collection.

Adoption of SupTech has followed different paths depending on the specific characteristics of individual organisations and countries. However, in the European context, the digital transformation of NCAs should be contextualised within current supervisory architecture to facilitate the technological development of SupTech and the stability of solutions (Carletti et al., 2021). Structural challenges and barriers must be analysed as internal and external factors that affect the adoption of SupTech and as a function of the different mandates NCAs have at the national and international levels in the European supervisory architecture. Indeed, there is a need to develop harmonised SupTech strategies that consider the national and EU dimensions as fundamental factors in scaling up the digital transformation of NCAs. Adoption of heterogeneous SupTech reflects different approaches followed by NCAs in developing strategies for the digital transformation of their organisation. Indeed, not all NCAs have followed top-down holistic approaches to SupTech which directly improve data and cloud strategies, re-design their IT infrastructure and relate internal and extra data collection processes to reformulated plans and changed management processes. This holistic approach requires a medium or long-term investment horizon to bring about lasting change in the organisation. This change will enable financial supervisors to effectively respond to challenges posed by the digital transformation by empowering them with the same technologies as market players. At the same time, most NCAs approach SupTech through bottom-up experience, in which single units or divisions develop in-house solutions for specific needs. These non-organic paths underlie structural barriers to SupTech which need cross-border collaboration with the EU perimeter to design blueprint solutions with codeshare pipelines for common solutions that can be implemented and adopted in an approach based on the specific needs of NCAs. This approach based on promoting collaboration and knowledge-sharing through NCA cooperation should be reflected in the current supervisory architecture to create a hub and spoke model of SupTech development to reduce the cost of development and improve scalability, thus overcoming the problem of a lack of human resources and capacity of NCAs (Crisanto et al., 2022; Gopalan, 2021). In the end, the efficiency and impact of SupTech would be limited without improving cross-border collaboration and radical change in how NCAs view emerging technologies.

4. The geopolitics of digital finance

Building on the analysis of recent FinTech growth trends and the role of innovation in shaping global financial markets, it is essential to recognise that broader geopolitical forces increasingly influence the digital finance landscape. As FinTech continues to evolve, its trajectory is now intertwined with a complex multipolar world marked by a growing nationalistic focus and international instability (Szczepanski, 2024). Geopolitical instability has shaken the financial world, with a recent survey showing that central banks and sovereign wealth fund managers now view geopolitical concerns, rather than inflation, as the primary risk to global economic growth (Torkington, 2024). The race for technological dominance by nations and corporations has intensified competition to control the next wave of financial innovation.

Understanding the impact of geopolitics on digital finance is complex. However, classical frameworks for analysing global power structures remain relevant. Classical power categories – such as security, knowledge and finance (Strange, 1988) – are now found in new national strategic objectives.

These new objectives include digital sovereignty, technological supremacy and monetary hegemony. In the following sections, we examine each of these objectives individually. Using specific technological examples, we illustrate how geopolitical struggles are shaped by the influence of Big Tech, advances in artificial intelligence and adoption of distributed ledger technologies (See Table 1).

Table 1: Strategic Objectives and Technological Frontiers in Digital Finance Geopolitics

Power structure	**Strategic Objective**	**Technological frontier**
Security	Digital Sovereignty	Big Tech and cloud computing
Knowledge	Technological Supremacy	Artificial Intelligence
Finance	Monetary Hegemony	DLT technologies and CBDCs

Source: Author's elaboration

Digital sovereignty and Big Tech concentration

Major Big Tech companies, in particular ones in the United States and China, play a pivotal role in technological advances in digital finance. These companies not only offer direct financial services but also provide critical digital infrastructure, including cloud services, cybersecurity software and AI applications.

The direct involvement of Big Tech in finance is mainly concentrated in payments and e-money. In Europe, a joint ESAs report (2024) concluded that direct finance services by Big Techs do not yet pose significant risks from a financial stability perspective, but continual monitoring is necessary (JC ESAs, 2024, p.19).

However, the indirect impact of Big Tech on financial services presents more significant challenges, especially in terms of operational resilience and cybersecurity risks (JC ESAs, 2024, p.12). Resilience concerns arise regarding the deep interconnections of Big Tech with established financial institutions, particularly through the provision of essential third-party services like cloud storage, which renders them "too critical to fail" (James and Quaglia, 2024, p.6). The concentration in processing and storage is vast. In the global cloud storage market, U.S. companies hold a dominant position with AWS capturing 31% of the market share, Microsoft Azure 25% and Google Cloud 11% (Richter, 2024). Some Chinese companies (Alibaba and Tencent) also account for a smaller market share (Richter, 2024).

In 2024, the criticality of Big Tech services became evident after a global IT outage caused by tech company CrowdStrike in an update of a Microsoft software, which showed the risks of over-reliance on a single technology. A corrupted file in a security software update caused hour-long outages for banks, investment firms and stock exchanges, which impacted the real economy and even led to airport closures (Davies, 2024). In addition to cyber incidents, processing concentration is notably evident in payment systems. For instance, a US-based FinTech notes that "a big portion of payments in Europe and the UK [relies on] US companies [...] This critical infrastructure is so stacked from a US standpoint that you may be the target of global actors having a go at that infrastructure" (Quinio, 2024).

To tackle concentration challenges, countries have adopted diverging regulatory approaches to Big Tech (Bradford, 2023), which could increase fragmentation and escalate geopolitical tensions. In the global battle to regulate technology, the USA, China and Europe have followed divergent paths, relying on market-driven, state-driven and rights-driven approaches respectively (Bradford, 2023). Big Techs are therefore poised to navigate these competing regulatory models – sometimes with regulatory arbitrage, or "the choice of violating one law or the other" (Bradford, 2023). Regulatory disputes on data sovereignty, taxation and competition may lead to changes in Big Tech behaviour, thus hindering efforts to ensure cyber security and financial stability.

Technological supremacy and artificial intelligence

The development of AI technologies has introduced a new dimension to the geopolitical landscape of digital finance. "Notable machine learning models" – ones identified as particularly influential in the AI and machine learning ecosystem – are heavily concentrated in a few countries, with the United States leading the field (Maslej et al., 2024). According to a 2024 Artificial Intelligence Index Report by Stanford University, in 2023 U.S.-based institutions developed 61 notable models, compared to 21 in the European Union and 15 in China. (Maslej et al., 2024). More significantly, the US west coast provides AI-generated responses to billions of users, relying on models trained on data lacking global diversity (Mayer-Schönberger, 2024). In response to this concentration, countries have implemented AI industrial policies, leading to a rise of "AI nationalism" and further regulatory fragmentation (Aaronson, 2024).

In the financial sector, the concentration of AI development introduces new risks. The BIS notes that reliance on a few Big Tech firms for AI development increases data dependence and raises concerns about cybersecurity and financial stability (Aldasoro et al., 2024). A concentrated AI ecosystem built on similar datasets can embed correlated biases, potentially resulting in inadequate risk assessment. This challenge is intensified by the complexity of AI models, making oversight more difficult for both companies and supervisors.

The risks posed by AI in finance are further exacerbated by AI nationalism and fragmented regulatory responses. The BIS highlights a need to foster dialogue among stakeholders and promote interdisciplinary collaboration to develop robust frameworks that harness innovation for societal welfare (Aldasoro et al., 2024, p.28). Moreover, the concentration on AI development has sparked calls for inclusive governance frameworks, context-specific solutions and collaborative funding to avoid perpetuating historical patterns of inequality (Ahmed, 2024).

The monetary hierarchy and the decentralisation of money

The digitalisation of finance also challenges the main structures in the international monetary system. In recent decades, the dominance of the US dollar has been pervasive, from the structure of external balance sheets to the currency composition of private portfolios to the choice of anchor currency, with consequences for trade and finance (Gopinath et al., 2020). While inertia and friction reinforce the dominance of the dollar, financial digitalisation could drive diversification and foster the development of new alternatives (Bilotta and Botti, 2023, p. 16).

New monetary alternatives may arise from the increased use of distributed ledger technologies by companies and governments. On the private front, the use of crypto assets, especially stablecoins, presents challenges to banks and payment institutions and is proposed as a way to reform the financial system (Catalini and Wu, 2024). The failed Facebook-led Libra project illustrates how stablecoins are perceived as a credible threat to existing monetary systems, facing sharp criticism from financial incumbents, legislative proposals to ban them and resistance from regulators (Catalini and Wu, 2024).

Countries have also reacted by exploring the implementation of Central Bank Digital Currencies (CBDCs). 134 countries, representing 98% of global GDP, are exploring CBDCs with a central aim to preserve the role of central bank money (Atlantic Council, 2024). Beyond national CBDC projects, international initiatives are becoming increasingly relevant. The BRICS-Bridge, for example, proposes a cross-border payment system designed to bypass traditional financial intermediaries, such as the U.S. dollar-based system (The Economist, 2024). Even BIS cross-border projects have gained geopolitical significance due to their potential to reshape the architecture of the global financial system (The Economist, 2024).

The long-term impact of the digitalisation of money on the decentralisation of the global financial system is still unclear. Bilotta (2024) outlines four potential scenarios: the emergence of a new hegemonic currency, the rise of a global digital currency, a fragmented and multipolar international monetary system or the continued dominance of the dollar. Although it is too early to predict how these scenarios will unfold, recent empirical studies suggest that CBDCs could enhance local control over payment systems and reduce reliance on foreign providers, underscoring their geopolitical importance (Berg et al., 2024). Nevertheless, any fundamental changes are likely to be gradual, and the dominance of the US dollar may endure, supported by its strong institutional and political foundation (Prasad, 2023).

The geopolitics of digital finance risks fragmenting the global financial system

Data sovereignty, technological supremacy and monetary hegemony are key strategic objectives shaping the geopolitics of digital finance. The interactions among these elements will play a crucial role in determining the future landscape of digital finance. Recently, countries have been competing for greater autonomy and displaying rising nationalism in all three areas.

In the realm of data, the concentration of power among a few Big Tech firms has attracted the attention of regulators and competition authorities due to their central role in storage, processing and cybersecurity. In the race for technological leadership, AI has taken centre stage, with nations concerned about the concentration of AI developments and potential biases stemming from skewed data sources intensifying their industrial policies. In the monetary sphere, cryptographic solutions have been promoted to decentralise international monetary systems, prompting countries to increasingly invest in CBDCs.

Pursuing these strategies in an uncoordinated way will lead to fragmentation of the global financial system. A lack of interoperability between national regulatory frameworks and digital currencies could exacerbate this fragmentation. Multilateralism and international cooperation are essential to establish clear, shared and neutral principles to guide future developments and prevent the risk of inefficiencies and fragmentation in the global economy (Bilotta, 2024).

References

Aaronson S. A. (2024). The Age of AI Nationalism and Its Effects. *Center for International Governance Innovation Papers*. No. 306. Available here. (last accessed on 22/10/2024).

Acemoglu D. (2024). The Simple Macroeconomics of AI. *MIT working paper*.

Ahmed S. (2024). The white saviour industrial complex and global AI governance. *EUI Ideas*. Available here. (last accessed on 22/10/2024).

Aldasoro I., Gambacorta L., Korinek A., Shreet, V., and Stein M. (2024). Intelligent financial system: how AI is transforming finance. *BIS Working Papers* No 1194. Monetary and Economic Department, June 2024.

Atlantic Council. (2024). Central Bank Digital Currencies Tracker. Available here. (last accessed on 22/10/2024).

Babina T., Buchak G., De Marco F., Gornall W., Mazzola F., and Yu T. (2024). Customer Data Access and FinTech Entry: Early Evidence from Open Banking. *NBER working paper series*.

Bakker B., Garcia-Nunes B., Lian W., Lui Y., Marulanda C., Siddiq A., Vasilyev D., and Yang Y. (2023). The Rise and Impact of FinTech in Latin America. *IMF FinTech Note* 2023/003.

Beck T., Cecchetti S., Grothe S., Kemp M., Pelizzon L., and Serrano A. (2022). Will video kill the radio star? – Digitalisation and the future of banking. *European Systemic Risk Board* No 12.

Bellavitis C., Fisch C., and Vismara D. (2023). Monetary Policy and Venture Capital Markets. *Review of Corporate Finance*. Vol. 3: No. 4, pp 627-662.

Berg T., Fuster A., and Puri M. (2022). FinTech Lending. *Annual Review of Financial Economics*. Volume 14.

Berg T., Keil J., Martini F., and Puri M. (2024). CBDCs, Payment Firms, and Geopolitics (No. w32857). *National Bureau of Economic Research*.

Bilotta N. (2024). The Geoeconomics of Money in the Digital Age. *Routledge*.

Bilotta N., and Botti F. (2023). Digitalisation and Geopolitics: Catalytic forces in the (future) International Monetary System. Istituto Affari Internazionali.

Boot A., Hoffmann P., Laeven L., and Ratnovski, L. (2021). FinTech: what's old, what's new? *Journal of Financial Stability*. 53.

Borio C., Claessens S., and Tarashev N. (2022). Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and Big Techs. *Financial Stability Institute*. Occasional Paper No 19.

Bradford, A. (2023). Digital empires: The global battle to regulate technology. Oxford University Press.

Buchak G., Matvos G., Piskorski T., and Seru, A. (2018). FinTech, regulatory arbitrage, and the rise of shadow banks. *Journal of Financial Economics*. 130(3), 453–483.

Carletti E., Dell'Ariccia G., and Marquez, R. (2021). Supervisory incentives in a banking union. *Management Science*. 67(1), 455–470.

Catalini C., and Wu J. (2024). The Race to Dominate Stablecoins. *Harvard Business Review*. Available here (last accessed on 22/10/2024).

Cevik S. (2024). Is Schumpeter Right? FinTech and Economic Growth. *IMF Working Paper*. WP/24/20.

Cornelli G., Doerr S., Gambacorta L., and Merrouche O. (2024). Regulatory Sandboxes and FinTech Funding: Evidence from the UK. *Review of Finance*. 28(1), 203-233.

Cornelli G., Frost J., Gambacorta L., Rau P. R., Wardrop, R., and Ziegler, T. (2023). FinTech and Big Tech credit: Drivers of the growth of digital lending. *Journal of Banking and Finance*. 148.

Crisanto J. C., Prenio J., Singh M., and Yong J. (2022). Emerging sound practices on supervisory capacity development. *FSI Insights on Policy Implementation*. No 46.

Davies P. (2024). CrowdStrike Outage Is Another Sharp Warning for Banks. *Bloomberg*. Available here. (last accessed on 22/10/2024).

Di Castri S., Grasser M., and Ongwae J. (2023). The State of SupTech Report 2023, *University of Cambridge*.

Di Castri S., Hohl S., Kulenkampff A., and Prenio J. (2019). The SupTech generations. *FSI Insights on Policy Implementation*. No 19.

Dinçkol D., Ozcan P., and Zachariadis M. (2023). Regulatory standards and consequences for industry architecture: The case of UK Open Banking. *Research Policy*. 52(6), 104760.

EC. (2024). The future of European competitiveness – A competitiveness strategy for Europe. European Commission.

Feyen E., Frost J., Gambacorta L., Natarajan H., and Saal M. (2021). FinTech and the digital transformation of financial services: implications for market structure and public policy. *BIS Papers*. No 117.

Financial Stability Board. (2019). FinTech and market structure in financial services: market developments and potential financial stability implications.

Gopalan Y., Kalda A., and Manela A. (2021). Hub-and-Spoke Regulation and Bank Leverage. *Review of Finance*, 25(5), 1499–1545.

Gopinath G., Boz E., Casas C., Díez F. J., Gourinchas P.-O., and Plagborg-Møller M. (2020). Dominant Currency Paradigm. *American Economic Review*, 110(3), 677–719. DOI: 10.1257/aer.20171201.

He Z., Huang J., and Zhou J. (2023). Open banking: Credit market competition when borrowers own the data. *Journal of Financial Economics*, 147(2), 449–474.

James S., and Quaglia L. (2024). Emergent regime complexity and epistemic barriers in 'bigtech' finance. *New Political Economy*, 29:6, 872-885, DOI: 10.1080/13563467.2024.2359940.

JC ESAs. (2024). Report on 2023 stocktaking of BigTech direct financial services provision in the EU. *Joint Committee of the European Supervisory Authorities*.

Jiménez G., Kuvshinov D., Peydró J., and Richter B. (2022). Monetary Policy, Inflation, and Crises: New Evidence from History and Administrative Data. *CEPR Working paper*.

Laeven L., Levine R., and Michalopoulos S. (2015). Financial innovation and endogenous growth. *Journal of Financial Intermediation*, 24(1), 1–24.

Ma T., and Zimmermann K. (2023). Monetary policy and innovation. *NBER Working Paper,* 31698.

Maslej N., Fattorini L., Perrault R., Parli V., Reuel A., Brynjolfsson E., Etchemendy J., Ligett K., Lyons T., Manyika J., Niebles J. C., Shoham Y., Wald R., and Clark J. (2024). The AI Index 2024 Annual Report. *AI Index Steering Committee*, Institute for Human-Centered AI, Stanford University. Available here. (last accessed on 22/10/2024).

Mayer-Schönberger V. (2024). A Realist Perspective on AI Regulation. *Foreign Policy*. Available here. (last accessed on 22/10/2024).

OECD. (2023). Open finance policy considerations. OECD Business and Finance Policy Papers. *OECD Publishing*, Paris.

Prasad, E. (2023). How will digital technologies influence the international monetary system? *Oxford Review of Economic Policy*, 39, 389–397. Available here.

Prenio J. (2024). Peering through the hype - assessing SupTech tools' transition from experimentation to supervision. *Financial Stability Institute Insights on policy implementation,* No 58.

Prospson D., Ajvazoska Ferri F., Mutinda S., Salman S., Shemin J., Suresh K., Xie Z., and Zhang B. (2024). The Future of Global FinTech: Towards Resilient and Inclusive Growth. *World Economic Forum & Cambridge Centre for Alternative Finance Report*.

Quinio A. (2024). Stripe-backed FinTech warns of Europe's over-reliance on US payment systems. *Financial Times,* 9 September 2024. Available here (last accessed on 22/10/2024).

Richter F. (2024). Amazon Maintains Cloud Lead as Microsoft Edges Closer. *Statista*. Available here. (last accessed on 22/10/2024).

Strange S. (1988). States and Markets: an Introduction to International Political Economy. *London: Pinter*.

Szczepanski M. (2024). The geopolitics of technology: Charting the EU's path in a competitive world. *European Parliamentary Research Service*. Available here. (last accessed on 22/10/2024).

The Economist. (2024). Putin's plan to defeat the dollar. *The Economist*. 20 October 2024. Available here. (last accessed on 22/10/2024).

Torkington S. (2024). Geopolitics replaces inflation as the top worry for central banks and sovereign wealth funds. *World Economic Forum*. 10 September 2024. Available here. (last accessed on 22/10/2024).

Ziegler T., Carvajal A. F., Propson D., Kekre N., Natarajan H., Suresh K., Salman D., Paes F. F. de C., Mutinda S., Wanga C., Xie Z., Zhang B., Rabadan G. A. G., Ramteke N. C., Closs C. L., Mammadova L., Alam N., Velandia C., Ghate K., Lauridsen N. and Rajain, V. (2022). The Global COVID-19 FinTech Market Impact and Industry Resilience Study. *World Bank, World Economic Forum & Cambridge Centre for Alternative Finance Report*.

2. A regulatory update on EU digital finance acts and measures

Leonardo Giani[1]

Florence School of Banking and Finance, European University Institute

1. Introduction

Following the elections of 6-9 June 2024 and the subsequent formation of a new European Commission, we are at the turn of a European term. At the time of writing this chapter, although digitalisation will probably remain at the top of the agenda, many details of European Union (EU) action in the coming years are not yet totally clear. Nonetheless, the time is ripe to review the initiatives taken in the past five years.[2] One of the six European Commission priorities for 2019-2024 was called 'A Europe fit for the digital age.'[3] Under this priority a wide number of initiatives were taken, and several acts were adopted. A com-

1 Leonardo Giani (EUI) devised and then coordinated the drafting of this chapter, but credit should be also given to: Daria Vernon De Mars (EUI) for the parts about Digital Operational Resilience Act (DORA), Laura Macchioni (EUI) for the parts about the Financial Data Access and Payments Package and Alessia Benevelli (EBA) and Nicola Bilotta (EUI) for the parts about the digital euro. Although responsibility remains with the authors, thanks for very helpful comments go to several members of the staff of the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA), who are involved in the EU-SDFA. This chapter was last updated on 1 November 2024.

2 A very useful briefing with an overview of the state of play concerning digital finance legislation was released on 16 May 2024 by the European Parliamentary Research Service. See Hallak (2024).

3 See here.

prehensive update about all these initiatives and acts would go far beyond the scope of this chapter.[4] It will therefore focus on initiatives taken at the EU level 'strictly speaking' on digital finance.

According to the European Commission,[5] 'strictly speaking' digital finance can be viewed as focusing on four main topics: (i) crypto-assets (e.g. MiCA, but also the DLT Pilot Regime); (ii) cyber resilience (e.g. DORA); (iii) open finance (e.g. FiDA, PSD3 and PSR); and (iv) the digital euro.

The first two of these topics were directly addressed in the so-called Digital Finance Package, which the European Commission released on 24 September 2020 and the EU has been implementing since then.[6] This package included the 'Digital Finance Strategy for the EU', a document setting out how Europe can support the digital transformation in the financial sector and regulate the risks involved,[7] which is built on the 2018 FinTech Action Plan[8] and the work of the European Supervisory Authorities (ESAs).[9] Together with the 'Digital Finance Strategy for the EU', the European Commission issued three now enacted legislative proposals concerning a new framework for the testing of DLT market infrastructures (the DLT Pilot Regime); the regulation on markets in crypto-assets (MiCA or MiCAR);[10] and the enhancement of digital operational resilience in the financial sector (DORA), plus a proposal on a review of some existing financial rules.

The Digital Finance Package also included a 'Retail Payments Strategy for the EU',[11] which together with the 'Digital Finance Strategy for the EU' can be viewed as the background documents for two additional legislative packages adopted at a later stage. Indeed, the last two topics mentioned above (i.e. open finance and the digital euro) have been covered by two more recent packages, both released by the European Commission on 28 June 2023, namely the Finan-

4 See the penultimate section of this chapter for more information.

5 See here.

6 See here.

7 COM(2020) 591 final.

8 COM(2018) 109 final.

9 For instance, following a request for technical advice on digital finance and related issues by the European Commission, in line with the intention to review the existing financial services legislation as outlined in the 'Digital Finance Strategy for the EU', the ESAs issued a joint report dated 31 January 2022, which is available here.

10 Both these acronyms are currently used in official documents as well as in the academic literature.

11 COM(2020) 592 final.

cial Data Access and Payments Package[12] and the Single Currency Package.[13] The first of these includes a legislative proposal for a Regulation on a framework for Financial Data Access (FiDA) and legislative proposals to amend and modernise the current Payment Services Directive (PSD2, which will become PSD3) and in addition to enact a Payment Services Regulation (PSR).[14] The second package includes a legislative proposal on the legal tender of euro cash and a legislative proposal establishing the legal framework for a possible digital euro.

Furthermore, other (legislative and non-legislative) initiatives were taken at the EU level. Some final information will be provided about one of the most relevant legislative initiatives, namely the Artificial Intelligence Act (AI Act).[15]

2. New legislation which is already applicable

Regulation (EU) 2022/858 was published in the Official Journal of the European Union on 2 June 2022. This Regulation is on a pilot regime for market infrastructures based on distributed ledger technology (DLT market infrastructures) and it is then usually referred to as the 'DLT Pilot Regime.' With a few exceptions, the DLT Pilot Regime applies since 23 March 2023.

The DLT Pilot Regime[16] aims to test DLT market infrastructures[17] in order to allow for the development of crypto-assets that qualify as financial instruments and distributed ledger technology (DLT). In doing so, a high level of investor protection, market integrity, financial stability and transparency should be preserved, and regulatory arbitrage and loopholes should be avoided. The largest part of the DLT Pilot Regime consists of seven articles that provide

12 See here.

13 See here.

14 In this field it is worth mentioning that on 19 March 2024 the so-called Instant Payments Regulation (IPR) [Regulation (EU) 2024/886] was published on the Official Journal of the European Union. Among other things, the IPR requires Payment Service Providers (PSPs) to make instant credit transfers available in addition to regular credit transfers, to do so at prices no higher than regular credit transfers and to carry out verification of the payee. Although the IPR entered into force on 8 April 2024, the timeline for the implementation of its various requirements follows a staggered approach (for more information see here).

15 Regulation (EU) 2024/1689.

16 See Recital 6 of Regulation (EU) 2022/858.

17 Meaning a DLT multilateral trading facility, a DLT settlement system or a DLT trading and settlement system.

for a discipline on requirements, exemptions and specific permission involving DLT market infrastructures. One of the most interesting parts of the DLT Pilot Regime concerns the exemptions to the general legislation applicable to the DLT market infrastructures, which are essentially conceived to allow for a tailored adaptation of the framework to the specific features and needs of crypto-assets.

The DLT Pilot Regime is (potentially) temporary. By 24 March 2026, the European Securities and Markets Authority (ESMA) shall present a report to the European Commission on a wide series of aspects related to the DLT Pilot Regime. On the basis of this report, within three months the European Commission shall present a report to the European Parliament and to the Council with a cost-benefit analysis on whether the pilot regime should be: (a) extended for a further period of up to three years; (b) extended to other types of DLT financial instruments; (c) amended; (d) made permanent through appropriate amendments of legislation; or (e) terminated.[18]

Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA or MiCAR) was published in the Official Journal of the European Union on 9 June 2023 and entered into force on 29 June 2023. Titles III and IV of MiCA [i.e. the regimes on asset-referenced tokens (ARTs) and electronic money tokens (EMTs)] entered into application on 30 June 2024. The remaining parts of MiCA shall apply from 30 December 2024, apart from some derogations.[19]

MiCA provides for a framework concerning the offer to the public and admission to trading on a trading platform of ARTs, EMTs and crypto-assets other than ARTs and EMTs, as well as requirements for crypto-asset service providers (CASPs).[20]

The difference between EMTs and ARTs is that the former are crypto-assets that purport to maintain a stable value by referencing the value of one official currency, while the latter are crypto-assets that are not EMTs and purport to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies.[21]

MiCA sets out that the European Banking Authority (EBA) is responsible for classifying ARTs and EMTs as significant and reassessing their significance on an annual basis. Additionally, issuers may voluntarily request their compe-

18 See Article 14 of Regulation (EU) 2022/858.

19 See Article 149 of Regulation (EU) 2023/1114.

20 See Article 1 of Regulation (EU) 2023/1114.

21 See Article 3 of Regulation (EU) 2023/1114.

tent authority to classify their ART or EMT as significant.

Once an ART or EMT is classified as significant, the relevant supervisory responsibilities are transferred from the respective home competent authority to the EBA. The EBA is responsible for conducting direct supervision of issuers of significant ARTs, while significant EMTs (when issued by electronic money institutions) are subject to 'dual supervision' by the EBA and the respective home competent authority. When these tokens are no longer classified as significant, the EBA transfers its supervisory responsibilities back to the respective competent authority.

It is important to note that MiCA does not apply, *inter alia*, to crypto-assets that qualify as financial instruments (or other specific types of tokenised financial products).[22] This marks an important difference between MiCA and the DLT Pilot Regime, as the latter focuses on a limited number of DLT financial instruments that can be admitted to trading on a DLT market infrastructure or be recorded on a DLT market infrastructure.[23]

MiCA provides for a large number of Level 2 and Level 3 measures to be developed by the ESAs before the Regulation (Level 1) becomes fully applicable.

The EBA has completed the delivery of all the technical standards and guidelines applicable to ARTs and EMTs[24] encompassing matters such as governance, own funds, reserve requirements, complaints handling, conflicts of interest identification and mitigation, and recovery and redemption plans.

The ESMA has consulted the public on a wide range of technical standards and guidelines under its MiCA mandates.[25] These technical standards, which are too numerous to summarise here, cover topics such as: information to be included in the application for authorisation as a crypto-asset service provider (CASP); sustainability indicators for crypto-asset white papers; business continuity and record-keeping obligations for CASPs; disclosure of inside information; prevention of market abuse; conflicts of interest; and a host of investor protection topics, including complaints-handling and suitability assessments. Some of these standards were prepared in cooperation with the EBA, the

22 See Article 2(4) of Regulation (EU) 2023/1114.

23 See Article 3 of Regulation (EU) 2022/858.

24 See here.

25 The first consultation package was published on 12 July 2023 and the final report was released on 25 March 2024. The second consultation package was published on 5 October 2023 and the final report was released on 3 July 2024. The third consultation package was published on 25 March 2024. For more information, see here the main ESMA webpage dedicated to MiCA Implementing Measures.

European Insurance and Occupational Pensions Authority (EIOPA), and the European Central Bank (ECB). In addition, ESMA launched two standalone consultations concerning the guidelines on reverse solicitation and qualification of crypto-assets as financial instruments under MiCA.

In the course of 2024, the European Commission has adopted several Delegated Regulations supplementing MiCA.[26]

3. Adopted but not yet applicable new legislation

Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) was published in the Official Journal of the European Union on 27 December 2022 and entered into force on 16 January 2023. The Regulation shall apply from 17 January 2025.[27] For the time leading up to its application, the ESAs have published a set of technical standards and guidelines under DORA.

Specifically, the first batch of technical standards was published by the ESAs on 17 January 2024.[28]

This first batch included Regulatory Technical Standards (RTS) on ICT risk management framework (RMF), RTS on classification of major ICT-related incidents, RTS on third-party provider (TPP) policies, and Implementing Technical Standards (ITS) on the register of contractual arrangements of financial entities with TPPs (ROI). The RTS on RMF aimed at identifying key elements, complementary to those outlined in DORA, related to ICT risk management, to harmonise tools, methods, processes and policies across the financial sector. The RTS on classification of major incidents set out harmonised approaches, criteria and thresholds for the classification of major ICT-related incidents and significant cyber threats, together with indications for the relevance of the incident in host Member State and the information sharing with them. The RTS on TPP policies specified policies for the governance, risk management and internal control framework that financial entities should have when dealing with ICT TPPs. The ITS on ROI defined templates for the reporting by financial entities of their registers of information regarding

26 See here.

27 See Article 64 of Regulation (EU) 2022/2554.

28 See here, here and here.

contractual arrangements with ICT TPPs for the purpose of third-party risk management and supervision of competent authorities, and also for the ESAs to designate critical TPPs. At the time of writing, the European Commission review of the final draft of these technical standards, and subsequent adoption, is underway, with the first group of RTS having been adopted as early as last spring.[29]

On 17 July 2024 the ESAs also published a second batch of technical standards under DORA.[30]

This second package focused on RTS and ITS on ICT-related incident reporting, Guidelines on costs and losses from major ICT-related incidents, RTS on subcontracting, RTS on threat-led penetration testing (TLPT)[31], the RTS on oversight conduct, RTS on Joint Examination Teams, and Guidelines on oversight cooperation between ESAs and competent authorities. RTS and ITS on incident reporting specified the content, templates, process and format for reports to the competent authority on major ICT-related incidents and significant cyber threats, together with the time limits for reporting. The RTS on TLPT include the criteria, requirements, methodology and the type of supervisory or other relevant type of cooperation needed for financial entities when conducting TLPT.

The RTS on subcontracting define requirements and conditions in terms of risk assessment processes and implementation, monitoring and management of the contractual arrangement, for the use of subcontracted ICT services for critical functions.

The RTSs on oversight conduct and Joint Examination Teams further specify the oversight framework under DORA[32], introducing the content and format of the information to be submitted by the critical ICT third-party service providers (CTPPs) to the Lead Overseer, and the criteria for the composition of the Joint Examination Team (JET) that will assist the Lead Overseer

29 For instance, on 13 March 2024 the European Commission adopted the technical standards relating to ICT risk management framework, to ICT-third party providers contractual agreements' criteria, and to ICT-related incident classification. For more information, see here.

30 See here, here and here.

31 Threat-led penetration testing is a type of information security tests, performed to verify the security of the system tested by uncovering vulnerabilities and the necessary security solutions. The peculiarity of this type of testing lies in the fact that it is done from the side of the threat actor, effectively impersonating a potential attacker.

32 The oversight framework outlined in the Regulation requires, *inter alia*, that critical ICT third-party service providers (CTPPs) shall have a designated "Lead Overseer" from one of the ESAs.

in its oversight activities, as well as the information to be provided by an ICT third-party service provider in the voluntary application to be determined as critical.

The Guidelines on costs and losses from major ICT-related incidents set out instructions on how to provide the estimation of aggregated costs and losses caused by major ICT-related incidents, that a financial entity will have to report if requested by a competent authority. The Guidelines on oversight co-operation focus on oversight cooperation and information exchange between ESAs and competent authorities, providing protocols to ensure a consistent supervision approach.

At the time of writing, the next steps are in the hands of the European Commission, which has already been working on the review and adoption of this second batch of rules.

4. New legislation in progress

In the 'Digital Finance Strategy for the EU'[33] the European Commission announced its intention to promote data-driven finance by putting forward a legislative proposal for an open finance framework. The objective is to enable data sharing and third-party access for a wide range of financial products while ensuring data and consumer protection standards. This initiative also falls under the umbrella of the Commission's cross-sectoral 'European strategy for data,'[34] which aims to create a single market for data within the EU.

As was mentioned at the beginning of this chapter, on 28 June 2023 the European Commission published the Financial Data Access and Payments Package, which included the proposal for a framework for Financial Data Access (FiDA).[35] The proposal sets out rules on which certain categories of data can be accessed, shared, and used. It also establishes rights and obligations of data users, data holders and financial information service providers. The goal of this framework is to support financial innovation and competition by boosting the digital transformation of the EU financial sector it promotes the adoption of data-driven business models while establishing clear rights and obligations for accessing and sharing individual and business customer data across a wide range of financial products, beyond payment accounts. The Financial

33 COM(2020) 591 final.

34 COM(2020) 66 final.

35 COM(2023) 360 final.

Data Access and Payments Package also includes the proposal for a Directive on payment services and electronic money services in the internal market (PSD3)[36] and the proposal for a Regulation on payment services in the internal market (PSR).[37] The former aims to modernise the current payment services regime (PSD2), which has already improved the functioning of open banking. The latter would establish a regulation laying down uniform requirements on the provision of payment services and electronic money services. These measures aim to guarantee safe and secure electronic payments and transactions to customers, both domestically and cross-border, in euro and other currencies.

In the European Parliament the responsibility for both FiDA and the revision of EU rules on payment services lies within the remit of the Committee on Economic and Monetary Affairs (ECON). On 18 April 2024 the ECON adopted its report on a harmonised framework for access to financial data at the EU level.[38] The report was tabled for plenary on 30 April 2024[39] and is awaiting European Parliament's position in first reading. At the time of writing, discussions have started also within the preparatory bodies of the Council[40]. On 14 February 2024 the ECON adopted its report on payment services in the internal market and on 23 April 2024 the European Parliament adopted the ECON report in plenary, first reading.[41] At the time of writing, in the Council working parties are holding meetings on the file.[42]

A second legislative proposal currently being discussed concerns the possibility of issuing a digital euro, a form of central bank digital currency (CBDC). The ECB started exploring the concept by publishing a 'Report on a digital euro' in October 2020 (Report).[43] A digital euro would be an electronic form of central bank money, just like banknotes and coins, but digital. In the Report the ECB laid down the main benefits and challenges of issuing a digital euro. Among the benefits, a digital euro would represent an additional means of payment that is safe, free and easy to use; the digital euro would also support

36 COM(2023) 366 final.

37 COM(2023) 367 final.

38 See here.

39 See here.

40 See here.

41 See here.

42 See here.

43 See here.

the digitalisation and independence of the European economy and preserve the monetary anchor role of central bank money in a landscape in which cash is used less and less. As for the challenges, instead, a digital euro may pose risks to bank intermediation, it may have a (negative) impact on financial stability and potentially accelerate bank runs, without forgetting the high development and set-up costs. In addition, the Report developed an overview of the potential design features of a digital euro. *Inter alia*, the Report foresees a possible different level of privacy for offline transactions, which could be "fully private." The Report also describes some possible tools to avoid the use of a digital euro as a means of investment: (i) limiting the amount of digital euro each user can hold at any given time, (ii) introducing a waterfall mechanism or (iii) relying on tiered remuneration schemes to disincentivise digital euro holdings.[44]

As a second step, the Governing Council of the ECB officially launched the digital euro project in July 2021. The project consists of three phases: the Investigation phase (October 2021-October 2023), the Preparation phase (November 2023-October 2025), and the Implementation phase (starting November 2025). In the first phase, the ECB focused on defining the concept of a digital euro while exploring technical and design issues.[45] During the Preparation phase, the ECB is setting the groundwork to develop a digital euro prototype that can be tested. The two main priorities of this phase are to finalise the scheme rulebook and to select the service providers who will support the ECB in developing the product (ECB 2024). To this end, in January 2024, the ECB launched five calls for applications related to digital euro components and related service providers. Once the Preparation phase is over, the final phase will be dedicated to developing and rolling out digital euro use cases. Any decision to officially issue a digital euro will be made by the ECB Governing Council only after a legislative act is adopted.

In parallel to the work conducted by the Eurosystem, in June 2023, the European Commission published the so-called Digital Euro Package[46], composed of (i) a legislative proposal for the establishment of the digital euro and (ii) a legislative proposal on the provision of digital euro services by payment services providers incorporated in Member States the currency of

44 On tiered remuneration, see also Bindseil, Panetta and Terol (2021).

45 See the four 'Progress in the investigation phase of a digital euro' published by the ECB and available here.

46 Together with a legislative proposal on the legal tender of euro cash, the so-called digital euro package forms the previously mentioned Single Currency Package. See here for more details.

which is not the euro.[47] According to the proposals, the digital euro will be distributed by Payment Service Providers (PSPs) to all natural and legal persons in the euro area and, subject to certain conditions, to natural and legal persons outside the euro area. Its use will be free of charge for natural persons, while merchants may be charged a fee. To further boost its acceptance and, in turn, its adoption, the proposals recognise the digital euro as legal tender and provide for higher levels of privacy for offline transactions. Finally, the proposals empower the ECB to introduce tools to limit the use of the digital euro as a store of value.[48] At the time of writing, the two proposals are still in the early stage of the legislative process, without a formal position agreed upon by the European Parliament or the Council.

5. Other regulatory (legislative and non-legislative) initiatives

Several other pieces of EU legislation on digital[49] have an impact on finance (e.g. the Data Governance Act,[50] the Digital Markets Act,[51] the Digital Services Act[52] and the Data Act[53]), plus other EU legislation with a general reach (e.g. the GDPR[54]). The significance of this legislation can be appreciated by looking at the texts of the proposals and acts mentioned above, where it is often considered. More precisely, the Digital Markets Act seeks to ensure contestability and fairness in markets and for users of core platform services provided by undertakings designated as "gatekeepers", which can also be active in the field of financial services. The Digital Services Act provides for harmonised rules aimed at ensuring a safe, predictable, and trusted online environment that supports innovation, and protecting fundamental rights and consumers. Meanwhile, the Data Governance Act and the Data Act create frameworks for access, re-use and sharing of data that are, *inter alia*, crucial for open finance and data-driven

47 The package is complemented by an impact assessment (here) and two reports drafted by the Joint Research Centre (JRC): Petracco Giudici and Di Girolamo (2023) and Bellia and Calès (2023).

48 COM(2023) 369 final.

49 For more comprehensive information see here.

50 Regulation (EU) 2022/868.

51 Regulation (EU) 2022/1925.

52 Regulation (EU) 2022/2065.

53 Regulation (EU) 2023/2854.

54 Regulation (EU) 2016/679.

financial innovation. Therefore, these acts support compliance with existing EU rules on payment services. The GDPR remains central by safeguarding privacy, ensuring that financial entities process personal data appropriately. Together, these regulations aim to create a framework in which digital and financial ecosystems can integrate, while fostering innovation and promoting consumer protection and competition. Additional non-legislative initiatives are also meaningful (e.g. the digital finance platform and the data hub[55]).

A wider analysis of other pieces of EU legislation on digital would go far beyond the scope of this chapter. However, some last few introductory remarks must be made with reference to the AI Act, which fits in this context although, it will be more specifically covered in one of the following chapters (Almada, 2024).

On 12 July 2024 the AI Act was published in the Official Journal of the European Union, it entered into force on 1 August 2024 and (apart from some exceptions) it shall apply from 2 August 2026.[56] The AI Act has been described by the European Commission as the first-ever comprehensive legal framework on artificial intelligence worldwide and, as such, it has the ambition to advance the global leadership of the EU in this field.[57] It is tasked to address risks to the health, safety, and fundamental rights of citizens while supporting innovative and responsible AI in the EU, and its relevance is not negligible in the financial sector, with AI systems used for assessments of the creditworthiness of natural persons and those used for risk assessment and pricing in life and health insurance classified as of high risk under the AI Act.

6. Final remarks

Digital finance is a fast-evolving field. One of the main challenges from a regulatory perspective is to keep up with the pace of this evolution. In 2019-2024 the EU made considerable efforts to establish a comprehensive legal framework for digital finance and it achieved important results. Besides the adoption of new legislation 2024-2029 will be the years of further implementation and, maybe most importantly, of the first (full) application of many pieces of legislation which constitute such a legal framework. In the coming years, therefore, the EU will be a test bench for the rules adopted and the other initiatives taken so far.

---

55 See here.

56 See Article 113 of Regulation (EU) 2024/1689.

57 See here and Almada, 2024.

References

Almada M. (2024). The EU AI Act: logic, content and implications for finance, in this e-book. Section 2.6.

Bindseil U., Panetta F. and Terol I. (2021). Central Bank Digital Currency: functional scope, pricing and controls, *ECB Occasional Paper Series*, No 286 / December 2021.

Bellia M. and Calès L. (2023). Bank profitability and central bank digital currency, *JRC Working Papers in Economics and Finance*, 2023/6, European Commission, 2023, JRC133796.

EC (2020). A European strategy for data. COM(2020) 66 final. *European Commission*.

EC (2020). Digital Finance Strategy for the EU. COM(2020) 591 final. *European Commission*.

EC (2020). Retail Payments Strategy for the EU. COM(2020) 592 final. *European Commission*.

EC (2023). Proposal for a Regulation on a framework for Financial Data Access. COM(2023) 360 final. *European Commission*.

EC (2023). Proposal for a Directive on payment services and electronic money services in the Internal Market. COM(2023) 366 final. *European Commission*.

EC (2023). Proposal for a Regulation on payment services in the internal market. COM(2023) 367 final. *European Commission*.

EC (2023). Proposal for a Regulation on the establishment of the digital euro. COM(2023) 369 final. *European Commission*.

EC (2023). Impact assessment report. SWD(2023) 233 final. *European Commission*.

ECB (2024). First progress report on the digital euro preparation phase. *European Central Bank*. Available here.

Hallak I. (2024). Digital finance legislation: Overview and state of play, *Briefing EPRS | European Parliamentary Research Service*, PE 762.308 – May 2024.

Petracco Giudici M. and Di Girolamo F. (2023). Central bank digital currency and European banks' balance sheets, *Publications Office of the European Union*, Luxembourg, 2023, doi:10.2760/1356, JRC132239.

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).

Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

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.

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

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).

Section 2

Artificial Intelligence and Financial Services

1. The Potential of AI in Traditional Finance

Branka Hadji Misheva
Bern University of Applied Sciences

1. Introduction

Artificial Intelligence (AI) in finance is not just a technological development; it is a fundamental shift in how financial institutions operate, strategise and interact with customers. As defined in Chapter 2.6: EU AI Act, AI refers to computer systems designed to perform tasks that traditionally required human intelligence, such as recognising patterns, analysing complex datasets and making decisions based on data-driven insights. The technology dates back to the 1950s but it has only reached its current transformative power in the past decade. So, what has changed? Why is AI suddenly at the centre of disruption in the financial sector?

Three key technological advances have propelled AI into this pivotal role. First, data generation has reached unprecedented levels. In today's world, we create vast, diverse data sets at scales that were previously unimaginable. Reports suggest that global data creation is projected to grow to more than 180 zettabytes by next year (International Data Corporation (IDC), 2021). A single zettabyte equals a billion terabytes, and 180 of them shows the scale of the data that AI has to work with. This enormous quantity of data, which is increasing exponentially, represents a rich foundation for AI systems to analyse and learn from.

The second major development driving AI adoption is the increase in computing power and storage capacity. Here, Moore's Law, proposed by Intel co-founder Gordon E. Moore in the 1970s, offers insight (Theis and Wong, 2017). Moore famously observed that the number of transistors that can fit on a microchip doubles approximately every two years. This exponential increase has not only made computers faster and smaller but also significantly cheaper.

Last, analytics, the third driver, has seen significant progress. Although foundational AI concepts, such as Neural Networks (NN), date back decades, the past twenty years have introduced a suite of new advanced tools and techniques. Deep Learning (DL), a subset of Machine Learning (ML), represents a pivotal shift. While Neural Networks were once theoretical constructs based on simplified models of how biological neurons interact, they have become highly sophisticated with today's data and processing power. Deep learning networks now handle complex tasks that are far beyond the capabilities of rule-based systems, allowing AI to achieve high levels of accuracy. In addition, advances in generative AI (GenAI) have a transformative potential in various sectors. These systems utilise AI to identify and replicate underlying patterns and structures in its training data, enabling them to create *new* data with similar features (OpenAI, 2023). A major driving force behind the recent success of GenAI is the development of *transformer* technology, a DL method adept at managing complex long-distance data relationships. Large Language Models (LLMs) exemplify this advance. They attract widespread interest in their capacity to generate coherent and contextually relevant content (Nie et al. 2024).

The synergy between increased computational power, vast datasets and innovative neural architectures allows AI to perform with levels of sophistication once thought impossible and create systems capable of performing tasks that mimic human-like reasoning and creativity. This emerging ecosystem is not only a key milestone in the evolution of AI but also a crucial step in the widespread adoption of this technology in research and commercial applications.

2. Use cases of AI in Traditional Finance

In this context, the finance sector, given its unique characteristics, is perfectly suited to integrate AI. Financial institutions operate with vast amounts of historical data, which are often highly structured and accurate. In addition, finance is fundamentally quantitative, with tasks grounded in understanding and managing risks, pricing assets, optimising portfolios, and forecasting financial market performance, all of which require quantitative techniques. These defining properties of the finance industry align almost perfectly with the conditions needed for full utilisation of the advantages of AI. Therefore, we can easily argue that there are few industries that are as well-suited to AI deployment as the finance sector.

Consequently, AI applications in finance span a wide range of areas, from risk management to compliance, asset management, and customer service. Recent surveys highlight the transformative impact of these applications (OECD, 2023a and OECD, 2023b). In risk management, for instance, AI models allow more accurate and timely assessment of creditworthiness and liquidity needs. This shift is particularly visible in loan origination. Traditional methods of assessing borrower risk are being supplemented or even replaced by Machine Learning models that can precisely process vast datasets at high speed. This leads to more accurate credit scoring, which in turn can promote financial inclusion by allowing individuals with limited financial histories to access loans. In addition, better risk assessments can yield more accurate liquidity pricing, making the overall system more efficient. AI also plays a critical role in compliance, particularly in detecting and preventing fraudulent activities. By analysing transaction patterns, ML algorithms can flag irregularities and suspicious behaviour for further review. This is especially important in Anti-Money Laundering (AML) and know-your-customer (KYC) processes, in which AI models can sift through enormous amounts of data to verify identities and spot potentially risky clients. The KYC process is multifaceted and involves data collection, identity verification, risk assessment, due diligence, and ongoing monitoring. In each stage, AI can streamline processes and improve accuracy. Optical Character Recognition (OCR) technology, for example, allows AI to extract relevant information from scanned documents and images, automating the data entry process and reducing human error. Similarly, ML models can verify document authenticity by detecting watermarks, recognising signatures and matching templates, thus further enhancing security and reliability.

The finance sector has also seen the impact of AI in asset management, in which it supports portfolio optimisation, market trend forecasting and personalised investment advice. Asset managers can use AI-driven models to analyse a wealth of data including historical prices, economic indicators, news sentiment and more, leading to better informed and precise decisions. The ability of AI to manage large data sets quickly and accurately enables financial professionals to adjust their strategies dynamically and respond to real-time market shifts, thus enhancing both the effectiveness and efficiency of asset management.

AI also enhances the banking experience by automating customer service and transactions. For example, AI-powered chatbots can respond to routine customer inquiries, freeing up human agents to handle more complex cases. These chatbots can process transactions, provide account information and even offer basic financial advice, improving customer satisfaction while reducing operational costs.

In the remainder of this chapter, we delve further into some of these specific applications of AI that are reshaping core functions in finance.

3. AI in Credit Risk Management

The literature on lending covers a wide range of topics, with researchers focusing on improving credit scoring models, understanding impacts on financial inclusion, and addressing consumer protection and regulatory concerns. In the area of credit scoring, a review of the literature (Byanjankar et al., 2015; Serrano-Cinca et al., 2015 and 2016; Emekter et al., 2015; Malekipirbazari et al, 2015; Guo et al.; 2016; Zhang et al.; 2017; Zhou et al.; 2019, Turiel and Aste, 2019; Giudici et al. 2019; Teply et al., 2020; Giudici et al., 2020; Lyocsa et al., 2022; Kriebel and Stitz, 2022) reveals two main areas in which credit risk estimation has changed due to technological developments. First, the literature offers evidence in favour of the hypothesis that advanced ML models can enhance the precision of credit scoring. Unlike traditional rule-based approaches that rely on static criteria (Serrano-Cinca et al., 2015; Emekter et al., 2015; Guo et al., 2016; Zhang et al., 2017; Lyócsa et al., 2020; Teply and Polena, 2020), ML models dynamically learn from complex large-scale datasets and capture non-linear relationships in the behaviour of borrowers (Byanjankar et al., 2015; Turiel and Aste, 2019). This shift to adaptive models allows more accurate evaluation of credit risk, as ML algorithms like neural networks and ensemble methods improve predictive power by integrating diverse data inputs and learning more complex relationships. For example, findings by Moscato et al. (2021) suggest that in different modelling conditions (different handling of imbalanced datasets) a neural network model consistently has higher accuracy. In the same context, a study by Plawiak et al. (2020) proposes a new deep genetic hierarchical network of learners to predict credit scoring and finds that the proposed model (comprising different types of learners including Support Vector Machines (SVMs), k-Nearest Neighbours (k-NNs) and Artificial Neural Networks (ANNs)) significantly outperforms simpler models. In addition, the literature finds that model stacking, i.e. using combinations of different algorithms like regression and neural networks, demonstrates an ability to improve the robustness of scoring and adaptability to new patterns of financial behaviour, and so reduces the likelihood of default (Tircovnicu and Hațegan, 2023). These papers underscore the potential of more advanced ML models to transform credit risk assessment and constitute more accurate and adaptable tools compared to traditional methods.

In addition to the development of sophisticated models, another significant shift in credit risk estimation is the expansion of the scope of data, which enables a more comprehensive and nuanced evaluation of the creditworthiness of a borrower. Traditionally, credit scores were based on financial data such as income, debt, and payment histories. However, recent AI-driven approaches incorporate non-traditional data sources such as digital footprint data, which include online behaviour, mobile device metadata, social media activity, online browsing patterns and more. These alternative data types are particularly valuable for individuals with limited credit histories, as they provide a more holistic view of their financial habits. A key study in this context is by Berg T. et al. (2019). They investigate the predictive power of digital footprints, trails of information left by individuals in online interactions in assessing consumer credit risk. By analysing over 250,000 cases, the study reveals that even simple readily accessible digital footprint variables can provide predictive accuracy comparable to traditional credit bureau scores. Specifically, the study identifies several specific digital footprint properties that contribute to credit risk discrimination, such as a device having been used to access a website (e.g., whether it is a mobile or desktop device), the email domain (e.g., professional vs. generic domains) and the time of the visit (e.g., during or outside business hours). These variables are found to have substantial predictive value of the likelihood of default. Moreover, combining such digital footprint characteristics with traditional credit bureau data significantly enhances the precision of risk estimation, ultimately aiding financial inclusion and decision-making. Berg T. et al. (2019) further argue that digital footprints have significant discriminatory power, especially for unscorable customers, i.e., those without sufficient credit history to be evaluated using traditional methods. This aspect of digital footprints supports financial inclusion by potentially extending credit access to the currently underserved population, such as the estimated 1.4 billion adults lacking access to formal financial services (World Bank Global Findex Database). Subsequent research has validated these findings, demonstrating that integrating digital footprint data with conventional metrics improves both the predictive accuracy and inclusivity of credit scoring (Berg et al., 2019 and Uzougbo et al., 2023).

4. AI in Sustainable Finance

Finance also stands to benefit from applications of AI in environmental, social and governance (ESG) evaluation. ESG data are increasingly relevant in investment decision-making, yet standard ESG ratings by major agencies often poorly correlate, which complicates comparisons. A study by Berg F. et al. (2022) examines differences in ESG ratings by analysing data from six leading ESG rating agencies, including KLD, Sustainalytics and MSCI. They categorise these divergences as measurement, scope, or weight, and attribute 56% of the variation to measurement, 38% to scope and 6% to weight. They identify a "rater effect," in which an agency's overall impression of a firm influences assessments of specific categories. The findings indicate a need for greater scrutiny of the methodologies used to generate ESG ratings. Table 1 comes from this study. Berg F. et al. (2022) report the pairwise Pearson correlations between aggregate ESG ratings and their environmental (E), social (S) and governance (G) dimensions.

Table I. Correlations between ESG ratings (Berg et al., 2022)

	SA MO	SA SP	SA RE	SA MS	MO SP	MO RE	MO MS	SP RE	SP MS	RE MS	Average
ESG	0.77	0.65	0.53	0.53	0.62	0.6	0.49	0.42	0.4	0.37	0.54
E	0.7	0.66	0.59	0.33	0.69	0.59	0.35	0.61	0.26	0.19	0.5
S	0.67	0.57	0.52	0.29	0.62	0.58	0.27	0.55	0.27	0.28	0.46
G	0.55	0.48	0.36	0.34	0.7	0.7	0.43	0.68	0.38	0.34	0.5

Note: SA, SP, MO, RE, KL, and MS stand for Sustainalytics, S&P Global, Moody's ESG, Refinitiv, KLD and MSCI respectively.

Table I reveals that ESG ratings by different agencies exhibit only moderate agreement, with an average correlation of 0.54, indicating significant variability across raters. The environment dimension shows the highest level of consistency (average correlation 0.53), while the governance dimension shows the least (average correlation 0.30). The substantial variation, particularly in the social and governance dimensions, underscores the methodological differences between rating agencies, which in turn lead to complexity and inconsistency in ESG evaluations among different providers.

In this context, AI systems can facilitate the convergence of ESG measures by streamlining the extraction, analysis, and benchmarking of ESG information from diverse unstructured data sources. Specifically, natural language processing (NLP) techniques can be used to extract ESG-related information from corporate reports and translate qualitative disclosures into quantifiable metrics. In addition, ML algorithms can analyse sentiment and cluster companies based on performance, thus enhancing predictive models and enabling consistent evaluation. Studies have shown that these AI-driven methodologies can mitigate discrepancies among ESG ratings and improve overall measurement reliability (Sklavos et al., 2024). Moreover, a key challenge in ESG performance assessment is effective benchmarking and providing actionable recommendations for improvement. Companies can significantly benefit from understanding how they compare with their peers and obtaining guidance on making meaningful progress. Unsupervised learning techniques, like clustering, are instrumental in this context. They can categorise firms into clusters based on similar characteristics of all observable inputs, and so help identify performance gaps and offer tailored recommendations for advances. This approach enhances decision-making and strategic planning in ESG management by leveraging data-driven insights for improvement (Sklavos et al., 2024).

5. AI in asset management

Stock price prediction is one of the most prominent applications of ML in finance. The subject has been extensively researched, as is reflected in numerous empirical asset pricing studies, such as those by Gu et al. (2020), Cong et al. (2021) and Chen et al. (2023). In addition to these, several other significant contributions have shaped this area. For instance, Zhang et al. (2017) explore financial market forecasting using a Recurrent Neural Network (RNN) model. Specifically, they introduce an innovative State Frequency Memory (SFM) recurrent network that enhances predictive accuracy by distinguishing between high-frequency patterns for precise short-term forecasts and low-frequency patterns for more reliable long-term projections focused on returns. Similarly, Chen et al. (2018) employ a Long Short-Term Memory (LSTM) model to identify time-based patterns in stock data and integrate a graph-based neural network to consider connections between companies. They construct a graph of companies linked by real market investment relationships and apply node embedding techniques to generate comprehensive representations for each firm. To make use of this relational data, they test two strategies: (i) a pipeline model, and (ii) a joint model using graph convolutional neural networks. Their experiments using stock market data from mainland China reveal that these company representations successfully capture intercompany relationships, resulting in more accurate stock price predictions. More recently, with the growth in popularity of generative pretrained transformers, Yoo et al. (2021) introduced a transformer-based model to predict stock prices. They introduce an advanced Deep Neural Network (Deep NN) framework designed to improve prediction accuracy by dynamically integrating a wide range of data. The model leverages both fundamental trading data and technical indicators as multi-dimensional inputs, while also incorporating local and global market information. Key features of this framework include dynamic weighting of stock features to assess their impacts, the use of Fourier transforms to capture long-term global trends and an attention-enhanced RNN model to analyse historical price data. Tests on stocks in the Chinese CSI 300 index demonstrate that this approach outperforms traditional models and other deep learning techniques and so constitutes a more accurate method for forecasting stock prices.

Beyond price prediction, some researchers have extended their focus to constructing investment strategies directly informed by ML techniques. Snow (2020a and b) explores diverse methods for developing algorithmic trading strategies. Zhang et al. (2021) employ deep learning, including LSTM models, to create portfolios optimised for the Sharpe ratio. In addition, Zhao et al. (2022) leverage LSTM-based approaches to implement statistical arbitrage strategies.

Drawing on evidence from the industry, the asset management sector has increasingly embraced algorithmic trading, which now dominates the U.S. equity market. While algorithmic trades accounted for only 15% of market volume in 2004, they now handle between 70% and 85% of all U.S. trades. In this context, as mentioned previously, generative AI, especially LLMs, represents the latest advance. These models enable NLP at a scale that makes applications like automated reporting, sentiment analysis and customer interaction feasible. LLMs such as ChatGPT are beginning to provide insights for stock forecasting, regulatory compliance and personalised wealth management, helping to redefine what AI can accomplish in finance.

6. Conclusion

Of course, integrating AI in finance presents numerous challenges that require careful navigation. One of the most pressing concerns is data privacy and security. Financial institutions handle vast amounts of sensitive customer information, making data protection a top priority. Compliance with stringent regulations, such as the General Data Protection Regulation (GDPR) in Europe, is mandatory. The GDPR imposes strict rules on how personal data are collected, processed and stored, with severe penalties for non-compliance. In addition, emerging regulations like the ePrivacy Regulation and national laws such as Germany's Federal Data Protection Act (BDSG) emphasise the importance of strong data protection measures. Related to this is the need for robust cybersecurity strategies. Protecting data from breaches and cyber threats is crucial to ensure compliance with privacy laws and maintain customer trust. Another major concern is ethical and fair use of AI. Biases in AI models can lead to discriminatory practices, especially in areas such as credit scoring and loan approving. To address this, financial institutions must continually monitor their AI systems for potential biases, perform regular audits, and update algorithms to promote fairness and equity.

Model interpretability remains a significant challenge too. Many AI models, especially those based on DL, function as 'black boxes' with opaque decision-making processes. In finance, transparency is not just beneficial but essential for regulatory compliance and for maintaining trust by customers. Financial institutions must develop tools and processes that make AI-driven decisions understandable for both regulators and clients. The GDPR, specifically Article 22, highlights the right of individuals to receive "meaningful information about the logic involved" in automated decisions, which reinforces the need for transparent and explainable AI systems.

Adding to this regulatory landscape is the EU AI Act, which has significant implications for financial intermediaries, as discussed in Chapter 2.6: EU AI Act. This legislation seeks to create a structured framework for AI systems and categorise them based on risk. Some financial applications of AI are designated as high-risk, meaning they must meet strict requirements related to risk management, transparency and regular audits. The Act aims to ensure that AI in finance is safe and reliable, and respects fundamental human rights.

In conclusion, AI offers enormous potential for traditional finance by creating opportunities for efficiency, innovation, and inclusivity. However, realising this potential requires thoughtful policies, ethical practices and an unwavering commitment to security and transparency. By addressing these challenges, the finance sector can unlock the full potential of AI and pave the way for a more advanced, accessible, and resilient financial future.

References

Berg F., Kölbel J. F., and Rigobon R. (2022). Aggregate confusion: The divergence of ESG ratings. *Review of Finance, 26*(6), 1315-1344. Available here.

Berg T., Burg V., Gombović A., and Puri, M. (2019). On the rise of FinTechs: Credit scoring using digital footprints. *Irish Finance Working Paper Series Research Paper No. 18-12.*

Byanjankar A., Heikkilä M., and Mezei, J. (2015, December). Predicting credit risk in peer-to-peer lending: A neural network approach. In *2015 IEEE Symposium Series on Computational Intelligence* (pp. 8-10). Cape Town, South Africa. Available here.

Chen L., Pelger M., and Zhu, J. (2023). Deep learning in asset pricing. *Management Science*.

Chen Y., Wei Z., and Huang X. (2018). Incorporating corporation relationship via graph convolutional neural networks for stock price prediction. In *Proceedings of the 27th ACM International Conference on Information and Knowledge Management* (pp. 1655-1658).

Cong L. W., Tang K., Wang J., and Zhang, Y. (2021). Deep sequence modeling: Development and applications in asset pricing. *Journal of Financial Data Science, 3*(1), 28-42.

Emekter T., and Jirasakuldech L. (2015). Evaluating credit risk and loan performance in online peer-to-peer (P2P) lending. *Applied Economics, 47*(54-70).

Giudici P., Hadji Misheva B., and Spelta A. (2020). Network scoring models to improve credit risk management in P2P lending platforms. *Frontiers in Artificial Intelligence, 2*, 3-9.

Giudici P., et al. (2019). Credit risk modeling in the era of big data. *Journal of Big Data, 6*(1), 47.

Gu S., Kelly B., and Xiu D. (2020). Empirical asset pricing via machine learning. *Review of Financial Studies, 33*(5), 2223-2273.

Guo Y., et al. (2016). Instance-based credit risk assessment for investment decisions in P2P lending. *European Journal of Operational Research*.

International Data Corporation (IDC). (2021). *Global DataSphere Forecast, 2021-2025.*

Kriebel J., and Stitz L. (2022). Credit default prediction from user-generated text in peer-to-peer lending using deep learning. *European Journal of Operational Research, 302*(1), 309-323.

Li J., Zhang M., Li N., Weyns D., Jin Z., and Tei, K. (2023). Generative AI for self-adaptive systems: State of the art and research roadmap. *ACM Transactions on Autonomous and Adaptive Systems, 19*(3), Article 13, 1-60. Available here.

Lyócsa Š., Vašaničová P., Hadji Misheva B., and Vateha, M. D. (2022). Default or profit scoring credit systems? Evidence from European and US peer-to-peer lending markets. *Financial Innovation, 8*, Article 32.

Lyócsa Š., et al. (2020). Machine learning techniques in credit risk modeling: A comprehensive overview. *Journal of Credit Risk, 16*(4), 1-28.

Malekipirbazari M., et al. (2015). Risk assessment in social lending via random forests. *Expert Systems with Applications, 42*, 4621-4631.

Moscato V., Picariello A., and Sperlí G. (2021). A benchmark of machine learning approaches for credit score prediction. *Expert Systems with Applications, 165*, 113986.

Nie Y., Kong Y., Dong X., Mulvey J. M., Poor H. V., Wen Q., and Zohren, S. (2024). A survey of large language models for financial applications: Progress, prospects and challenges. *arXiv*. Available here.

OECD. (2023a). *Artificial Intelligence, Machine Learning and Big Data in Finance.* OECD Publishing. Available here.

OECD. (2023b). *Generative Artificial Intelligence in Finance.* OECD Publishing. Available here.

OpenAI. (2023). *Generative AI: Transforming industries with transformer models*. OpenAI Publications.

Plawiak P., et al. (2020). DGHNL: A new deep genetic hierarchical network of learners for prediction of credit scoring. *Information Sciences, 516*, 401-418.

Serrano-Cinca C., and Gutiérrez-Nieto B. (2016). The use of profit scoring as an alternative to credit scoring systems in peer-to-peer (P2P) lending. *Decision Support Systems, 89*(2), 113-122. Available here.

Serrano-Cinca C., Gutierrez-Nieto B., and Lopez-Palacios, L. (2015). Determinants of default in P2P lending. *PLOS ONE, 10*, e0139427. Available here.

Sklavos, G., Theodossiou, G., Papanikolaou, Z., Karelakis, C. & Ragazou, K. (2024). Environmental, social, and governance-based artificial intelligence governance: Digitalizing firms' leadership and human resources management. *Sustainability, 16*(16), 7154. Available here.

Snow D. (2020a). Machine learning in asset management—Part 1: Portfolio construction—Trading strategies. *Journal of Financial Data Science, 2*(1), 10-23.

Snow D. (2020b). Machine learning in asset management—Part 2: Portfolio construction—Weight optimization. *Journal of Financial Data Science, 2*(2), 17-24.

Teply P., and Polena, M. (2020). Best classification algorithms in peer-to-peer lending. *North American Journal of Economics and Finance, 51*, Article 100904.

Theis T., and Wong H.-S. P. (2017). The end of Moore's law: A new beginning. *Nature Electronics, 1*(1), 204-210.

Tircovnicu G. I., and Hategan, C. D. (2023). Integration of artificial intelligence in the risk management process: An analysis of opportunities and challenges. *Journal of Financial Studies, 8*(15), 198-214. Available here.

Turiel J. D., and Aste T. (2019). P2P loan acceptance and default prediction with artificial intelligence. *arXiv preprint arXiv:1907.01800*.

Uzougbo N. S., Akagha O. V., Coker J. O., Bakare S. S., and Ijiga, A. C. (2023). Effective strategies for resolving labour disputes in the corporate sector: Lessons from Nigeria and the United States.

Yoo J., Soun Y., Park Y. C., and Kang, U. (2021). Accurate multivariate stock movement prediction via data-axis transformer with multi-level contexts. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery and Data Mining* (pp. 2037-2045).

Zhang Y., Li H., Hai M., Li J., and Li, A. (2017). Determinants of loan funded success in online P2P lending. *Procedia Computer Science, 122*, 896-901.

Zhang Z., Zohren S., and Roberts S. (2021). Deep learning for portfolio optimization. *arXiv*. Available here.

Zhao J., Xu Y., and Ossowski S. (2022). Deep learning meets statistical arbitrage: An application of long short-term memory networks to algorithmic trading. *Journal of Financial Data Science, 4*(4), 133-150. Available here.

2. Artificial Intelligence in the Financial Sector: Risks to Financial Stability

Claudia Guagliano

European Securities and Markets Authority (ESMA)

Valentina Mejdahl

European Securities and Markets Authority (ESMA)

1. Introduction

Artificial intelligence (AI) is a prominent and rapidly evolving technology that is increasingly driving innovation in the financial industry. AI presents immense opportunities in the banking, insurance and securities sectors given the heavy reliance of the finance industry on data and advanced analytics. While the use of AI in the financial sector is not new and has long existed in the form of statistical and econometric modelling ("early AI" – Liang, 2024), the recent surge in adoption of AI is largely driven by breakthroughs in generative AI, the unprecedented availability of data – particularly unstructured data – and increased computing power.

Adoption of generative AI in the financial sector is projected to grow significantly. According to IMF estimates, spending on software, hardware and services for AI systems in the financial sector is expected to more than double and reach USD 97 billion by 2027, with an annual growth rate of 29% (IMF, 2023). In addition, a recent McKinsey report estimates that generative AI could increase productivity in the banking industry by 2.8% to 4.7% of its annual revenue, translating into an additional USD 200 billion to 340 billion (McKinsey & Company, 2023).

There are various benefits that AI can offer financial consumers, the finance industry and its regulators. These include increased operational efficiencies, costs reductions, optimised customer outcomes, personalised products and services, improved risk management, enhanced decision-making and better regulatory oversight.

However, AI adoption also amplifies existing risks and introduces new ones. Current discussion on AI risks ranges from "existential concerns" to scepticism about AI's potential being overstated by tech firms (The Economist, 2024d). This article provides a brief overview of analyses related to a specific category of AI risks: risks to financial stability.[1]

2. Challenges in assessing the impact of AI and key risks to financial stability

Identifying and assessing how AI can adversely impact financial stability is challenging for several reasons. First, there are no comprehensive data on the extent and nature of AI use by financial institutions. While international and national regulators have intensified their efforts to monitor and assess AI adoption,[2] the overall picture remains approximate. In the absence of a clear requirement for financial institutions to report their use of AI and with AI service providers mostly outside the financial supervisory perimeter, data are likely to continue to be sparse. Second, the rapid advances in AI technology and its application to various tasks in financial institutions make such assessments a constantly moving target. Accordingly, discussion on the risks and systemic consequences of AI is largely based on conjecture.

1 Financial stability is the capacity of the global financial system to withstand shocks and contain the risk of disruptions in the financial intermediation process and other financial system functions that are severe enough to adversely impact the real economy (FSB, 2021).

2 For example, the European Commission targeted consultation on AI in the financial sector (EC, 2024); the OECD survey on regulatory approaches to AI in finance (OECD, 2024); ESMA surveys in 2022 and 2023 of credit rating agencies, central counterparties, trade and securitisation repositories, and data reporting service providers (ESMA,2023a; ESMA, 2024a).

A recent OECD report based on responses from 48 jurisdictions indicates that the majority of the survey respondents have not yet observed major risks to financial stability arising from the use of AI in finance. However, nearly all the respondents stated that such risks are expected to emerge in the future, although they have not been clearly defined at this stage. As a result, jurisdictions have called for further assessments to determine whether these risks are already significant enough to threaten financial stability (OECD, 2024).

In July 2023 SEC Chair Gary Gensler mentioned that many of the challenges to financial stability that AI may pose in the future will require new thinking on system-wide and macro-prudential policy interventions (SEC, 2023). In 2021 the IMF warned that AI could introduce new sources of systemic risk and transmission channels (IMF, 2021). In 2023 it further stated that generative AI, with its new complex risks, could have broad systemic implications for the financial sector (Shabsigh and Boukherouaa, 2023).

In Europe, ECB market intelligence suggests that, while European banks are relying on traditional AI, the use of generative AI is still in the early stages of deployment (Leitner et al., 2024). In 2023, ESMA noted that while AI is increasingly used to support and optimise certain activities in the securities sector, it has not yet caused a disruptive overhaul of business processes (ESMA, 2023a). In 2024 ESMA reported that most credit rating agencies, central counterparties, trade and securitisation repositories, and data reporting service providers are either already using generative AI tools or planning to do so, although deployment remains in the early or planning stages for most (ESMA, 2024a).

Some focused analyses (Danielsson and Uthemann, 2024) suggest that AI can undermine financial stability due to malicious use, misinformation, misalignment and the structure of the AI analytics market. In addition, AI introduces new risks when its known vulnerabilities interact with established drivers of financial instability.

In this context, significant policy and analytical efforts are focusing on understanding and identifying financial stability risks, including their sources, transmission channels and potential mitigation strategies. Drawing on the most prominent analyses of stability risks to date, we identify and provide a brief overview of the following areas of risks to financial stability:

- Concentration of AI models in only a few service providers.
- Interconnectedness, herding and market correlations.
- Operational risks and cybersecurity.

- Model risk and algorithmic biases.
- Hype around AI companies.
- Risks amplified by social media.

2.1 Concentration risk

Concentration risk in AI adoption in the financial sector arises primarily from the increasing reliance of financial institutions on a limited number of third-party providers of AI- related products and services. The effects of AI on individual financial institutions can scale up to a systemic level due to both widespread technology integration and dependence on a limited number of suppliers. If supplier concentration and technological penetration are high, financial stability could be at risk. The transition from micro to macro could be gradual but not necessarily linear (Leitner et. al., 2024).

One of the major sources of concentration risk, which is particularly relevant to generative AI, is the dominance of a few key AI suppliers, often BigTechs, in critical aspects of the AI supply chain, including hardware, software, cloud services and data aggregation. The markets for hardware, such as the accelerated computing chips necessary for training and running AI models and cloud services are highly concentrated, with a few entities controlling most of the market. Moreover, few firms can afford the costs of developing AI tools inhouse, especially for LLM-based generative AI models, which leaves them with no choice but to rely on third-party providers, which are often the same for many financial institutions.

This concentration creates dependencies among financial institutions that rely on the same or similar AI models and services. It increases the vulnerability of the financial system to single points of failure in which disruptions at a single supplier could spread across the entire system. Furthermore, vertical integration in the AI supply chain occurring when certain entities, such as BigTechs, are providers of various combinations of hardware, software, cloud services and models exacerbates this risk.

An additional risk may arise from the recent trend of generative AI startups emerging. These companies focus on developing smaller specialised AI models in areas like text, image and audio generation, and also chatbots. Without proper safeguards, the use of these quick-to-train and potentially less monitored models could pose risks if they are adopted on a large scale by financial institutions (ESMA, 2023b).

In addition to technological dependencies, market concentration can arise from economic factors. Only large financial institutions can afford the substantial investments needed to integrate AI, thanks to their established data infrastructure and resources. Moreover, large firms, and BigTechs in particular, have a competitive advantage in attracting scarce AI talent, making it difficult for smaller firms to compete. For example, one popular destination for AI workers is Nvidia, a chipmaker the graphics-processing units of which are powering the AI boom and the ambitions of which extend beyond hardware to software and applications (The Economist, 2024c). Smaller firms lacking the ability to keep pace with AI developments may fall behind, further reinforcing the dominance of larger players. This 'winner-takes-all' dynamic concentrates market power among a few major players, particularly BigTechs, the role of which as essential tech and cloud providers may create too-big-to-fail risks and limit competition.

The concentration risk in AI services may soon resemble the concentration and interconnectedness risks seen in cloud service provision and the broader spectrum of outsourced services in finance, including data provision. In these areas, many firms and intermediaries become reliant on a small number of dominant outsourcers or third-party providers. This concern was highlighted in the European Supervisory Authorities' Advice on Digital Finance (JC ESAs, 2022). The Digital Operational Resilience Act (DORA) [Regulation (EU) 2022/2554] is a key regulation aimed at addressing information and communication technology (ICT) risks in the financial services value chain.

2.2 Interconnectedness, market correlations and herding

Another risk related to concentration in the AI supply chain is that due to the widespread use of the same training data and common pre-trained models market participants are increasingly relying on similar AI models to interpret financial market dynamics. This amplifies interconnections between institutions and introduces a market correlation risk (IMF, 2024).

When AI models produce similar outputs based on identical data, the potential for correlated decisions across the financial system increases. This can result in herding behaviour, in which investors and institutions collectively follow trends driven by AI predictions rather than underlying economic fundamentals. This can distort asset prices and increase volatility, particularly if retail investors guided by similar AI tools simultaneously influence trading volumes and market sentiment.

In 2017 the Financial Stability Board (FSB) noted that correlated risks resulting from many financial market participants using similar machine learning models might threaten financial stability (FSB, 2017). SEC Chair Gary Gensler highlighted this concern in 2023, noting that "AI may heighten financial fragility as it could promote herding, with individual actors making similar decisions because they are getting the same signal from a base model or data aggregator" (SEC, 2023). Similarly, the IMF outlined that the widespread use of AI could "drive greater homogeneity in risk assessments and credit decisions in the financial sector, as well as out-of-sample risk that, coupled with rising interconnectedness, could create the conditions for a buildup of systemic risks" (Shabsign and Boukherouaa, 2023).

Identical signals from AI models that institutions and investors receive can lead to uniform behaviour inflating asset bubbles during periods of optimism and exacerbating market vulnerabilities during downturns. This creates volatility and liquidity risks that impact financial stability. If models inform trading strategies that are executed automatically, incidents like flash crashes may become more likely. Depending on the use case and the extent of reliance on AI models, this data-related risk of correlations can manifest itself in different ways. Shock amplification, procyclicality and overreliance on AI systems are often mentioned when analysing risks resulting from market correlations (OECD, 2024).

The risk is likely to be even more pronounced with generative AI. As the volume of generative AI outputs on the internet grows and is recycled into future training data, model correlations intensify. If financial institutions integrate these AI tools in critical business processes, such as developing investment strategies or managing risk, the vulnerabilities related to these correlations increase.

2.3 Operational risks and cybersecurity

Operational risks are inherent in any digitalised process and may be amplified by the use of AI technology. AI can escalate the sophistication, impact and frequency of cyber-attacks, which may significantly disrupt markets, possibly with systemic consequences. The ability of financial institutions and market infrastructure to withstand and recover from AI-induced disruptions (e.g. system outages, technological failures) is critical in maintaining stability. A lack of operational resilience could result in prolonged downtimes, disrupt market liquidity and weaken consumer and investor confidence.

This risk can also manifest itself as financial institutions increasingly apply AI in decision-making processes, potentially leading to an overreliance on AI and automation in critical functions, which could make the financial system more vulnerable to operational flaws, failures and cyberattacks.

Generative AI has brought challenges to operational resilience to a new level. The possibility of easily producing realistic deepfakes in videos, audio and images could cause significant harm to financial institutions with a potentially systemic impact.[3] Generative AI tools enable adversaries to become more proficient. In addition, generative AI models are susceptible to data poisoning and input attacks (IMF, 2021).

2.4 Model risk and algorithmic biases

Model risk refers to the potential consequences of poor quality training data, algorithmic biases, design flaws and improper use of models. While this risk applies to models in general, it can be amplified by AI due to its increasing complexity and wide-ranging applications. As models are increasingly relied on to make critical decisions in financial institutions, such as in trading, risk management and customer profiling, this risk can become systemic.

Excessively complex and increasingly autonomous AI models present significant challenges when it comes to assessing the quality of training data and evaluating, validating and correcting outputs. Financial institutions are required to be able to explain their decisions and actions internally and to their clients and supervisors, but explainability is an issue with AI models. This lack of understanding and transparency on how models make their decisions creates challenges in monitoring and correcting their outputs, especially in complex systems and in times of crisis. The FSB has highlighted concerns that the complexity and opacity of these models make it difficult to predict their performance (Liang, 2024).

Explainability issues are exacerbated by generative AI. The diversity of input data from online sources and the complex architecture of models with multiple neural network layers make it even more difficult to explain output and control of so-called 'hallucinations.' Large language models, for example, continue to hallucinate even with the best algorithmic and architectural stabilisers available (GPT-4 hallucinates in 3% of its summaries, Claude 2 in 8.5% and Gemini Pro in 4.8%) (The Economist, 2024a). Hallucinations in algorithms generating news, for instance, can spread misinformation that may destabilise the financial system if it escalates to crises or triggers bank runs.

3 An example of such a high-impact attack occurred when a finance employee at a multinational firm was deceived into transferring USD 25 million to fraudsters who used deepfake technology to impersonate the company's chief financial officer during a video conference (Chen and Magramo, 2023).

Model biases are also an issue. Algorithmic biases can emerge from the design of algorithms or from the way data are collected and processed. Biased AI models produce systematically unfair or unequal outcomes due to biased assumptions and data used during development. If biases are present in the training data (embedded biases) they will lead to biases in algorithms. In financial services such as lending and insurance underwriting in which clients' personal data are used, embedded and algorithmic biases can lead to discriminatory outcomes. Moreover, an AI model trained on data with embedded biases will perpetuate similar biases. Biases can also stem from the design of algorithms themselves, as human developers may unintentionally encode their own biases in models.

Another vulnerability of AI models is that they are trained on historical data. As such, they are limited to the examples of stress and outlier events present in these data and are not trained for black swan (OECD, 2024) events. Therefore, they may be less reliable and less predictive during future periods of stress.

2.5 Hype around AI-centred companies

Booming valuations of AI-centred companies pose a potential risk to financial stability as they may lead to price bubbles. Hyping the transformative potential of AI floods the market with capital. It overinflates valuations of companies that may not deliver the expected technological breakthroughs, thus increasing the risk of a market correction (Waters and Bradshaw, 2024).

In such an environment, companies, especially start-ups, may strategically market themselves as "AI-driven" to attract funding, even if their core technology or business model does not fully align with AI innovation ["AI washing" (Marr, 2024)]. Moreover, this rush toward AI investments can lead to a lack of diversification in portfolios, as investors concentrate too heavily on AI companies. If AI-driven companies fail to deliver on their promises or if the broader market corrects, these concentrated portfolios could suffer significant losses.

Regarding securities markets, preliminary analysis by ESMA of European fund investments in AI indicates that European equity funds have significantly increased their exposure to AI-related companies. Between 2021 and 2024, the average exposure of these funds to AI companies and related instruments grew from 8% to 12.5%. In addition, 10% of equity funds now allocate more than 30% of their portfolios to AI companies.[4]

4 Upcoming ESMA article.

2.6 Risks amplified by social media

Social media is another area of concern when it comes to risks amplified by AI, particularly generative AI. Social media platforms have become powerful tools for information dissemination in financial markets as they influence shifts in market sentiment, stock price movements and other market developments. Social media platforms use AI algorithms to enhance engagement on the platform and thus increase advertising revenue (The Economist, 2024b).

Social media algorithms are often designed to identify and promote the content most likely to capture users' attention, including financial rumours and market speculation. This amplification of misleading information can increase market volatility. Recognising these risks, in May 2024 ESMA reported that AI can be used to assist in drafting marketing communications, including advertisements and social media posts (ESMA, 2024b). In its statement, ESMA provided initial guidance to firms using AI when offering investment services to retail clients to address the potential risks of misleading information and other such risks.

Moreover, AI can be exploited to create sophisticated disinformation campaigns, such as deepfakes and fake news, which can be strategically deployed to manipulate market sentiment. False narratives can rapidly spread and influence investor behaviour, trigger panic selling and artificially inflate stock prices.

Another manifestation of this risk occurs at the interplay between algorithmic trading, social media and AI. AI-enhanced trading systems, which execute trades based on real-time data analysis, may respond to sudden shifts in sentiment triggered by social media content. This can create feedback loops in which AI algorithms amplify price movements based on misinformation or rumours, causing swings in asset prices. In extreme cases, these AI-driven responses to social media misinformation can lead to flash crashes or bubbles (Gopinath, 30 May 2024).

3. Supervisory considerations

While there is broad consensus that AI technologies are transforming the financial intermediation process and other critical financial system functions, the current level of AI penetration and the factors outlined in this paper suggest that its impact on the real economy has not yet reached destabilising levels. However, this may quickly change as AI continues to be integrated in financial services, and so requires continual monitoring.

To stay ahead of potential disruptions, regulators must closely track the evolving applications of AI in the financial sector, deepen their understanding of emerging risk sources and transmission channels, and engage in cross-sectoral and cross-border dialogue.

From a supervisory perspective, it is important to note that some risks associated with AI in Europe are addressed by the AI Act [Regulation (EU) 2024/1689], a risk-based cross-sectoral regulation with only a few provisions specific to the financial sector. The Act covers AI-based creditworthiness assessments by banks, and pricing and risk assessments in life and health insurance, but no high-risk use cases have been identified in the securities sector.

However, this does not mean that the application of AI technologies by financial institutions falls outside the regulatory perimeter. In the technology-neutral approach, regulations apply to financial activities regardless of the technology used to produce them. This means that existing regulations remain in force for the financial sector, whether or not AI models and tools are applied. For example, in the European securities sector, ESMA has confirmed that firms using AI are expected to comply with relevant MiFID II requirements, particularly in relation to organisational issues, conduct of business and their obligation to act in the best interests of their clients. The current regulatory framework provides a solid foundation for addressing potential risks to financial stability and to customers.

References

Chen H. and Magramo K. (2023). Finance worker pays out $25 million after video call with deepfake 'chief financial officer.' *CNN*. 4 Februay 2023. Available here (last accessed 20.09.2024).

Danielsson, J. and Uthemann, A. (2024, June 5). On the use of artificial intelligence in financial regulations and the impact on financial stability. *SSRN*. Available here (last accessed 19.09.2024).

DNB, AFM. (2024). The impact of AI on the financial sector and supervision. Available here (last accessed 18.09.2024).

EC. (2024). Targeted consultation on artificial intelligence in the financial sector. *European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union*. Available here (last accessed 19.09.2024)

ESMA. (2023a). Artificial intelligence in EU securities markets. *ESMA TRV Risk Analysis, 1 February 2023.* Available here (last accessed 18.09.2024).

ESMA. (2023b). Artificial intelligence. *ESMA TRV Report, No. 2, 2023, pp.35-36.* Available here (last accessed 18.09.2024).

ESMA. (2024a). Artificial intelligence. *ESMA TRV Report, No. 1, 2024, p.36.* Available here (last accessed 18.09.2024).

ESMA. (2024b). Public statement on the use of artificial intelligence (AI) in the provision of retail investment services (ESMA35-335435667-5924). 30 May 2024. Available here (last accessed 20.09.2024).

FSB. (2017). Artificial intelligence and machine learning in financial services (November 2017). *The Financial Stability Board.* Available here (last accessed 18.09.2024).

FSB. (2021). FSB Financial Stability Surveillance Framework (September 2021). *The Financial Stability Board.* Available here (last accessed 19.09.2024).

FSB. (2023). Enhancing Third-Party Risk Management and Oversight (4 December 2023). *The Financial Stability Board.* Available here (last accessed 18.09.2024).

Gopinath, G. (2024). Crisis amplifier? How to prevent AI from worsening the next economic downturn. *Remarks at the AI for Good Global Summit, Geneva, Switzerland. International Monetary Fund. 30 May 2024.* Available here (last accessed 20.09.2024).

IMF. (2021*).* Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance (22 October 2021). *International Monetary Fund.* Available here (last accessed 18.09.2024).

IMF. (2023). Financial institutions are forecast to double their spending on AI by 2027 (December 2023). *International Monetary Fund.* Available here (last accessed 18.09.2024).

IMF. (2024). Global Financial Stability Report: Steadying the Course: Uncertainty, Artificial Intelligence, and Financial Stability (October 2024). *International Monetary Fund.* Available here (last accessed 11.11.2024).

IOSCO. (2021). The use of artificial intelligence and machine learning by market intermediaries and asset managers (September 2021). *International Organisation of Securities Commissions.* Available here (last accessed 18.09.2024).

JC ESAs. (2022). Response to the European Commission's February 2021 Call for Advice on digital finance and related issues: regulation and supervision of more fragmented or non-integrated value chains, platforms and bundling of various financial services, and risks of groups combining different activities. *Joint Committee of the European Supervisory Authorities.* ESA 2022 01, 31 January 2022. Available here (last accessed 20.09.2024).

Leitner G., Singh J., van der Kraaij A., and Zsámboki, B. (2024). The rise of artificial intelligence: benefits and risks for financial stability. *Financial Stability Review (May 2024).* Available here (last accessed 18.09.2024).

Liang N. (2024). Remarks on Artificial Intelligence in Finance. *Speech delivered at the FSB Roundtable on Artificial Intelligence in Finance. 4 June 2024.* Available here (last accessed 18.09.2024).

Marr, B. (2024). Spotting AI washing: How companies overhype artificial intelligence. *Forbes. 25 April 2024.* Available here (last accessed 20.09.2024).

McKinsey & Company. (2023). The economic potential of generative AI: The next productivity frontier. Available here (last accessed 19.09.2024).

OECD. (2021). Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers. *OECD Publishing.* Available here (last accessed 18.09.2024).

OECD. (2024). Regulatory approaches to Artificial Intelligence in finance. *OECD Artificial Intelligence Papers, No. 24. OECD Publishing.* Available here (last accessed 18.09.2024).

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.

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).

SEC. (2023). "Isaac Newton to AI": Remarks before the National Press Club. *Speech by SEC Chair Gary Gensler. 17 July 2023.* Available here (last accessed 19.09.2024).

Shabsigh G. and Boukherouaa E. B. (2023). Generative artificial intelligence in finance: risk considerations. *IMF Fintech Notes 2023/006 (October 2023). International Monetary Fund.* Available here (last accessed 18.09.2024).

The Economist. (2024a). AI models make stuff up. How can hallucinations be controlled? 28 February 2024. Available here (last accessed 20.09.2024).

The Economist. (2024b). A tech ethicist on how AI worsens ills caused by social media. *29 May 2024.* Available here (last accessed 18.09.2024).

The Economist. (2024c). The war for AI talent is heating up. 8 June 2024. Available here (last accessed 18.09.2024).

The Economist. (2024d). Regulators are focusing on real AI risks over theoretical ones. *22 August 2024.* Available here (last accessed 18.09.2024).

Waters, R. and Bradshaw, T. (2024). Wall Street frets over Big Tech's $200bn AI spending splurge. *Financial Times. 1 November 2024.* Available here (last accessed 11.11.2024).

3. The risks and impact of AI in the financial sector: AI and sustainability risks

Giuseppe Sciascia

European Commission DG Reform

1. Introduction

The mutually reinforcing and simultaneous 'digital' and 'green' transitions are having significant impacts on our economies and financial systems (EC, 2022). They have resulted, among other things, in the formation of a complex network of interrelationships between the deployment of advanced technologies and efforts aimed at ensuring a transition to a more sustainable economic model which considers and integrates environmental, social and governance (ESG) elements. While advanced technologies have the potential to contribute to a more efficient use of natural resources and to the achievement of sustainability aims, they also have impacts that reverberate across multiple ESG dimensions, and that might therefore prevent the achievement of these same overarching aims. This observation extends to applications based on artificial intelligence (AI), which have been gaining unprecedented momentum and are being mainstreamed in several economic domains, including the financial sector, and are attracting large investment flows.

This chapter seeks to outline the complex interrelationship between AI and sustainability, with a particular focus on the implications for financial intermediation, regulation and supervision. The first section sets out the general context of the interaction between AI and sustainability elements. It reviews the opportunities and costs associated with the design, development and utilisation of AI-based applications from an ESG perspective, makes a distinction between the environmental and social dimensions, and outlines how they might be affected both positively and negatively. The second section discusses the specific implications for the financial sector, in particular by exploring a number of overarching questions pertaining to the interaction between the use of AI and the achievement of sustainability goals. How can AI-based applications be leveraged to meet sustainability targets? How should financial institutions integrate ESG considerations when approaching the use of AI-based applications? How and to what extent should financial supervisory authorities consider ESG factors when employing AI-based technologies for supervisory and regulatory purposes? What might the potential implications be for the EU financial supervisory architecture? The last section summarises the overall conclusions and acknowledges the need for further evidence and research in the field.

2. Artificial intelligence and ESG factors: opportunities and risks

A growing body of literature stresses the potential of AI not only as a tool for optimisation and automation but also as a catalyst for innovative, sustainable and socially responsible development (Shkalenko and Nazarenko, 2024). AI-based tools can undisputably act as enablers of the transition to a more sustainable economic system, as they contribute to efficient management of scarce natural resources, to reducing the impact of human activities on the environment and to building more resilient and just societies. A growing number of use cases demonstrate that AI can be regarded as beneficial in tackling the challenges in all sustainability dimensions, that it helps achievement of the global UN sustainable development goals (SDGs) and that it brings relevant benefits to humanity as a whole (Sætra, 2022). For instance, according to McKinsey (2024), AI is being used to help achieve 17 UN SDGs, including those aimed at eradicating poverty, establishing sustainable cities and communities, and providing quality education.

From an environmental perspective, AI tools can improve the management of global ecosystems and natural resources, thus contributing to the race towards decarbonisation, climate neutrality and adaptation. AI-based applications can also support the management of systems that play a pivotal role in achieving climate targets and restoring environmental sustainability, as is demonstrated by AI use cases concerning climate and emission management, energy, transport, water, food and agriculture, buildings, infrastructure and cities (Winston, 2024). Relevant examples include optimised building design and control, efficient management of energy and power grids, improvements in the efficiency of farms with so-called 'precision agriculture' (Cleary, 2017) and better emission and water management, along with improved traffic flows and logistics. Further enhancements are expected in terms of the production of goods and supply chain optimisation with a potential to reduce the carbon footprint of product creation and delivery. AI is also likely to contribute to predicting supply chain disruptions due to external events and factors, allowing companies to proactively address these issues. This could have positive effects in terms of adaptation and resilience to the challenges brought by climate change.

The beneficial impacts of AI in the social dimension are also gaining attention. AI-based applications are expected to positively impact several domains such as health and well-being, education, and the functioning of cities, and to contribute to better access to food and water; AI tools are also part and parcel of the recent trend towards digitalisation of public administration services and their functioning, as they contribute to speeding up and streamlining the provision of public services to citizens and their engagement in democratic processes (Madan and Ashok, 2023). As an example, AI-based tools are being deployed to enable students in the most remote parts of the globe to access education and to address the barriers preventing equal access to healthcare. Therefore, they cater for the needs of under-served populations. AI can also help with assessing governance risks in large firms and public institutions. For example, AI tools can evaluate the likelihood of regulatory breaches and unethical behaviour in a company or organisation, and so initiate the adoption of mitigation strategies aimed at proactively ameliorating the overall management of ESG risks.

Despite the positive elements sketched above, the costs and negative externalities associated with the development and deployment of AI-based tools are a matter of growing concern, which partially offsets the enthusiasm about this technology. Ironically, these downsides often relate to the very same environmental and social dimensions that AI can benefit. Criticisms are particularly relevant (and vocal) when factual evidence increasingly points to the notable environmental costs of AI. The concern is that the 'massification' of access to energy-hungry AI-based technologies may severely affect global decarbonisation. These considerations are partially addressed by the recent regulatory framework on AI that has been emerging in Europe. The AI Act explicitly cites the principle of social and environmental well-being developed by the Commission High Level Expert Group on AI. This means that AI systems should be developed and used in a sustainable and environmentally friendly manner and in a way that benefits all human beings while monitoring and assessing the long-term impacts on individuals, society and democracy.

The breakthrough of generative models which require a very intense use of computational power has clearly resulted in a massive global increase in the resource intensity and environmental footprint of AI. In this regard, commentators have referred to the dawn of the 'internet's hyper-consumption era,' a period defined by the spread of a new kind of computing that requires excessive amounts of electricity and water to build and operate (Rogers, 2024). A seminal analysis by Crawford (2021) already argued that AI is neither artificial nor particularly intelligent, as it depends on a very wide range of political and social structures, and it massively exploits human and natural capital. The functioning of AI-based tools is indeed the result of sequencing an intricate value chain. This requires intensive extraction of significant natural resources, which not only allow the infrastructure to 'run' but also AI-hardware to exist and perform. It is then followed by the collection and computation of data, in which automation is combined with the execution of human 'micro-tasks' compensated at very low rates.

Several recent investigations have added evidence and further substantiated concerns about the risks of AI from an environmental perspective, notably regarding energy and freshwater consumption. The increased popularity and ongoing development of generative models has increased the thirst for the energy required to increase computational capacity. This trend is today jeopardising the plans of big techs to achieve carbon neutrality (Taylor, 2024). Research by Goldman Sachs, for instance, has recently spotlighted a significant growth in power demand to a pace faster than the GDP increase in the US which is driven by data centres located in Virginia. The main takeaways of the report are that AI and data centres are not only boosting US power demand but also giving rise to potential power transmission bottlenecks that could constrain the future growth of data centres. This highlights the challenges that rising power demand is likely to create, and the need for investment in energy infrastructure (Goldman Sachs, 2024).

As for water consumption, a group of researchers at the University of California Riverside and the University of Texas Arlington have assessed the environmental impact of AI training with the use of water to cool data centres. They have devised a methodology to estimate the water footprint of AI models and found that in order to train GPT-3 alone, Microsoft and OpenAI used more than seven hundred thousand litres of water, the equivalent of cooling a nuclear reactor or producing more than three hundred cars. Moreover, when it comes to the use of the model, ChatGPT is equally demanding, as it requires half a litre of freshwater to run a conversation with 20-50 questions (Li, Yang et al., 2023).

Last but not least, AI might also cause risks with respect to the social and governance dimensions of the ESG triad. Related concerns are at the essence of the regulatory approach to AI recently promoted at the European level, as they reflect the potential impact AI can have on decision-making, economic relations and structure, and human society as a whole. In this respect, one of the most widespread concerns related to the use of AI-based tools is the potential perpetuation of biases embedded in the data with which these models are trained and in the perspectives of the designers of models. Fears also exist regarding the impact of AI on the workforce and access to the labour market, given the possibility of shifting tasks from humans to automated applications. Further specific concerns have been increasingly substantiated with regard to heightened risks of gender (Gender Shades, 2018) and racial discrimination, for example when it comes to applications aimed at identifying individuals using facial recognition and assessing credit scoring.

3. Artificial Intelligence, ESG factors and the financial sector

While not immune to the AI-driven revolution, the financial sector is being increasingly called on to contribute to the achievement of sustainability goals and – in particular – to the global fight against climate change, notably with respect to the implementation of urgent mitigation and adaptation actions. In a world in which the fiscal space for public authorities is increasingly narrower and does not allow the necessary flow of massive transformational investments, financial institutions play a crucial role in re-orienting credit and investment towards sustainable activities, and they are therefore increasingly required to embrace a radical change in their strategic approach to lending and asset management.

The multi-faceted interrelationship between AI-driven solutions and sustainability considerations is therefore particularly relevant to financial institutions and markets, and to the sectoral regulatory and supervisory authorities. As has been observed in other economic sectors, digital innovation can act as an enabler of a much-sought transformation that can help financial sector players manage ESG risks and achieve sustainability objectives. However, it can also introduce new types of sustainability risks that can negatively affect these very same aims.

On the bright side, AI-based applications have a very significant potential in terms of the capacity of financial institutions to manage ESG risks. An obvious case in point is the possible use of AI to improve and facilitate reporting and disclosure obligations stemming from the sustainable finance regulatory framework. This potential also attracts the interest of public financial sector supervisory and regulatory authorities, as they strive to both manage a sheer amount of data and information to secure an appropriate management of ESG risks in their supervisory remit and to follow their own institutional path towards sustainability and decarbonisation.

Not surprisingly, an area in which AI may bring relevant benefits for financial sector stakeholders is integration of ESG factors in their risk management practices. The ability of AI-based models to analyse extensive amounts of data from different sources and in different formats can support financial institutions in assessing the sustainability performance of their counterparts, anticipate potential risks and adopt appropriate mitigating actions according to their urgency and importance. Climate risk management is a particular area in which the use of AI-powered models shows a very large potential. In particular, the extrapolation, processing and analysis of structured and unstructured data from different sources can inform advanced modelling tools deployed by financial institutions – including banks and (re)insurance undertakings – to assess the impact on different balance sheet components in various climate scenarios. This can inform the development of appropriate mitigation strategies for different areas of risk.

Furthermore, AI tools can help financial institutions streamline activities to improve their sustainability profiles, including regarding compliance with sectoral regulatory requirements. For example, AI-driven investment portfolio strategies can help financial institutions seize opportunities linked to the achievement of specific sustainability goals. Further tools can also be deployed to improve monitoring of the carbon footprints of supply chains and the sustainability performance of clients, together with facilitating reporting of ESG-related data to supervisory authorities and the market.

AI-based applications are also being explored by supervisory authorities to assess sustainability claims and greenwashing risks associated with specific financial products on the market. Central banks are exploring how AI can be used to analyse company disclosures on carbon emissions, green bond issuance and voluntary net-zero commitments. This has been the ambitious task carried out by the implementation of Project Gaia, an AI application developed by the Bank for International Settlements (BIS) and its project partners (the Bank of Spain, the Deutsche Bundesbank and the European Central Bank) aimed at addressing the challenges brought by the need to extract salient information from various texts and sources stemming from the various reporting standards applicable to financial institutions (BIS, 2024).

Against the backdrop of this enormous potential, however, financial institutions and supervisory authorities should not fail to investigate how the deployment of AI-based applications can affect their path towards sustainability. With particular regard to the EU supervisory landscape, the spread of these applications might also affect the dynamics of cross-border cooperation and the integration of supervisory processes as a result of a quest for carbon footprint reduction and resource-use optimisation.

A first consideration is understanding the impact of the use of AI tools on the scope 3 emissions of firms and authorities. For companies leveraging AI, a significant portion of this category of emissions stems from data centres and server infrastructure used to support AI applications. The energy-intensive nature of AI algorithms and data processing tasks results in heightened electricity consumption, driving up carbon emissions associated with server operations (FRDM, 2024), and ultimately the carbon footprint of the whole supply chain. Therefore, as AI solutions increasingly become an integrated element of the value chains of financial institutions, the emissions associated with their use should necessarily be estimated and reported as indirect ones – assuming that they stem from sources that are neither owned nor directly controlled by the company itself. Of course, this will introduce complex problems of estimation and material assessment vis-à-vis the overall operations of the firm. Acknowledging the relevance of these emissions might lead financial institutions to actively engage with AI-solution providers and promote higher levels of transparency in their operations and improvements in terms of efficiency, processes optimisation and recourse to renewable energy and carbon offsetting.

A second factor conducive to appropriate management of the ESG risks associated with the use of AI-tools is assessment of the impact of AI on a financial institution's workforce. As has been shown by a recent IMF analysis

(IMF, 2024), almost 40 percent of global employment is exposed to AI, with advanced economies facing greater risks – and more opportunities – resulting from the use of these technologies. Impacts span from lower labour demand to reduced wages and hiring rates. The pervasive use of AI in the operations of financial institutions has similar effects negatively affecting employees by giving rise to redundancies, job replacements and growing inequalities. As part of the management of the social and governance risks associated with extensive operational deployment of AI tools, therefore, financial institutions need to engage in active dialogue with their workforces and social stakeholders, to invest in upskilling and reskilling workers, and to understand how working conditions and benefits can be affected.

As part of the management of the ESG risks associated with the use of AI, financial institutions also need to consider the impact of AI tools on respect for the principles of fairness and non-discrimination, particularly when it comes to manufacturing and distributing products and services to their clients. This is closely associated with broader ethical considerations stemming from the use of AI-based tools in the finance industry, and it has been extensively explored by European supervisory authorities. For example, in a 2021 report EIOPA (EIOPA, 2021) called for firms to adhere to the principles of fairness and non-discrimination when using AI, in particular by taking into account the outcomes of AI systems. This requires balancing the interests of all stakeholders involved, appropriately considering financial inclusion issues and undertaking mitigating actions to prevent bias and discrimination.

A final but not less important consequence stemming from integrating ESG considerations in assessments of the impact of AI-based applications in the finance sector relates to the role of, and interactions among, regulatory and supervisory authorities. AI-based applications might act as catalysts for changes in the extremely fragmented European supervisory and regulatory landscape. These tools clearly have the potential to not only optimise the efficiency of the supervisory processes of individual competent authorities but to also facilitate and strengthen cross-border cooperation, for example by establishing fully integrated processes in which the secure execution of tasks by different authorities in the same supervisory procedure is possible thanks to these advanced technologies. When taking into account ESG factors, and in particular the environmental costs associated with the design, development and deployment of AI-based tools, one can easily see the advantages of a centralised approach in which single applications might serve the whole supervisory community in an optimised and efficient manner. In short, will the aims and forces of the 'twin transitions' become the drivers of a new phase of centralisation in the EU supervisory landscape?

4. Conclusions

At the end of 2020, Dr. Timnit Gebru – a pioneer critical researcher in AI – was suddenly ousted from her role as co-leader of the Google ethics AI team, the reason being her contribution to a prominent research paper on the risks of large language models. Dr Gebru and her co-authors had identified a wide variety of costs and risks associated with the rush towards these models, including environmental costs, financial costs erecting barriers to entry, opportunity costs for researchers taking effort away from directions requiring less resources, prominent risks of stereotyping and denigration, and increases in extremist ideology (Bender et al., 2021). Her story is a dramatic testament to the problematic, unresolved relation between AI development and ethical concerns, and the difficulties associated with properly examining, exploring and assessing the implications stemming from the use of AI from the perspective of sustainability.

The interaction between the use of AI and the management of ESG risks in the financial sector raises a number of new unaddressed questions, and it is a matter only partially addressed by the current AI regulatory framework. As is well known, the AI Act adopted by the European Union defines two groups of high-risk use cases for the financial sector: those used to evaluate the creditworthiness of individuals and those aimed at assessing risks and at pricing life and health insurance for individuals. Nonetheless, all the while they play an increasingly prominent and central role in the financial strategies, processes and activities of institutions, AI-based applications will be a matter of concern requiring appropriate consideration in the ESG risk management practices of institutions.

This chapter has attempted to provide a first bird-eye view of the ESG implications stemming from the deployment of AI-based tools by financial institutions. It has argued that the advantages associated with their use should be appropriately weighed against the impact they might have on various ESG dimensions. For good or for bad, AI-based tools might indeed gradually impact the path of an institution towards achieving specific sustainability targets, and so planning and gradually introducing them therefore require due consideration. This should also be considered by supervisory authorities, which should not only investigate the potential risks associated with mainstreaming AI in the activities of financial institutions from an ESG perspective but should also carefully assess the impact these tools might have on their own activities.

Given the novelty of this topic, and the fact that analyses and empirical studies related to the interaction between AI and sustainability are in an early stage, future research should help to shed further light on the matters touched on in this contribution, and to investigate how AI can and will influence – for good or for bad – the race towards a more just and sustainable equilibrium by human society.

References

Bender E., Gebru T., McMillan-Major A., and Shmitchell S. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? F*AccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*. Available here.

BIS (2024). Project Gaia: Enabling climate risk analysis using generative AI. *BIS Innovation HUB*. Available here.

Cleary D. (2017). Precision Agriculture: Potential and Limits. Available here.

Crawford K. (2021). Atlas of AI. *Yale University Press*. Available here.

Danelski D. (2023). AI programs consume large volumes of scarce water. *UCR Edu*. Available here.

EC (2022). Muench S., Stoermer E., Jensen K., Asikainen T., Salvi M., and Scapolo F. Towards a green and digital future. *Publications Office of the European Union, Luxembourg*. JRC129319. Available here.

EIOPA (2021). Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector. *European Insurance and Occupational Pensions Authority*. Report. Available here.

FRDM (2024). Navigating Your Company's Growing AI Carbon Footprint. Available here.

Gender Shades. (2018). Gender Shades Project. Available here.

Goldman Sachs. (2024). Global Markets Daily: Is AI Already Boosting US Power Demand? Available here.

IMF (2024). Gen-AI: Artificial Intelligence and the Future of Work. *International Monetary Fund.* Staff Discussion Notes No. 2024/001. Available here.

Madan R. and Ashok M. (2023). AI adoption and diffusion in public administration: A systematic literature review and future research agenda. *Government Information Quarterly*. Volume 40, Issue 1, January 2023, 101774. Available here.

McKinsey. (2024). AI for social good: Improving lives and protecting the planet. Available here.

Rogers R. (2024). AI's Energy Demands Are Out of Control. Welcome to the Internet's Hyper-Consumption Era. *Wired*. 11 July 2024. Available here.

Shkalenko A. V., and Nazarenko A. V. (2024). Integration of AI and IoT into Corporate Social Responsibility Strategies for Financial Risk Management and Sustainable Development. *Risks*. 12(6), 87. Available here.

Sætra H. S. (2022). AI for the Sustainable Development Goals. *Taylor & Francis Group*. Available here.

Taylor C. (2024). How much is AI hurting the planet? Big tech won't tell us. Available here.

Winston A. (2024). Will AI Help or Hurt Sustainability? *MIT Sloan Management Review*. Available here.

4. Transforming Financial Supervision with AI: Insights from the EU

Samir Kiuhan-Vásquez

Cambridge SupTech Lab and Florence School of Banking and Finance, European University Institute

The rapid advance and widespread adoption of AI technologies have been driven by the recent availability of vast unstructured data, significant increases in computing power and a surge in funding of innovative tech projects (Bahoo et al., 2024). Given the heavy reliance of the financial sector on big data and process automation, financial institutions have greatly benefited from these technological advances. Machine learning and deep learning models are applied to asset pricing, credit scoring and risk analysis, creating efficiencies and new business opportunities (CRS, 2024).

The changes brought about by AI, particularly machine learning, are also impacting the way financial supervisors oversee the market conduct and prudential behaviour of financial firms, thus improving current supervisory technology (SupTech) tools. Supervisors are recognising the potential for AI to enhance compliance and safety while being vigilant about its possible misuse to circumvent regulations. The development of AI challenges supervisors to stay abreast of industry advances and offers them opportunities to deploy their resources more efficiently and effectively to fulfil their mandates (Wall, 2018).

Specifically, AI has the potential to enhance macroprudential policy by developing advanced risk assessment models and improving our ability to predict institutional failures and detect market manipulation. The strength of machine learning and other AI-powered tools in recognising patterns in large datasets makes them valuable for supervisors to prospectively identify emerging risks (Aldasoro et al., 2024). Furthermore, these types of tools have the potential to provide efficiency gains in regulatory reporting and compliance by automating repetitive tasks and reducing costs for agencies and supervised entities (Beerman et al., 2021).

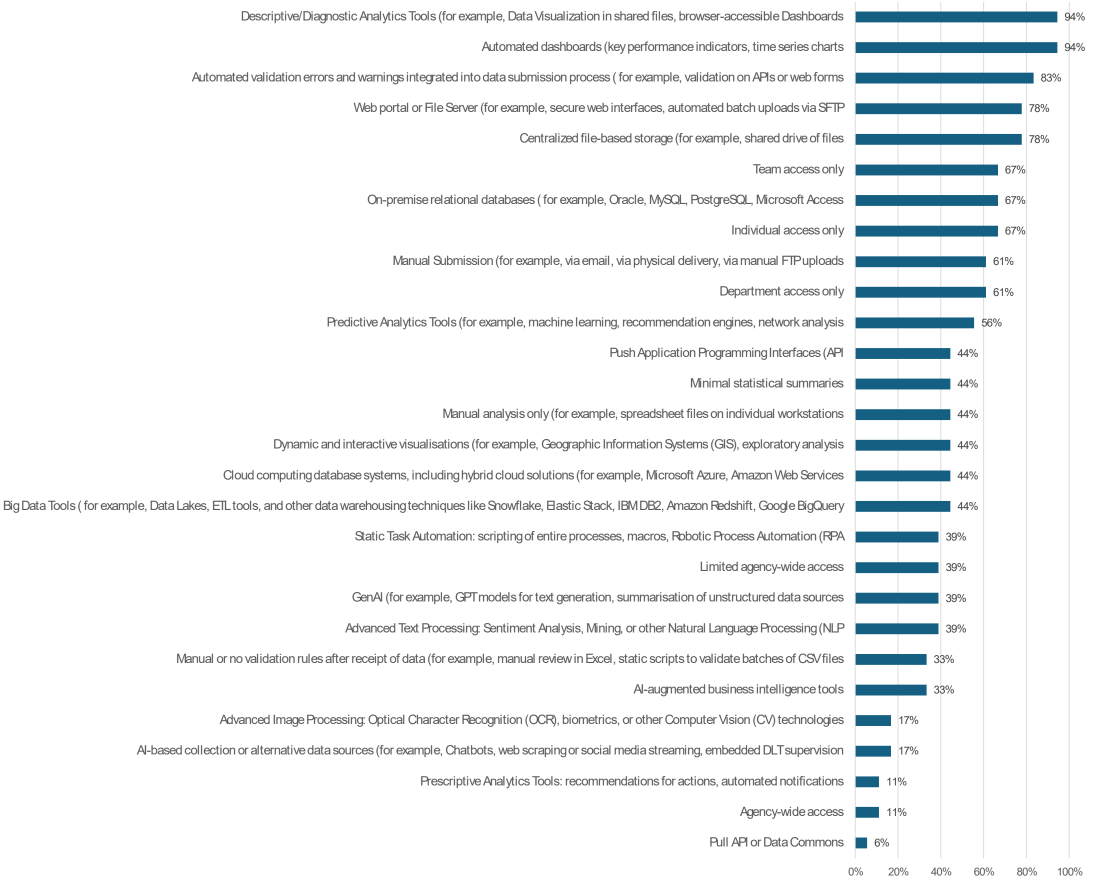
In order to measure SupTech adoption and the prevalence of AI-powered tools in the day-to-day activities of financial authorities, the Cambridge SupTech Lab (the Lab) has been producing a State of SupTech (SOS) Report since 2022. The SOS Report presents insights into the digital transformation of financial supervision and supervisory authorities worldwide. (Cambridge SupTech Lab, 2023).

The SOS Report is more than just an analysis; it is a collaborative tool for the entire ecosystem. In the latest version, the Lab included the Florence School of Banking and Finance as a technical partner, enriched the survey questions, showcased its capacity-building initiatives and increased the capillarity and reach of the report in the EU member states. The sample for the EU includes the European Central Bank and 17 national competent authorities, each in a different country. Respondents included 14 central banks, two financial supervisory authorities and two securities commissions.

The SOS Report is an extensive tool that provides a global perspective on suptech. It addresses a range of topics, including the supervisory use cases facilitated by SupTech, the challenges and enablers associated with digital infrastructure and technologies, and the processes that enhance the digital transformation of supervisory agencies. The 2024 SOS Report has two main sections. The first section covers fundamental questions about the SupTech landscape, supervisory areas, challenges, risks and technologies, consistent with previous editions for longitudinal analysis. The second section delves into specialised topics and offers detailed insights into AI, generative AI (GenAI), data governance, the data journey, collaboration and capacity building. For this chapter, we selected questions from both sections to measure AI adoption in SupTech and the main challenges faced on this journey. The SOS Report did not reveal specific answers at the EU member state level.

Figure 1 displays experimentation with AI at the National Competent Authority (NCA) level. For instance, a third of NCAs use AI-augmented business intelligence tools, and 17% use AI-based collection or alternative data sources (e.g. chatbots, web scraping, social media streaming or embedded DLT supervision). In comparison, 39% of respondents use GenAI (e.g. GPT models for text generation or summarisation of unstructured data sources). Interestingly, 56% of the agencies implement predictive analysis tools (e.g. machine learning, recommendation engines, network analysis) and 39% use advanced text processing (e.g. sentiment analysis, mining or other natural language processing).

Figure 1: What underpinning tools, techniques and technologies does your agency use to enable supervisory processes?



This zoom-in on the data stack of NCAs reflects the significant adoption of AI-driven supervisory methods in the region. The high adoption rates demonstrate successful integration, regulatory compliance and resource allocation.

Furthermore, these results show a solid commitment to leveraging AI capabilities in supervisory tasks.

The integration of AI in SupTech is in its early stages. The survey data show widespread deployment of AI by only 14% of NCAs, but with continual improvement, and no agency reports that AI is fully integrated and optimised in their processes. Around 71% of NCA pilot projects have limited deployment, and 14% are in the initial phase of exploration and research into AI applications. These results suggest a cautious and incremental approach to AI adoption, with agencies focusing on understanding and testing the abilities of AI before committing to full-scale implementation.

The data reveal that machine learning and natural language processing (NLP) are the most commonly adopted AI technologies used by most agencies in the EU for tasks such as predictive analytics and text analysis. Automating regulatory reporting processes and monitoring financial transactions are notable AI application areas. Meanwhile, AI applications in audio processing and computer vision tools are less frequently used. This distribution strongly emphasises leveraging AI for data analysis and regulatory compliance in the EU.

In the only question on the effects of the regulatory environment on SupTech implementation, the SOS Report asked if the existence or absence of AI regulations impacts agencies' strategy concerning adopting SupTech. The answers provide several important insights. First, 28.6% of agencies find that clear regulations accelerate their adoption of SupTech by providing a safe framework. This suggests that well-defined regulatory guidelines boost confidence and facilitate faster implementation. Another 14.3% of agencies find that collaborating with regulatory bodies to align their strategies better is beneficial. This shows the importance of cooperation between agencies and regulators to ensure the smooth adoption of SupTech.

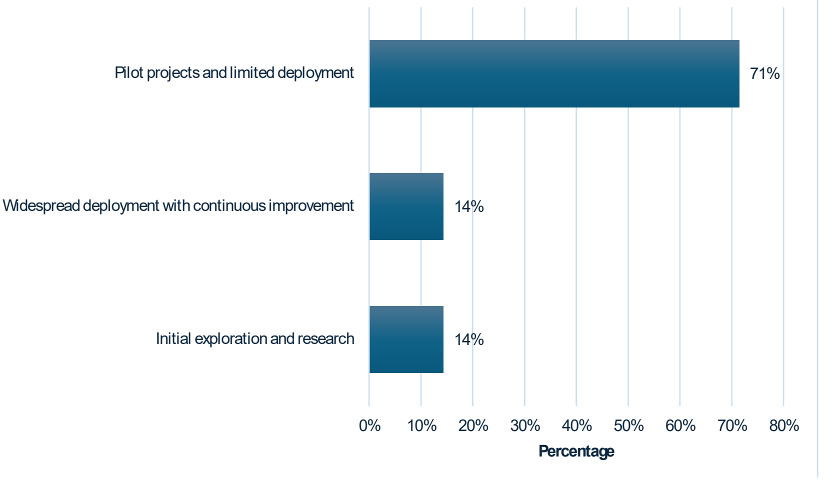
Conversely, 14.3% of NCAs also report that strict or unclear regulatory requirements hinder the adoption of SupTech, indicating that over-stringent or ambiguous regulations may create barriers to implementation. Overall, these responses reflect the diverse ways AI regulations influence the adoption of SupTech by agencies in the EU, revealing a need for clear and supportive regulatory frameworks and collaborative efforts.

In addition, NCAs were asked about the maturity level of their implementation of GenAI in SupTech applications. Most financial supervisors are either in the early stages of exploring GenAI or are conducting pilot projects. Specifically, half the institutions are in the initial exploration and research phase, suggesting that many are still trying to understand and experiment with GenAI technologies. A significant proportion, 36%, are engaged in pilot projects or limited deployment, indicating that while some institutions have moved beyond initial exploration, they are still in the testing and evaluation phase.

Meanwhile, 15% of the institutions have not implemented GenAI, possibly due to a lack of resources, expertise or perceived need. Only a tiny fraction, 2.5%, have achieved widespread deployment and continually improved their GenAI systems, which shows that fully mature GenAI implementations are still rare. This overall distribution suggests that GenAI is still an emerging technology with great potential.

According to a Financial Stability Institute (FSI) study, supervisory authorities are exploring new technologies to develop more user-friendly tools. Many are experimenting with GenAI to create chatbots to assist supervisors – and eventually the public – in finding, summarising and interpreting laws and regulations and to establish database co-piloting that allows supervisors to locate data using natural language, thus eliminating the need to learn programming languages (Prernio, 2024).

Figure 2: What is the maturity level of AI implementation in your agency's SupTech applications?



EU NCAs report several challenges in integrating AI in their supervisory processes. Integrating existing systems and workflows is the most prevalent issue affecting all the agencies answering this question. High implementation costs, resource requirements and limited computing resources further complicate the adoption of AI. Other notable barriers faced when deploying AI include poor data quality, limited technological capacity and a lack of transparency in AI systems, which is often referred to as the 'black box' problem.

One of the main challenges in adopting and integrating AI in SupTech is a need for skilled workers and initiatives to enhance the expertise of current staff, as nearly half the respondents highlighted these issues. It is of utmost importance to address concerns about talent acquisition and skill enhancement. There is a critical need for enhanced training and skill development programmes to upgrade the AI literacy and technical competences of supervisors – an agenda that the EU-SDFA continues to promote.

Such programmes can ensure that supervisors develop the necessary skills to effectively leverage AI by focusing on real-world applications to bridge the gap between theoretical knowledge and practical implementation.

Figure 3: Has your team undertaken capacity building or other programmes on data science in SupTech applications?

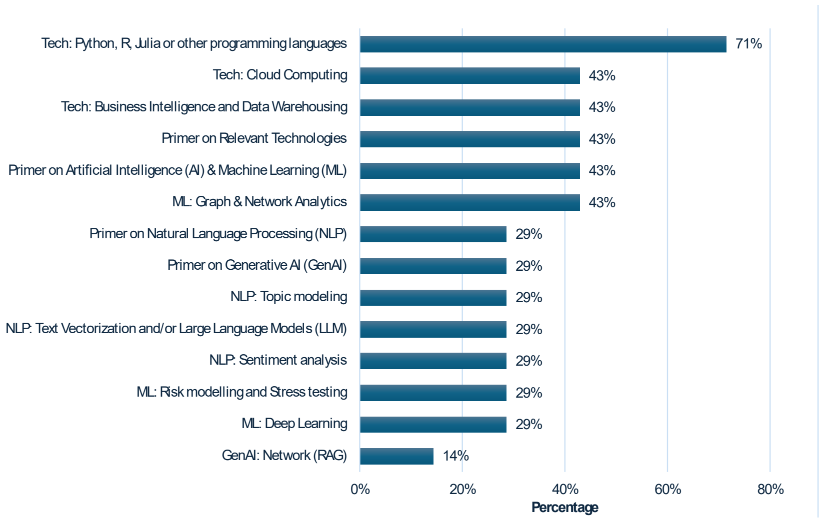


Figure 3 shows the variety in training preferences and reveals the commitment of NCAs to building comprehensive AI abilities in multiple domains. The most sought-after training – in programming languages such as Python, R and Julia – indicates a robust foundational need for technical skills. There is also significant interest in machine learning, particularly in graph and network analysis, risk modelling and deep learning. In addition, agencies are keen to understand NLP techniques, including sentiment analysis, text vectorisation and topic modelling. Training in generative AI, business intelligence, data warehousing and cloud computing is also in considerable demand.

Meeting the demand for technical skills can also mitigate the 'black box' challenge by promoting the development and use of transparent and explainable AI systems. When developers and data scientists are well-trained, they are better equipped to help develop more explainable and trustworthy AI. This means they can build AI models that clearly show how decisions are made, rather than being mysterious or opaque (Vorras and Mitrou, 2021).

In an open-ended question NCAs were asked to identify the anticipated challenges in implementing SupTech. One of the predominant themes that emerged was the integration of AI technologies. One of the primary obstacles is limitation of resources, both financial and human. Developing, deploying and maintaining sophisticated AI-driven tools require substantial investment, and budget constraints can limit the speed and scope of implementation. In addition, the need for highly specialised skills in AI and data science adds another layer of complexity in future implementation of SupTech as competition for talent in these fields is fierce. Keeping up with the rapid pace of technological advancement is also a challenge, as what is cutting-edge today may become obsolete tomorrow. This requires continual learning and development to ensure that the workforce remains up to date with the latest technologies and methodologies.

Finally, NCAs state that as they transition to more tech-driven supervision, they must ensure compliance with existing regulations and maintain robust data security protocols. Using AI and big data analysis introduces new regulatory challenges, particularly regarding privacy, transparency and accountability. It is essential to ensure that AI tools operate within the law and respect regulations such as the GDPR and the AI Act. In addition, it is vital to find the right balance between leveraging technology and maintaining the critical role of human judgment. While AI can significantly enhance capabilities, it is not infallible, and over-reliance on technology can lead to blind spots or a false sense of security. Therefore, it is crucial to continue valuing and investing in human expertise to ensure effective supervision.

References

Aldasoro I., Gambacorta L., Korinek A., Shreeti V., and Stein, M. (2024). Intelligent financial system: How AI is transforming finance (BIS Working Paper No. 1194). *Bank for International Settlements*. Available here.

Beerman K., Prenio J., and Zamil R. (2021). SupTech tools for prudential supervision and their use during the pandemic (FSI Insights No. 37). *Bank for International Settlements*. Available here.

Bahoo S., Cucculelli M., Goga X., and Mondolo J. (2024). Artificial intelligence in Finance: a comprehensive review through bibliometric and content analysis. *SN Business & Economics.* 4, 23. Available here.

Cambridge SupTech Lab. (2023). State of SupTech Report 2024. Available here.

Congressional Research Service. (2024). Artificial Intelligence and Machine Learning in Financial Services. *CRS Report.* No. R47997. Available here.

Prernio J. (2024). Peering through the hype assessing SupTech tools' transition from experimentation to supervision. *FSI Insights on policy implementation.* No 58. Available here.

Vorras A., and Mitrou L. (2021). Unboxing the Black Box of Artificial Intelligence: Algorithmic Transparency and/or a Right to Functional Explainability. In Synodinou TE., Jougleux P., Markou C., and Prastitou-Merdi T. (eds) *EU Internet Law in the Digital Single Market*. Springer, Cham. Available here.

Wall L. D. (2018). Some financial regulatory implications of artificial intelligence. *Journal of Economics and Business*. 100, 55-63. Available here.

5. The global artificial intelligence regulatory landscape[1, 2]

Iota Kaousar Nassr

Organisation for Economic Co-operation and Development (OECD)

Artificial intelligence (AI) technologies and tools have been around for many decades and employment of them in finance has been increasing in recent years. Most recently, the advent of generative AI (GenAI), such as large language models (LLMs), represents a breakthrough in the evolution of AI innovation and it has captured public attention and renewed interest by financial market participants, financial consumers and policymakers.

Integrating AI in the financial sector can offer market participants and consumers significant advantages by enhancing efficiency and productivity (e.g. cost savings), improving product and service quality (e.g. tailored personalised offerings) and potentially promoting financial inclusion (e.g. servicing underserved clients such as thin-file SMEs) (OECD, 2021). However, a broader application of AI in finance may intensify existing market risks and introduce new challenges. GenAI in particular can exacerbate AI-related risks and intensify concerns about the use of AI tools in finance (e.g. data privacy and confidentiality, robustness of outputs, the potential for market manipulation) (OECD, 2023). It is therefore critical to consider policy frameworks to protect financial

1 This chapter is based on the OECD publication 'Regulatory Approaches to AI in Finance.' See (OECD, 2024) for a more detailed analysis.

2 The opinions and arguments expressed in this chapter are the sole responsibility of the author(s) and should not be reported as representing the official views of the OECD or its member countries.

markets and their participants, and ensure that financial product and service markets remain fair, orderly and transparent when AI is utilised in finance.

A recent study has analysed the different regulatory approaches to using AI in finance in 49 OECD and non-OECD jurisdictions based on an OECD survey (OECD, 2024)[3]. Most respondents indicated that they have appropriate regulations in place, although they also acknowledged that potential gaps may exist or emerge, and more general guidance for market participants may be valuable.

The absence of specific regulations on AI in finance can be (at least partly) attributed to the fact that existing financial regulations, laws and guidance only apply to financial activities regardless of the technology used. Technological advances do not negate existing safety and soundness standards or compliance requirements. In fact, most OECD jurisdictions take a technology-neutral approach to the applicable requirements and expectations. When AI is used in areas covered by existing rules or guidance, such rules or guidance should generally apply whether the decision is made by AI (with or without human intervention), traditional models or humans (OECD, 2024).

In Japan, although there is no specific legislation, regulation or policy framework on AI use in the financial sector, existing regulations and guidance may apply depending on the use case (e.g. model risk management, IT governance, cybersecurity or consumer/investor protection). Similarly, in the UK the Bank of England and the Financial Conduct Authority (FCA) adopt a technology-agnostic outcome-based approach to supervision and regulation, including on the use of AI. They consider the existing policy framework fit for purpose to manage the risks and challenges posed by AI in finance. The Bank of England and the FCA have provided their views on the regulatory framework for AI use in UK financial markets, including an overview of the key rules and guidance in the existing framework that are most relevant to mitigating AI-related risks (Bank of England and FCA, 2022).

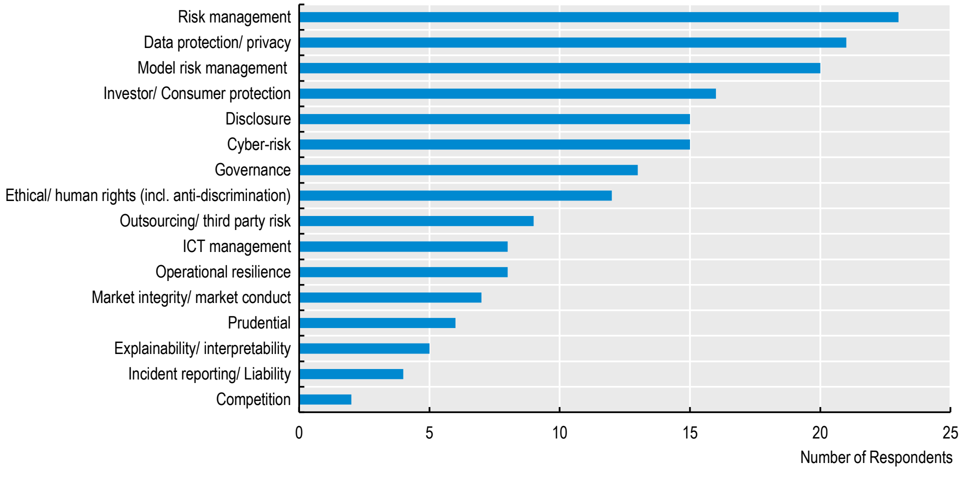
3 The report is based on 49 responses to the OECD Survey on Regulatory Approaches to AI in Finance by 38 OECD countries (i.e. Australia, Austria, Belgium, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, the United Kingdom and the United States), by 6 accession candidates to the OECD (i.e. Argentina, Brazil, Bulgaria, Croatia, Peru and Romania) and by 4 non-OECD member jurisdictions (i.e. Hong Kong (China), Indonesia, Singapore and South Africa), together with a consolidated answer provided by EU Institutions (i.e. EC, EBA, EIOPA, ESMA), which was conducted in Q1 2024.

In the US, the 2021 interagency Request for Information (RFI) and Comment on Financial Institutions' Use of AI, Including ML issued by financial authorities[4] contains an appendix with a non-exhaustive list of laws, regulations, supervisory guidance and other statements relevant to AI issued by agencies. The RFI includes existing laws and regulations relating to safety, soundness and consumer protection. It also explains that other laws, regulations, guidance and statements may be relevant depending on the particular facts and circumstances, while some laws and regulations are applicable to any process or tool a financial institution employs, regardless of whether or how a financial institution uses AI (US Interagency, 2021). In addition, the 2023 Financial Stability Oversight Council annual report states that existing requirements and guidance may apply to AI (FSOC, 2023). These include general risk management requirements that apply to any technology used and to domain-specific use cases, such as fair lending, that already have established rules with which AI must conform.

The OECD analysis provides examples of rules and regulations that may apply to the use of AI in finance and that can be grouped into the set of areas depicted in Figure 1. These include ethical and equity considerations (e.g. rules protecting against bias and discrimination), risk management and in particular model risk management, prudential frameworks, market conduct regulations, consumer and investor protection, data-related frameworks, governance and accountability requirements, disclosure obligations, information and communication technology (ICT) management frameworks, rules on operational resilience, policies to protect against cyber-risk and rules on third-party risk management and outsourcing.

4 RFI is issued by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Consumer Financial Protection Bureau, the Federal Deposit Insurance Corporation and the National Credit Union Administration.

Figure 1. Examples of areas covered by existing financial sector rules



Note: As reported by respondents to the survey. Non-exhaustive.
Source: (OECD, 2024).

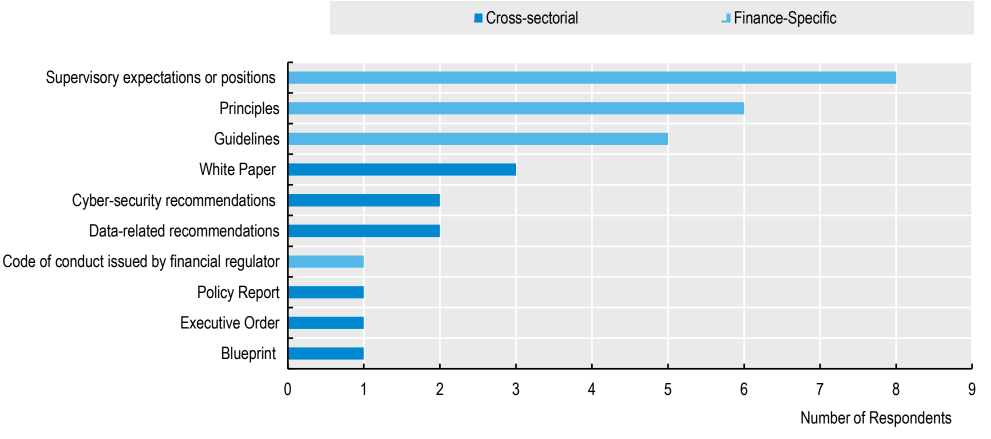
In addition to the existing rules and regulations, most respondent jurisdictions have introduced forms of binding and/or non-binding policies addressing AI in finance. Some jurisdictions have introduced cross-sectoral legislation that covers some financial activities (e.g. the AI Act in the EU, legislation in Brazil, Colombia and Peru) and/or have proposed other binding rules aimed at certain types of activity e.g. US SEC 2023 proposing release for broker-dealers and investment advisers (US SEC, 2023). More than a dozen respondents to the OECD survey reported non-binding policy guidance (e.g. blueprints, recommendations, principles, white papers etc.) either at the cross-sectoral level or targeting finance-specific areas of activity. The aim is to set priorities and provide guiding principles for the safe and responsible promotion of AI innovation (see Figure 2).

Although the form of policy guidance varies across jurisdictions (and even within the same jurisdiction), there are significant commonalities in its content. The guidance sets general expectations for AI users and systems, and highlights the importance of fairness and ethical use, accountability, compliance, transparency, governance and the development of safe, secure and robust AI systems. In a number of jurisdictions, the guidance encourages financial regulators to use their full range of authority to protect consumers and investors from AI-related risks (e.g. the United States). In addition, the supervisory authorities of some respondents have internal or public guidance setting out supervisory expectations for AI in finance.

For example, in the US Executive Order 14110 encourages federal agencies, such as the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC), to "consider using their full range of authority to protect American consumers and investors from fraud, discrimination and threats to privacy and to address other risks that may arise from the use of AI" (The White House, 2023). Previously, the White House Office of Science and Technology Policy had published a blueprint for an AI Bill of Rights providing guidance on the design, development and deployment of AI and other automated systems so that they protect the rights of the American public (The White House, 2022). Individual US agencies and offices have also issued reports related to AI, including sections of the annual reports by the Financial Stability Oversight Council (FSOC, 2023).

Similarly, in the UK in March 2023 the government published a white paper entitled 'A pro-innovation approach to AI Regulation,' outlining a non-statutory framework to drive innovation in AI, while also mitigating potential risks (UK Government, 2023). It adopts a principle-based approach to governing AI, with five core principles. In line with the US framework, the UK government indicated that it would be for UK independent regulators to interpret and apply these cross-cutting principles to AI use cases in their remits as they consider appropriate. Other examples include Japan, where the government is currently developing AI guidelines for businesses that take into account advances in GenAI, to complement existing cross-sectoral AI guidelines (METI Japan, 2024). In Switzerland, the Federal Council adopted guidelines on AI for the Confederation in 2020, while in Israel a policy report issued in 2023 by the Ministry of Innovation, Science and Technology, in conjunction with the Ministry of Justice, provides cross-sectorial policy recommendations for AI.

Figure 2. Examples of non-binding policy guidance reported by respondents to the survey



Note: Only at the national level. A non-exhaustive list of respondent actions. Excludes national strategies.
Source: (OECD, 2024).

Importantly, the different approaches outlined above are not mutually exclusive. In jurisdictions with binding legislation covering financial issues, existing sectoral regulations continue to apply without necessarily mentioning AI, reflecting the tech-neutral stance of OECD member countries. For example, in the EU, AI in the financial sector beyond the cases identified as high-risk and any other use cases (e.g. onboarding) included in the EU AI Act will be dealt with in accordance with pre-existing applicable legislation (e.g. Markets in Financial Instruments Directive (MiFID) II) irrespective of the technology used (see for example ESMA, 2024). By way of example, MiFID II includes requirements for investment firms and trading venues engaged in algorithmic trading and high-frequency trading (HFT) – activities that can also be based on AI systems.

Notwithstanding the fact that existing regulations have been reported to be applicable to AI in finance, there may still be a need to continually review existing frameworks to ensure they remain fit for purpose. Many respondents noted that they are still analysing whether further strengthening or expanding existing rules is necessary or beneficial to meet the policy objectives of regulatory authorities. This could be beneficial if, for instance, in the future gaps are identified in risk mitigation, or if reinterpreting existing rules or guidance would help achieve these objectives. This may also be needed when new laws/regulations are being introduced, and when it may be necessary to evaluate the interaction between existing and new rules, potentially requiring further adjustments to address any incompatibilities that may become apparent after new laws/regulations are implemented. All these considerations should take into account future developments in AI innovation, particularly in light of its rapid evolution.

At the implementation level there may also be a need for additional regulatory and supervisory guidance to assist authorised/supervised entities in their compliance. A small number of financial regulators and supervisors have issued clarifications noting the potential need for additional guidance, given the unique issues arising in the deployment of AI innovation in certain fields. Responding regulators in some jurisdictions continue to evaluate whether further clarifications are appropriate, including guidance on the way some of the existing requirements should be delivered to help supervised entities with their compliance. In terms of future plans for new regulation, however, the majority of respondents to the OECD survey do not plan to introduce new regulations on AI in finance in the near future.

At the international level, additional initiatives could be encouraged to promote convergence in the interpretation and application of existing rules. In addition, international policy dialogue and coordination, information sharing and efforts to support greater alignment between domestic and international regulators could be beneficial in effectively identifying and addressing emerging risks related to the deployment of AI in finance.

References

Bank of England and FCA. (2022). DP5/22 – Artificial Intelligence and Machine Learning. *Bank of England*. Available here. (accessed 23 April 2024).

ESMA (2024). ESMA provides guidance to firms using artificial intelligence in investment services. *European Securities and Markets Authority*. Available here. (accessed 19 September 2024).

FSOC. (2023). Financial Stability Oversight Council Releases 2023 Annual Report. *U.S. Department of the Treasury*. Available here. (accessed 29 April 2024).

METI Japan. (2024). (Draft) AI Guidelines for Business. Available here. (accessed 24 April 2024).

OECD. (2024). Regulatory approaches to Artificial Intelligence in finance. *Organisation for Economic Co-operation and Development*. Available here. (accessed 17 September 2024).

OECD. (2023). Generative artificial intelligence in finance. *Organisation for Economic Co-operation and Development*. Available here. (accessed 15 December 2023).

OECD. (2021). Artificial Intelligence, Machine Learning and Big Data in Finance Opportunities, Challenges and Implications for Policy Makers. *Organisation for Economic Co-operation and Development*. Available here. (accessed 14 September 2021).

The White House. (2023). Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence. *The White House*. Available here. (accessed November 2023).

The White House. (2022). Blueprint for an AI Bill of Rights. OSTP. *The White House*. Available here. (accessed 3 August 2023).

UK Government. (2023). A pro-innovation approach to AI regulation. p. 34. Available here. (accessed 21 April 2024).

US Interagency. (2021). Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning. Available here. (accessed 9 June 2021).

US SEC. (2023). Proposed rule: Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers. Available here. (accessed 21 April 2024).

6. The EU AI Act: logic, content and implications for finance

Marco Almada

University of Luxembourg

The AI Act[1] is the cornerstone of the EU's approach to AI regulation. One of the first laws on artificial intelligence to be enacted worldwide,[2] it governs AI technologies with a risk-based approach. This approach aims to foster the adoption of AI systems in the EU by creating a legal framework that balances the economic opportunities created by AI with the need to address the risks that the use of AI might create in terms of protecting public values such as fundamental rights, democracy, and the rule of law.[3]

In general terms, the Act relies on an ex-ante assessment by the lawmaker of the risks associated with some AI technologies, which will determine the legal framework applicable to AI-based products and services. Each framework establishes different legal requirements drawn from different strands of EU product safety law (Almada & Petit, 2025) which address the perceived risks that AI creates in that context. In the following pages, we examine the core elements of the AI Act.

1 Regulation (EU) 2024/1689. All article, annex and recital numbers mentioned in the text come from this regulation, unless otherwise stated.

2 Even though the AI Act was the first major legislative initiative on AI, both the Council of Europe and the US state of Colorado approved AI-related regulations before the AI Act was published in the EU Official Journal on 12 July 2024.

3 Art. 1(1).

Because the AI Act is a long and complex legal instrument,[4] the following pages only offer a bird's-eye view of its legal framework. By doing this, they offer a glimpse of its relevance in financial supervision[5] and allow the reader to examine whether the AI Act succeeds in its ambition to foster innovation in AI, or whether, as feared by some commenters (Draghi, 2024, p. 26), it can be a roadblock in the European approach to AI.

First, Section 1 discusses the overall policy logic that underpins the EU's approach to AI regulation. Then, Section 2 sketches the main regulatory requirements established by the Act and Section 3 discusses the interplay between the Act and EU financial market regulation. Finally, the chapter concludes (Section 4) with a brief discussion of how and why the AI Act matters to financial institutions and supervisory authorities.

1. The EU's rationale for AI regulation

In April 2021, the Commission introduced its original proposal for an Artificial Intelligence Act. After many years of sustained progress in AI technologies, which were being applied in an ever-growing number of fields, this proposal was a reaction to substantial controversy regarding the opportunities and risks associated with AI (Bakiner, 2023). The Commission relied on various sources, such as the work of a High-Level Expert Group on AI that operated from 2018 to 2019, and the EU's experience with product safety law (Mazzini & Scalzo, 2022). This process resulted in a legislative proposal that built on existing product safety instruments but featured some fundamental changes which reflected the unique risks associated with AI technologies.[6]

During the AI Act legislative procedure, the original proposal evolved in several important ways. In particular, the final version of the Act reflected the need to address general-purpose models, such as large language models, which only became widespread after the proposal was introduced.[7] Nevertheless, the Act that is now in force largely follows the regulatory architecture proposed in 2021 by the Commission, even though many details underwent substantial adjustments.

4 It has 113 articles, accompanied by 180 recitals and 13 annexes.

5 For an in-depth analysis of this sector, see Passador (2025).

6 See Section 2.6.2 below.

7 On this point, see (Almada & Petit, 2025, sec. 4).

One crucial thing that remained unchanged is that the AI Act pursues a broad range of aims. Just like traditional product safety legislation, the provisions of the Act are meant to ensure a high level of health and safety protection of those affected by the use of AI. At the same time, as mentioned above, they also aim to protect other public values such as fundamental rights. These aims do not always align with one another. For example, Article 10(5) creates a new legal basis for processing sensitive personal data on the grounds that existing rules under EU data protection law[8] were not enough to enable measures to mitigate potential biases in data used to train algorithms in high-risk contexts. Thus the structure of the AI Act reflects a variety of compromises and trade-offs.

To address the risks associated with AI technologies, the AI Act controls access to the EU single market. It defines two AI-related products, the *AI system* and the *AI model*. It then stipulates that such products can only be placed on the EU single market if they meet certain requirements.[9]

An AI system is a machine-based system that infers from its input data how to generate outputs that can influence physical or virtual environments. These outputs can take various forms, such as predictions, recommendations or decisions.[10] For example, a system that uses a machine learning technique to detect outliers in financial transactions would meet this definition. An AI model, instead, is a component that allows an AI system to make such inferences.[11] For example, many uses of AI in 2024 are powered by large language models such as GPT-4 and Claude (OECD, 2023). To make an analogy with another branch of product safety law, the AI Act sets rules for both cars (AI systems) and engines (models).

Different types of systems and models are subject to different requirements, which are examined more closely in Subsection 2.6.2 below. Some of these requirements stipulate technical properties that an AI system or model must have. Others, instead, oblige actors involved in the AI supply chain to monitor incidents related to their systems or models, adopt measures to address hazards and cooperate with market surveillance authorities. These two sets of obligations aim to both mitigate risks and create a mechanism for responding to any harms that escape the initial measures.

8 See, in particular, Art. 9 Regulation (EU) 2016/679 (GDPR).

9 In addition, the AI Act lays down rules regarding how AI systems are put into service and used, as is discussed below.

10 Art. 3(1). Under this definition, an AI system may or may not rely on self-learning technologies, and it might be based on techniques other than machine learning.

11 Recital 97.

2. Risk regulation in the AI Act

The two kinds of products regulated by the AI Act – systems and models – involve different risks. When it comes to AI systems, the Act focuses on the purpose for which the system is developed and used:[12]

- Article 5 stipulates a closed list of practices in which AI poses an unacceptable risk. For each practice listed, placing on the market, putting into service and using an AI system to that end are prohibited.[13] For instance, one cannot use AI to download facial images from the internet or CCTV footage in order to create or expand facial recognition databases.[14]

- Article 6 defines a set of high-risk applications. Developing and using AI for such applications is only acceptable if done in conformity with a harmonised EU legal framework, as is detailed in Subsection 2.6.2.1 below.

- If the purpose of an AI system is not covered by either of the two lists, the AI Act considers that its risks are addressed by sector-specific regulation, either at the EU or at the national levels.

In addition, some rules apply regardless of the risk level of an activity. Providers[15] and deployers[16] of AI systems are required to foster AI literacy in their organisations.[17] Some systems are subject to transparency requirements.[18] For example, the provider of a chatbot must, in most cases, make sure that human users are aware they are interacting with an AI system.[19] For the most part, however, the legal framework applicable to an AI system is a function of its intended purpose.

For AI models, the AI Act follows a different approach. It creates cumulative layers of rules that apply to models. Most AI models are not subject to any special conditions to be placed on the EU market. If a model can be used

12 Recital 12.

13 Even if the practice itself remains lawful.

14 Art. 5(1)(e).

15 That is, an actor (regardless of its legal form) which either develops an AI system or commissions its development to market it under its own name or trademark: Art. 3(3).

16 That is, an actor (regardless of its legal form) using an AI system under its own authority: Art. 3(4).

17 Art. 4.

18 Art. 50.

19 Art. 50(1).

as a component of a broad range of AI systems, it is subject to a lightweight set of legal requirements that apply to all *general-purpose AI models*.[20] Additional rules apply to general-purpose models deemed to pose a systemic risk.[21] This framework is introduced in Subsection 2.2 below.

2.1 The legal framework(s) for high-risk AI systems

Under the AI Act, high-risk AI systems are subject to harmonised rules at the EU level.[22] Like a traditional product safety instrument, the Act establishes requirements that the provider of an AI system must meet before the system can be placed on the market.[23] However, it also creates obligations for other actors in the AI supply chain, in particular by stipulating requirements that deployers must observe when putting into service or using AI systems.[24]

These requirements can be categorised in three sets. The first set obliges the provider to ensure that the system is designed in a way that mitigates risks. For example, a financial institution designing a credit scoring system[25] must ensure that the data it uses are sufficiently representative of the group of persons it covers,[26] and take into account contextual factors that might be relevant for its operation, such as geographical or behavioural attributes of the population assessed.[27] Providers must also incorporate safeguards in their technical designs, such as functionalities for automated logging[28] and human oversight.[29] Furthermore, they must ensure that the system is transparent enough for deployers to understand its outputs and how to use it.[30] Last but not least, providers must ensure that systems have appropriate levels of accuracy, robustness and

20 Art. 3(63).

21 Art. 3(65).

22 Art. 1(2)(c).

23 Art. 16(a).

24 Art. 26.

25 Point 5(b), Annex III.

26 Art. 10(3).

27 Art. 10(4).

28 Art. 12.

29 Art. 14.

30 Art. 13(1).

cybersecurity.[31] For instance, the credit scoring system mentioned above would need to show that its outputs are good enough to guide credit decisions, and that the results can stand up to changes in the data about the population, and also against potential cyberattacks that might manipulate one's score or extract sensitive information.

The second set of requirements establishes disclosure duties. Providers must draw up and update detailed technical documentation which enforcement authorities can use to assess the conformity of a system with legal requirements.[32] They must also supply the deployers of their system with instructions to use it.[33] In the case of the credit scoring system, this would involve, for instance, information about how to interpret the outputs and what safeguards to use when running the system. Providers of high-risk AI are also required to register themselves and their systems in an EU-wide database.[34]

Finally, the third set of requirements consists of behavioural obligations. Providers must adopt a system of quality management practices[35] including practices aimed at detecting and managing risks throughout the life cycle of the system.[36] Deployers must follow the instructions for use[37] and perform various other duties. In particular, some deployers must conduct a fundamental rights impact assessment before certain AI systems are used.[38] This obligation covers any high-risk system used by public bodies, and, *inter alia*, systems used to assess creditworthiness (including credit scores) and risk assessment and pricing systems for life and health insurance. In addition to these duties, providers and deployers must cooperate with one another and with enforcement authorities to detect and address AI-related risks.

31 Art. 15(1). This obligation applies not only at the moment of initial deployment but also during the entire life cycle of the system. That is, from its initial conception to its deactivation.

32 Art. 11.

33 Art. 13(2).

34 Art. 49.

35 Art. 17.

36 Art. 9.

37 Art. 26(1).

38 Art. 27.

2.2 The governance of general-purpose AI models

General-purpose AI models are governed by two cumulative layers of obligations for providers. For every general-purpose AI model, its provider must put in place a policy to comply with the law on copyright and related rights,[39] draw up technical documentation and keep it up to date,[40] make available information and documentation to providers who want to incorporate the model in their own systems[41] and make public a summary of the content used to train the model.[42] These obligations do not require any technical intervention in the model but are meant to ensure that actors which integrate the model in their products can discharge their own legal duties.[43]

Some models are deemed to pose systemic risk due to their technical sophistication and widespread impact on the EU market.[44] A model is considered a general-purpose AI model with systemic risk if it meets certain technical thresholds.[45] If it does, its provider is subject to additional rules which oblige it to identify and mitigate risks proactively.[46] In this way, providers contribute to the safe(r) incorporation of such models in other AI-based products. However, this approach has been criticised for creating heavy burdens for cutting-edge innovation (Draghi, 2024) and failing to capture relevant sources of risk stemming from AI (Hooker, 2024). Its effects therefore remain to be seen in practice.

3. Implications for financial supervision

One of the distinctive properties of the AI Act is its horizontality. It applies in all domains covered by EU law, with few exceptions.[47] Therefore, AI systems used by financial institutions and by the financial sector are covered by the Act. In particular, systems used to assess creditworthiness or credit scores and those

39 Art. 53(1)(c).

40 Art. 53(1)(a).

41 Art. 53(1)(b).

42 Art. 53(1)(d).

43 Recital 101.

44 Art. 3(65).

45 Art. 51.

46 Art. 55.

47 Art. 2.

used for risk assessments and pricing life and health insurance fall in the high-risk category.[48] This means that a decision to use AI in a financial context is often bound by AI-specific legal requirements, in addition to the usually applicable legal framework.

To a large extent, the AI Act incorporates its new requirements in existing procedures for financial supervision. For example, the monitoring duties that apply to deployers of high-risk AI systems are deemed fulfilled if the deployer complies with the existing internal governance requirements in relevant financial services law.[49] In addition, financial supervisory authorities are designated as the market surveillance authorities for high-risk AI systems directly connected with the provision of regulated financial services.[50] Financial supervisors therefore become enforcers of AI regulation, but they must themselves comply with the requirements of the Act when they use AI.

As AI enforcers, financial supervisory authorities are granted additional powers to deal with technology-specific issues. They can carry out joint investigations with other market surveillance authorities,[51] and request access to documentation and to data sets used during development,[52] and even to the system's source code.[53] If they detect any risks in the course of these investigations (e.g. as a result of reports by providers or deployers, or from complaints lodged by natural or legal persons),[54] the Act empowers the authorities to request corrective measures, restrict or remove market access,[55] or impose fines and other sanctions.[56]

Keeping in line with the dual ambition of the Act to foster the use of AI while safeguarding public values, it also obliges national authorities to adopt measures to support innovation. For instance, each member state is required to have at least one regulatory sandbox in operation by 2 August 2026,[57] in which

48 Point 5, Annex III.

49 Art. 26(5).

50 Art. 74(6).

51 Art. 74(11).

52 Art. 74(12).

53 Art. 74(13).

54 Art. 85.

55 Art. 79.

56 Art. 99.

57 Art. 57(1).

the competent authorities are required to supply providers and prospective providers with guidance on regulatory expectations[58] in a controlled environment in which systems can be tested before being put on the market, put into service or used.[59] In particular, these sandboxes facilitate the reuse of personal data for the development of AI systems in the public interest,[60] potentially favouring the construction of systems to support the operation of financial authorities. Therefore, financial supervisors will be actively involved in governing the sandbox while their own use of AI technologies might benefit from it.

4. Conclusions

The AI Act creates a series of legal frameworks targeted at AI systems and models. Many uses of AI in the financial sector – both by regulators and by regulated actors – are not subject to additional requirements. Nevertheless, some important uses of AI, such as credit scoring and some law enforcement applications, are singled out as posing a particularly high risk to fundamental rights and other public interests protected by law. Therefore, the AI Act is an additional regulatory layer to be considered both by financial institutions and financial supervisors.[61]

In order to carry out their duties in the age of AI, financial supervisory authorities need to develop additional capabilities. They need to foster technical competencies in AI, and the legal expertise required to navigate risks to fundamental rights that fall outside their traditional remit. Therefore, the AI Act is likely to have tangible operational implications for the authorities responsible for financial markets, especially at first. If properly wielded, however, these new competences will be powerful tools to address the specific impacts of technological change in the financial sector.

58 Art. 57(6).

59 Art. 57(5).

60 Art. 69.

61 In fact, various provisions in the Act specify that its compliance requirements should be integrated in existing requirements under EU financial services law rather than duplicating information. See, e.g, Art. 72.

References

Almada M., and Petit N. (2025). The EU AI Act: A medley of product safety and fundamental rights? *Common Market Law Review*. Issue 62(1) forthcoming.

Bakiner O. (2023). Pluralistic sociotechnical imaginaries in Artificial Intelligence (AI) law: The case of the European Union's AI Act. *Law, Innovation and Technology*. 15(2), 558–582. Available here.

Draghi M. (2024). The future of European competitiveness, Part A – A competitiveness strategy for Europe. *European Commission*. Available here.

Hooker S. (2024). On the Limitations of Compute Thresholds as a Governance Strategy. *arXiv*. Available here.

Mazzini G., and Scalzo S. (2022). The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts. In C. Camardi (ed.), *La via europea per l'Intelligenza artificiale*. Cedam.

OECD. (2023). AI language models: Technological, socio-economic and policy considerations (DSTI/CDEP/AIGO(2022)1/FINAL). *Organisation for Economic Co-operation and Development*. Available here.

Passador M. L. (2025). AI in the Vault: AI Act's Impact on Financial Regulation. *Loyola University of Chicago Law Review*. Available here.

7. Ethical and consumer protection considerations

Pascale Lamb

European Insurance and Occupational Pensions Authority (EIOPA)

Julian Arevalo

European Insurance and Occupational Pensions Authority (EIOPA)

1. A forward-looking perspective on AI, ethics and consumer protection

As is amply documented by the insightful contributions in this volume, artificial intelligence (AI) offers the finance sector numerous advantages, including improved efficiency, automation, personalisation, and risk management. These advantages can be extended to consumers by enhancing their experiences with personalised recommendations based on their preferences, thus allowing them to make more informed decisions with real-time insights. The use of virtual assistants means that consumers can also interact with chatbots to ask questions about financial products, report incidents, and process information such as images and invoices. Meanwhile, the advent of generative AI is influencing how consumers make choices and how they interact with the products and services of firms (BEUC, 2020). As consumer behaviour shifts, individuals are seeking diverse sources of information beyond traditional channels, such as social media. Consequently, it is possible that generative AI tools will emerge as a prominent means for consumers to acquire information and recommendations, especially in financial services (Mogaji and Jain, 2024). Apart from the potential risk of misinformation, however, the general use of AI in financial services is not risk-free for consumers.

Besides important environmental implications and risks (see chapter 2.3 of this e-book by Sciascia), AI also brings substantial ethical and consumer protection risks. Assuming a wide take-up of AI technologies in the finance world in the years to come, this forward-looking section focuses on these risks and the measures that can be introduced to mitigate them.

One of the most pressing ethical concerns stemming from the use of AI in finance is its potential to entrench biases and inequalities. AI systems excel at recognising patterns in data. They are skilled at identifying and categorising information from training data and then using this knowledge to make predictions about new unknown data. However, any bias, errors or inaccuracies in the training data, whether intentional or accidental, will be reflected in the output (EIOPA, 2021a). However, while it is impossible to eliminate bias from data, as some groups will always be more heavily represented than others, financial firms are increasingly urged to implement fairness metrics and to evaluate AI systems for potential biases that can unfairly disadvantage certain groups.

Generally, and on the basis of well-designed algorithms and good quality data, the more data an algorithm is trained on, the more accurate its predictions become. While AI systems can identify numerous correlations in large datasets, not all correlations are cause-and-effect relationships. Regardless of how large the dataset is, it still represents a limited snapshot of reality. It is crucial to identify and address spurious correlations as they can lead to poor performance in real-world situations with changing circumstances. This can result in discriminatory outcomes, especially when these predictions affect individuals. For example, algorithms used in lending decisions may deny marginalised groups credit based on patterns present in historical data which have no relation to their actual creditworthiness (Orwat, 2020).

Another ethical concern tied to the application of AI in financial services is the rise of differential pricing (EIOPA, 2023), in which consumers are charged different prices for similar services based on insights derived from their data. While this practice can enhance personalisation and offer competitive advantages, it can also lead to unintended consequences. For instance, consumers with limited access to competitive offers or with lower bargaining power may end up paying higher prices for the same services, which exacerbates inequalities. Moreover, without transparency about how these prices are determined, consumers may not be able to make informed decisions or may feel unfairly treated, which undermines their trust in financial institutions.

To address this, regulators and firms must ensure that pricing algorithms adhere to fairness principles and provide clear explanations of price differences, thus fostering transparency and equity in consumer transactions.

The issue of transparency is indeed another critical ethical concern, given the 'black-box' nature of many AI models. The increasing complexity of AI systems, especially those based on neural networks and deep learning, poses significant challenges to transparency and explainability. While these systems can deliver highly accurate predictions, their decision-making processes often remain opaque, making it difficult to understand how they arrive at specific outcomes and decisions (EIOPA, 2021b). This black-box dimension of some AI systems limits the effectiveness of traditional ex-ante model risk management measures. It therefore increasingly requires financial firms to assess model outcomes, in particular by implementing fairness metrics (Giudici and Raffinetti, 2023) to evaluate AI systems for potential biases that could unfairly disadvantage certain groups.

Furthermore, consumers, as well as regulators, may find it challenging to understand the reasoning behind AI-driven decisions, especially in areas like credit scoring, insurance pricing and investment recommendations. Without transparent explanations, consumers have limited recourse to either disputing decisions or knowing what they need to do to improve their behaviour to have access to products. This ultimately undermines trust in AI-driven financial services. Financial firms are encouraged to adopt explainable AI models to ensure that consumers and regulators understand how decisions are made. Firms should be able to provide comprehensive explanations about the inherent functioning of their AI systems to supervisors and auditors. Consumers should be informed that they are interacting with an AI system or that an AI system has influence on a decision that has a material impact on them. This information should be provided by using simple clear non-technical language to allow consumers to make informed decisions.

It can, however, also be argued that the automation of certain decisions and processes powered by AI systems increases transparency and explainability. The automation of decisions previously made by humans is now more transparent because the digital trail of data and methodologies used in these decisions is more readily available for review and replication. For example, in the area of insurance and claims management, the decision to accept or reject an insurance claim has traditionally been made by claims handlers of the insurance undertaking, and potential prejudices that these individuals could have are left undetected. This would be more difficult if the decision were automated by means of an (explainable) AI system with predefined and duly traceable / documented parameters and inputs. As is discussed in this section of the e-book, some scientific contributions on AI establish that digital footprints can be an incredibly rich source of consumer default prediction, meaning that it is very likely that the data could have crucial relevance in insurance decisions too.

Clear accountability is also required as AI systems often involve complex decision chains, with contributions from various parties, including third-party vendors and data providers, making it difficult to assign responsibility for errors or harm. Financial firms and their boards must develop accountability structures to ensure proper AI governance and assign responsibility in each stage of the AI lifecycle to prevent harm and uphold ethical standards, and guarantee complaint and redress mechanisms. Such an approach fosters transparency, ensures that mistakes are rectified and ultimately increases consumer trust in AI-driven financial services.

AI technology also poses several ethical risks, primarily related to its enormous environmental impact, as is documented in this volume by Sciascia (2024). Training and deploying AI models, especially large-scale machine learning systems, consumes significant amounts of computational power, leading to high energy and water use and causing high carbon emissions. The finance sector, which is driven by high-frequency trading and complex risk modelling, is a heavy user of such AI systems. For instance, machine learning models used in algorithmic trading analyse vast datasets in real time, requiring continuous processing power and increasing the carbon footprint of the sector.

As is addressed in this volume by our colleagues at ESMA, another risk to general social welfare (this risk may also be characterised as ethical) is related to the potential destabilising impact AI can have on financial markets. AI systems, particularly those used in high-frequency trading, can contribute to market volatility, as they can react to market data faster than human traders. This speed can lead to flash crashes, as has been seen in past cases in which automated trading systems triggered rapid market sell-offs, which may in turn sow the seeds for large market panic.

In conclusion, given these risks associated with AI, embedding ethical considerations in AI development[1] and strengthening consumer protection measures are necessary to promote responsible AI use. Regulatory frameworks (such as the AI Act. See the contribution in this volume by Almada) and codes of ethics

1 To engage further in this discussion, including on the absence of ethical neutrality of AI, see for example 'Ethical implications of using AI and ML in the financial industry,' BIS Innovation Summit 2023, 21-22 March 2023. Available here.

(which have mushroomed in recent years – Munn, 2023), robust industry governance structures and collaborative efforts are essential to address these challenges and ensure that AI serves the broader interests of consumers, society and the financial system. As AI technology continues to advance, financial firms and regulators must remain attentive to the risks and foster a fair, sustainable and consumer-focused approach in the finance sector. In this context, AI even has the potential to "enhance the financial sector's accountability and public trust" (Wang, 2024) and can become a tool not just for operational efficiency but also to strengthen trust between financial institutions and the public.

References

BEUC. (2020). Artificial Intelligence: what consumers say. *BEUC - The European Consumer Organisation*. Report. Available here.

EIOPA. (2021a). Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector. 17 June 2021. *A report from EIOPA's Consultative Expert Group*. Available here.

EIOPA. (2021b). Artificial intelligence governance principles: Towards ethical and trustworthy artificial intelligence in the European insurance sector. *A report from EIOPA's Consultative Expert Group on Digital Ethics in Insurance*. Available here.

EIOPA. (2023). Supervisory statement on differential pricing practices in non-life insurance lines of business. *Consumer Protection Department*. EIOPA-BoS-23/076. Available here.

Giudici P. and Raffinetti E. (2023). SAFE Artificial Intelligence in finance. *Finance Research Letters*. Volume 56, September 2023, Elsevier. Available here.

Mogaji E. and Jain V. (2024). How generative AI is (will) change consumer behaviour: Postulating the potential impact and implications for research, practice, and policy. *Journal of consumer behaviour*. Available here.

Munn L. (2023). The Usefulness of AI ethics. *AI and Ethics*. Volume 3, pages 869-877. Available here.

Orwat C. (2020). Risks of Discrimination through the Use of Algorithms. *Federal Anti-Discrimination Agency, Germany*. Available here.

Wang Y. (2024). Ethical considerations of AI in financial decision. *Computing and Artificial Intelligence*, 2024; 2(1): 1290. Available here.

Conclusions

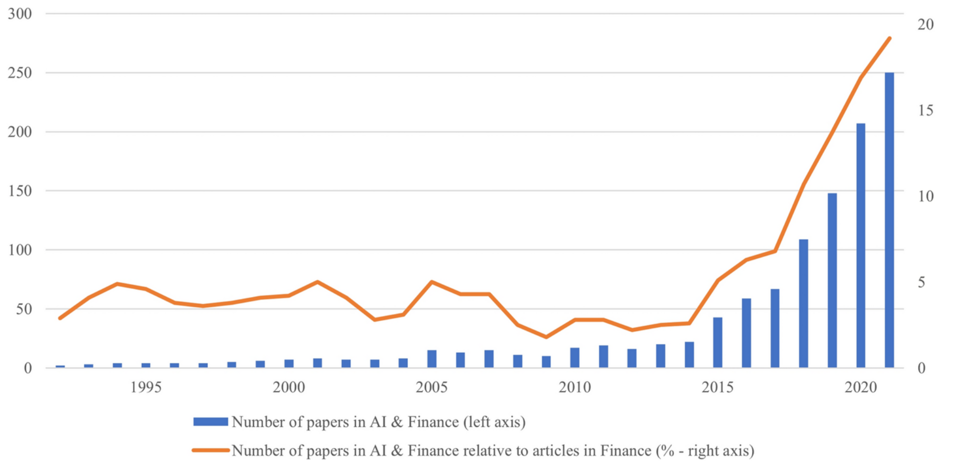
Pierre Schlosser

Florence School of Banking and Finance, European University Institute

The present e-book has covered a diversity of topics, perspectives and crucial dimensions of digital finance. It has taken stock of market development of innovation both in terms of new products and business models in the financial sector, including distributed ledger technologies, and in terms of regulatory initiatives. It has assessed ethical considerations related to the uptake of artificial intelligence (AI) technologies in finance, discussed the huge potential opportunities for real-life applications of AI technologies – not just in finance but also in financial supervision – and walked us through the risks that AI is posing to supervisors. The various contributions have provided us with a *tour d'horizon* that gives the reader the latest knowledge in the field. Equally, the authors have helped us consider technological developments in finance with both enthusiasm and critical sense.

Overall, this work has also contributed to the emerging literature – in terms of both policy and research publications – in the field of AI and finance. Bahoo et al. (2024) document a drastically increasing – and potentially exponential – trend of publications on AI and finance in particular since 2018.

Figure 1: Yearly incidence of academic papers focusing on AI and Finance



(Source: Bahoo et al. 2024)

According to Bahoo et al. (2024) AI applications fall in 10 categories: "stock market, trading models, volatility forecasting, portfolio management, performance, risk and default evaluation, cryptocurrencies, derivatives, credit risk in banks, investor sentiment analysis and foreign exchange management." Our e-book has looked at selected aspects of these categories.

While it is beyond the scope of this concluding section to exhaustively summarise each contribution, I would like to focus these concluding remarks on a few selected transversal issues that have come up in many if not all the chapters and situate them in a critical perspective of the limitations of AI. I will end with some considerations on current open questions related to AI.

Consider first the risks in AI application. Three risks are usually singled out: the general increase in cyber risk vulnerability that will accompany widespread use of AI; the rather alarming implications of an opaque use of AI in credit risk scoring and its discriminatory potential; and last but not least the use of AI in life insurance assessment and its adverse selection potential. Moreover, several of the contributions also mention that when looking upstream at AI development and its capacities, there are only a few large actors at the frontier. These are all large companies (because of the need for economies of scale) and based in the United States. For an idea of what we can anticipate in the future in terms of counterparty risk due to over-high exposure to market concentration, one can simply think of the Crowdstrike incident. On 19 July 2024 a software update of Crowdstrike, an external cyber provider of Microsoft, led to a global IT outage that impacted all types of public and private actors (including financial actors) and led to a globally widespread airport shutdown.

A second important dimension cutting across all the contributions is the centrality of regulation. Regulating new technologies is essential to ensure that certainty is provided to all marketplace participants – the (in)famous level playing field – and to safeguard the interests of consumers by preventing technologies leading to all sorts of possible abuses. However, regulation ought to also be as light as possible and as technology-neutral as is feasible to ensure that innovation in all forms is encouraged. As the Draghi Report (Draghi, 2024) outlines, Europe is still struggling to find the right balance in developing regulatory frameworks that also encourage innovation.

A third and last issue that I consider important to recall is the strategic relevance of technology in empowering banking, insurance and financial market supervisors to carry out their mandates going forward. One can predict myriad new applications in the coming decade. For now, we have a series of new use cases in the testing stage and all BIS members surveyed report at least one Suptech tool being deployed (BIS, 2024a). However, given the number of Suptech projects in the pipeline, it is fair to assume that so far we have only seen the tip of the iceberg of SupTech development. Regarding supervision risks, however, it is likely that we are only at the beginning of a journey judging by some calls made for a "technoprudential approach" (BIS, 2024b). This derives from the limitations and blind spots of AI, to which we will now turn briefly.

Over recent years scholars and analysts alike have investigated the limits of AI, an issue sometimes also described as the fallacies of AI, or what Barassi (2024) coined a "theory of AI errors." This trend is based on the acknowledgement that AI, and in particular generative AI, in addition to the various bias risks and limits already pointed out in this volume by all the contributors, on occasions can also be genuinely dumb, or to put it more elegantly "cluelessly clueless" (Hofstadter cited in Brooks, 2023). After all, AI "doesn't possess understanding, self-awareness, concepts, emotions, desires, a body or biology. It's bad at causal thinking. It doesn't possess the nonverbal, tacit knowledge that humans take for granted" (Brooks, 2023). However, we are all witnesses to the huge improvements that AI and AI applications have made in recent years and would be foolish to consider that AI will not in the future manage to minimise many of its limitations and mistakes through deep learning. This source of tension will remain with us for quite some time.

In this context it would be presumptuous to come up with firm conclusions on such an overwhelming topic. Let me, therefore, more realistically ask: what are the questions one is left with, after going through the stimulating contributions by the authors of this volume?

The development of new technologies and their applications in finance will push all organisations, public and private, out of their comfort zone. They will notably need to rethink the way they collaborate with outside actors. The simple reason for this is that most organisations will not be able to compete for the best AI talents and will therefore need to access this knowledge by buying or borrowing AI products and services or by relying on contracted external human resources. One consequence will be stronger collaboration along the AI value chain, both upstream and downstream. Another consequence will be a need for private and public actors to collaborate more with each other. One can see this already in academia, where large AI players have developed close links with universities in their quest for talent. This development will require a culture change on both sides. Do public actors of all sizes understand that fully embracing the potential and risks of AI will also mean working more closely with outside players?

Related to these public-private dynamics, it is safe to assume that over the next decade or so the largest AI developers will still be U.S. and China-based. According to a recent Bruegel analysis, only 6% of the 35 billion USD invested globally in AI start-ups in H1 2024 went to EU-based firms (Martens, 2024). If this trend were to continue, which is likely, it would lead to greater "dependency risks" (DNB, 2024). Besides developing a strong regulatory and supervisory arsenal, what is Europe doing to counteract or indeed mitigate these dependency risks? A first answer is the strategic discussion on 'sovereign AI.' This debate has recently started in Europe and, besides the industrial policy logic behind it, is largely driven by a concern to keep European data in Europe, under the roof of European data-protection laws.

As Deputy Director of an executive education school, I cannot resist providing a few personal remarks – in closing – on the impact of AI on the world of education. More specifically, what is the role of lifelong learning in leading us to a world of AI? There are indeed few areas like AI in which the case for lifelong learning, i.e. targeted education initiatives for adults/professionals, is highly compelling. AI technologies strongly disrupt the way we have learned to do things. To be fully embraced, the take-up of AI technologies ought to be accompanied by a large-scale parallel training effort for an entire generation of adults. We all need to learn what AI is in the first place, how it works and what it can do for us. It is also very likely that to learn the last of these we will need to unlearn some of what we were originally taught in school and make space in our brains for new knowledge and ways of thinking. For some of us this paradigm shift might also mean eliminating some forms of anti-technology bias.

However, collectively we will need to get there. Lifelong education on AI could be a way to strengthen the position of humans, making them stronger vis-à-vis AI, i.e. to develop "one's personal strength to control a device rather than being remote controlled by it" (Gigerenzer, 2022). Embracing the implications of this recommendation would obviously go beyond lifelong education. It might result in coding being considered a genuine language that children ought to become proficient with at the earliest possible age in school. This would be not just in a logic of digitalising our societies for the mere sake of it, but rather with a broader aim of empowerment. Empowerment that I hope will lead us to embrace AI but with sharp critical sense. Only then will we be in a position to make the most of its potential without harming our fellow citizens. We are very proud, at the Florence School of Banking and Finance (EUI), to contribute to this wider empowerment effort through our training courses, of which every year a handful are now focused on AI.

References

Bahoo et al. (2024). Artificial intelligence in Finance: a comprehensive review through bibliometric and content analysis. *SN Business & Economics*. Volume 4, article number 23. Available here.

Barassi (2024). Toward a Theory of AI Errors: Making Sense of Hallucinations, Catastrophic Failures, and the Fallacy of Generative AI. *Harvard Data Science Review, (Special Issue 5) Grappling With the Generative AI Revolution*. Available here.

BIS (2024a). Peering through the hype – assessing suptech tools' transition from experimentation to supervision. *FSI Insights on policy implementation No 58*. Available here.

BIS (2024b). Managing AI in banking: are we ready to cooperate? *Speech by Pablo Hernández de Cos*. 17 April 2024. Available here.

Brooks (2023). Human Beings Are Soon Going to Be Eclipsed. *The New York Times*. 13 July 2023. Available here.

DNB (2024). The impact of AI on the financial sector and supervision. *De Nederlandsche Bank*. Available here.

Draghi M. (2024). The future of European competitiveness. *European Commission*. Available here.

ECB (2024). The rise of artificial intelligence: benefits and risks for financial stability. *Financial Stability Review*, May 2024. Available here.

Gigerenzer (2022). Staying Smart in a Smart World: A Conversation with Gerd Gigerenzer. *Behavioral scientist*. Available here.

Martens (2024). Catch-up with the US or prosper below the tech frontier? An EU artificial intelligence strategy. *Bruegel*. Available here.

Publications Office
of the European Union

ISBN: 978-92-9466-637-6
doi: 10.2870/8600400
QN: QM-01-24-186-EN-N

Funded by
the European Union