PRE-PRINT
AUG '24

AI Governance in Algorithmic Trading: Some Regulatory Insights from the EU AI Act

Alessio Azzutti*

27 August 2024

Abstract

The frenzied race toward Artificial Intelligence (AI) adoption is causing profound transformations within the financial sector, rendering capital markets an increasingly complex system. These dramatic and sweeping changes are most pronounced in data-intensive and high-performance computing domains, such as algorithmic trading. While AI-powered trading offers numerous benefits to financial firms, markets, and society, it also raises significant concerns regarding potential risks to market quality, integrity, and stability. Recent studies underscore the dangers posed by AI advancements, particularly when not accompanied by robust governance and regulatory frameworks, which could lead to new and heightened risks of market abuse. Amidst this risk-prone environment, there is growing recognition among policymakers and financial regulators of the pressing need to regulate AI deployment. This emerging awareness is crucial, as effective AI governance is essential to ensure that the benefits of technological innovation are not overshadowed by its inherent risks. In this very direction, the EU AI Act stands out as a landmark effort in establishing comprehensive AI regulation. Hence, this Article critically examines this fundamental piece of (global) legislation and compares it to sectoral regulation on algorithmic trading. By focusing on key legal provisions, the analysis demonstrates the potential superiority of the EU AI Act's regulatory requirements for providers of "high-risk" AI systems over those for deployers of algorithmic trading systems under MiFID II. The Article concludes with some ideas for future risk-based regulation of AI applications in financial trading.

Keywords: Artificial Intelligence, Algorithmic Trading, Financial Regulation, AI Regulation and Governance; MiFID II; EU AI Act.

* Lecturer in Law & Technology (FinTech) at Glasgow University; Visiting Researcher at the Faculty of Law, The University of Hong Kong. Contact the author at: Alessio.Azzutti@glasgow.ac.uk. I thank Prof. Cheng-Yun (CY) Tsang, Prof. Virginia Torries, Prof. Iain MacNeil, Prof. H. Siegfried Stiehl, and Prof. Giuliano Castellano for their valuable feedback on early drafts of this Article. I also express my sincere appreciation to Prof. Douglas Arner for his support and guidance during my one-month research visit at the University of Hong Kong, Faculty of Law, during which I worked on earlier versions of this Article. Finally, I extend my gratitude to Jacob Yunger and other colleagues at the Financial Industry Regulatory Authority (FINRA) for insightful discussions on the challenges of financial AI applications for capital market integrity. None of them shall be held responsible for any opinion expressed herein. All mistakes are my own.

1. INTRODUCTION

Financial regulators are increasingly concerned about the potential negative effects of inadequately regulated Artificial Intelligence[1] (AI) adoption in financial markets.[2] Numerous initiatives over the past year alone underscore these concerns. In some jurisdictions, legislators are discussing the need for additional regulations for financial AI systems.[3] For instance, following the adoption of the *European Union's Artificial Intelligence Act* (EU AI Act)[4], the European Commission has engaged industry stakeholders in a consultation to better understand AI use cases in finance, their risks to market integrity and stability, and the scope of relevant laws and regulations.[5] Similarly, certain sectoral regulators have solicited public comments to gather insights on how best to regulate AI applications in financial markets.[6] Some authorities have made public statements to raise awareness of AI risks,[7] while others have published recommendations to promote responsible AI development and deployment within the industry.[8] Although primarily focused on consumer-facing financial services, industry regulators like the US Securities and Exchange Commission (SEC) have proposed new rules for AI.[9] Moreover, some financial regulators, such as the UK Financial Conduct Authority (FCA), are fostering collaboration with industry stakeholders to discover innovative solutions for market conduct supervision, including organizing

[1] In the present work, the term "AI" generally refers to the scientific field and engineering practices aimed at creating computational systems — particularly software — designed to perform tasks that typically require human intelligence. See Michael Veale, Kira Matus, and Robert Gorwa, "AI and Global Governance: Modalities, Rationales, Tensions" (2023) 19 Annual Review of Law and Social Science 255 at 256.

[2] The Financial Stability Board's 2017 report is the first documents published by a financial authority addressing the risks introduced by advances in AI. See FSB, "Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications" (1 November 2017), online: *FSB* <https://www.fsb.org/wp-content/uploads/P011117.pdf>.

[3] Among the latest developments, the U.S. Congress has put forward amendments to the Financial Stability Act of 2010 that would grant the Financial Stability Oversight Council new oversight duties regarding AI. See S.3554 – 118th Congress (2023-2024): FAIRR Act, s.3554, online: *118th Cong. (2023)* <https://www.congress.gov/bill/118th-congress/senate-bill/3554>.

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L.

[5] EU Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, "Consultation Document: Targeted Consultation on Artificial Intelligence in the Financial Sector" (18 June 2024), online: <https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/targeted-consultation-artificial-intelligence-financial-sector_en> [EU Commission].

[6] See, e.g., U.S. CFTC, "CFTC Staff Releases Request for Comment on the Use of Artificial Intelligence in CFTC-Regulated Markets" (25 January 2024) Release No. 8853-24, online: <https://www.cftc.gov/PressRoom/PressReleases/8853-24>.

[7] See ESMA, "Public Statement: On the Use of Artificial Intelligence (AI) in the Provision of Retail Investment Services" (30 May 2024), online: *ESMA35-335435667-5924* <https://www.esma.europa.eu/sites/default/files/2024-05/ESMA35-335435667-5924__Public_Statement_on_AI_and_investment_services.pdf>.

[8] See, e.g., U.S. CFTC, "Responsible Artificial Intelligence in Financial Markets: Opportunities, Risks & Recommendations" (2 May 2024), online: *A Report of the Subcommittee on emerging and Evolving Technologies, Technology Advisory Committee of the U.S. Commodity Futures Trading Commission* <https://www.cftc.gov/media/10626/TAC_AIReport050224/download>.

[9] See, e.g., U.S. SEC, Proposed Rule, "Conflict of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Adviser", Exchange Act Release No. 97990, File No. S7-12-23.

TechSprints and other initiatives.[10] Others, like the Financial Industry Regulatory Authority (FINRA) in the US, are more directly investing in AI and related technologies to enhance their market surveillance capabilities.[11] Despite all these efforts, regulatory reforms have yet to materialize.

To be fair, the concrete threats that AI, particularly its subfield of Machine Learning (ML) methods, pose to the fair and orderly functioning of financial markets are still relatively underexplored and poorly understood. Except for a few explorative studies, the legal scholarship has yet to substantiate many of these risks.[12] To advance the scientific debate in this field and place it within the context of emerging regulatory initiative on AI governance, the rest of this Article is structured into four sections.

Section II examines how advancements in AI research and its application to financial trading can be conceptually traced to three successive AI generations. Each of these generations is marked by increasing “technological complexity”[13], which, in turn, contributes to the overall growing “complexity” of capital markets as a system. To illustrate the additional uncertainties and regulatory concerns stemming from these technology-led developments, Section III addresses the new and heightened risks of market manipulation associated with the latest AI generations. Furthermore, commenting on the widening gap between law and technology, it highlights the limitations of current EU regulatory frameworks and enforcement regimes in ensuring effective AI governance in this domain. Acknowledging the growing challenges in regulating AI in algorithmic trading, Section IV explores emerging AI regulations, specifically focusing on the recently adopted EU AI Act. By comparing regulatory requirements for algorithmic trading with those for “high-risk” AI applications, this section contrasts sectoral regulation and AI regulation and highlights the greater prescriptiveness of the latter. Drawing from the EU AI Act’s risk-based regulatory framework, the Article advocates for a fractal replication of this approach within the

[10] See U.K. FCA, “TechSprints” (18 March 2024), online: *FCA* <https://www.fca.org.uk/firms/innovation/techsprints>.

[11] See, e.g., FINRA, “Deep Learning: The Future of the Market Manipulation Surveillance Program” (28 May 2024) online: *Youtube*, <https://www.youtube.com/watch?v=QlsVMTK2L8E>.

[12] This research *lacuna* is particularly evident in the legal literature. Although there is a substantial body of research on algorithmic trading and its regulation, many of these studies lack sufficient depth and understanding of AI, particularly it subfield of ML. Notable exceptions include: Alessio Azzutti, Wolf-Georg Ringe, Siegfried Stiehl, “Machine Learning, ‘Market Manipulation, and Collusion on Capital Markets: Why the “Black Box” Matters” (2021) 43:1 University of Pennsylvania Journal of International Law 79 [Azzutti, Ringe, and Stiehl I]; Alessio Azzutti, “AI Trading and the Limits of EU Law Enforcement in Deterring Market Manipulation” (2022) 45 Computer Law & Security Review, Article No. 105690 [Azzutti I]; Alessio Azzutti, “The Algorithmic Future of EU Market Conduct Supervision: A Preliminary Check”, in Lukas Böffel and Jonas Schürger, eds, *Digitalisation, Sustainability, and the Banking and Capital Markets Union: Thoughts on Current Issues of EU Financial Regulation* (Palgrave Macmillan, 2023) at 53-98 <https://doi.org/10.1007/978-3-031-17077-5_2> [Azzutti II]; Alessio Azzutti, Wolf-Georg Ringe, and H. Siegfried Stiehl, “Regulating AI trading from an AI lifecycle perspective”, in Nydia Remolina and Aurelio Gurrea-Martinez, eds, *Artificial Intelligence in Finance: Challenges, Opportunities and Regulatory Developments* (Edward Elgar Publishing, 2023) at 198-242 <https://doi.org/10.4337/9781803926179.00019> [Azzutti, Ringe, and Stiehl II].

[13] The term refers to the tendency of technological systems to become increasingly complex over time. This is mainly due to (i) each generation building upon the socio-technological environment of previous ones, (ii) the growing range of technological capabilities, and (iii) the increasing interdependence among multiple technologies, leading to greater system sophistication. See, e.g., Tom Broekel, “Measuring Technological Complexity – Current Approaches and a New Measure of Structural Complexity” (2018) arXiv preprint 1 at 7-9.

domain of algorithmic trading. Eventually, Section V concludes by summarizing the key findings.

2. AI-POWERED TRADING: A PRIMER

The adoption of innovative technologies such as AI, especially among the most resource-equipped market participants, is a major cause of the increasing overall complexity of capital markets.[14] This section aims to shed light on the disruptive impact of AI in capital markets and its broader effect on the economy and society. It does so by exploring the three main stages of AI in financial trading (or AI generations), characterized by progressively more "intelligent" machines.[15] These AI generations have evolved from the mere automation of tasks within the trading cycle to the employment of advanced ML methods that support — and may soon fully replace — the work and judgment of human experts.[16] This analysis enables us to conceptualize how the various stages of AI adoption underpin increasing technological and market complexity in the financial trading domain, which has substantial implications for financial regulation and technology governance in this area.

(a) AI Generations In Financial Trading: From Early Days Automated Trading To Augmented Financial Intelligence

The financial industry is historically one of the most technologically innovative sectors.[17] Since the 1980s, the gradual shift from the old-fashioned "open outcry" model to electronic trading and computerized matching engines has paved the way for future developments in algorithmic trading, undoubtedly a pioneering application of AI in the economy.[18] Human experts and the financial organizations they work for have been leveraging AI and related technologies to automate and seek to optimize various tasks within the trading cycle. AI applications help improve financial decision-making across all stages, from the collection and analysis of relevant financial data to signal generation, selection of optimal trading strategies, order routing and execution, and post-trade analysis.[19]

---

[14] See, e.g., Azzutti, Ringe, and Stiehl II, *supra* note 12 at 202; Scott James and Lucia Quaglia, "Emergent Regime Complexity and Epistemic Barriers in 'Bigtech' Finance" (2024) *New Political Economy* 1, however examining these issues with a focus on the interplay between BigTech and finance.

[15] Although AI systems are capable of performing tasks that typically require cognitive abilities, they lack the fundamental essence of human intelligence. For a discussion, see Gerhard Paaß and Dirk Hecker, *Artificial Intelligence: What Is behind the Technology of the Future?* (Springer, 2024) at 1-13.

[16] See, e.g., Anna-Helena Mihov, Nick Firoozye, and Philip Treleaven, "Towards Augmented Financial Intelligence" (2022) SSRN preprint 1 [Mihov, Firoozye, and Treleaven].

[17] Douglas W. Arner, Janos Barberis, and Ross P. Buckley, "The Evolution of FinTech: A New Post-Crisis Paradigm" (2015) 47:4 Georgetown Journal of International Law 1271 at 1274-1283 (providing a chronicle of the intertwined relationship between finance and technology according to the tree main FinTech eras).

[18] David Cliff, Dan Brown, and Philip Treleaven, "Technology Trends in the Financial Markets: A 2020 Vision" (2011), online (pdf): *UK Government Office for Science* <https://assets.publishing.service.gov.uk/media/5a7c277eed915d1b3a307c4a/11-1222-dr3-technology-trends-in-financial-markets.pdf> at 5-7.

[19] See Fethi A. Rahbi, Nkolay Mehandjiev, and Ali Baghdadi, "State-of-the-Art in Applying Machine Learning to Electronic Trading", in Benjamin Clapman and Jascha-Alexander Koch, eds, *Enterprise Applications, Markets and Services in the Finance Industry*, vol 401, 1st ed. (Springer, 2020) at 3-20.

The past few decades have witnessed a rapid growth in sophisticated, high-performance AI trading systems, enabled by parallel advances in AI research, technological capability (e.g., in terms of computing power and data storage), and related ICT infrastructures.[20] *Table 1* below visually outlines the chronological development of the three main generations of AI in financial trading, namely (*i*) "*Good Old-Fashioned AI*" (GOFAI), (*ii*) the "*first ML era*", and (*iii*) "*Deep Computational Finance*"[21] While not scientifically perfect, the proposed taxonomy at least aims to provide a conceptual framework for understanding basic concepts of AI methods and applications in their progression to present days.

***Table 1*: The three "AI generations" in financial trading**

AI Generation	Time Period*	AI Methods	Examples
"GOFAI"	From 1980 ca.	"Symbolic AI" or "deterministic AI" methods	Rule-based, expert systems
"First ML era"	From 2000 ca.	"Conventional ML" methods	Supervised learning: statistical models (e.g., regression), decision trees; unsupervised learning: statistical methods (i.e. clustering); Reinforcement learning
"Deep Computational Finance"	From 2010 ca.	"Deep learning" and other advanced ML methods	Neural networks, deep reinforcement learning, generative AI models, and other innovative models

* As reflected in publicly available research on Computational Finance. Actual implementation by financial firms may be delayed.

[20] Azzutti, Ringe, and Stiehl II, *supra* note 12 at 203.

[21] The proposed taxonomy is based on extensive literature review in Computational Finance conducted by the author within his Doctoral research project. The author successfully defended his Doctoral dissertation, "Artificial Intelligence and Market Manipulation: Challenges for Market Abuse Regulation and Governance of Algorithmic Trading", with honours (*cum laude*) at the University of Hamburg in Hamburg (Germany) on 20 June 2024.

(i) "GOFAI"

The term GOFAI refers — somewhat nostalgically — to early applications of "Symbolic AI" or "deterministic AI". These algorithmic problem-solving systems were based on the explicit embedding of domain knowledge and assumptions into computer programs by human experts.[22]

Operating on the basis of "if/then" rules, these early AI systems assisted human traders in automating tasks and processes according to pre-defined commands and strategies.[23] These systems typically generate outputs (e.g., datasets, predictions, recommendations, graphs, etc.) from financial and other relevant data. When directly integrated into algorithmic trading, for instance, they can be programmed to buy or sell assets when certain market conditions are met ("trade execution"), or to route orders to various exchanges or liquidity providers to ensure cost-effective and efficient trading ("order routing").[24]

Due to their inherent techno-methodical limitations, early AI-powered trading systems often struggled to adapt to the dynamic and unpredictable statistical properties of financial markets.[25] Despite these limitations, this first generation of algorithmic trading undoubtedly revolutionized capital markets, making them faster, more interconnected, and potentially more efficient. At the same time, however, it also introduced new risks, which led policymakers and financial regulators to adopt specific regulatory frameworks and reform market abuse regulations.

(ii) The "first ML era"

Advances in ML and data science R&D have enabled the unfolding of the second AI generation.[26] Unlike GOFAI, ML methods entail the creation of computer programs that employ algorithms to process empirical data in order to optimize a mathematical function pre-set by human experts.[27]

ML-based systems can augment human cognitive abilities and support financial decision-making. Their performance, however, closely depends on the availability of vast amounts of high-quality data relevant to the problem at hand, which may also be acquired from multiple sources.[28] In cases where input data is not sufficient in volume, synthetic data might also be used. Regardless of this, it is paramount to ensure that training data is of the utmost quality (e.g., accurate, valid, and statistically representative).[29] Another main techno-methodical limitation of ML systems is their tendency to operate as "black boxes".[30] In "high-stake" application domains like

[22] The term GOFAI is attributed to contemporary philosopher John Haugeland. See John Haugeland, *Artificial Intelligence: The Very Idea* (The MIT Press, 1989) at 112-121.

[23] Roy S. Freedman, "AI on Wall Street" (1991) 6:2 *IEEE Intelligent Systems* 3, <https://doi.org/10.1109/64.79702>.

[24] See, e.g., Philip Treleaven, Michal Galas, and Vidhi Lalchand, "Algorithmic Trading Review" (2013) 56:11 *Communications of the ACM* 76.

[25] See, e.g., Bonnie G. Buchanan, "Artificial Intelligence in Finance" (27 March 2019), online (pdf): *The Alan Turing Institute 2019* <https://zenodo.org/records/2612537> at 4-5.

[26] See, e.g., Christian Borch and Bo Hee Min, "Machine Learning and social Action in Markets: From First- to Second-Generation Automated Trading" (2023) 52:1 *Economy and Society* 37,

[27] For an introduction to ML applied to financial trading, see Azzutti, Ringe, and Stiehl I, *supra* note 12 at 86-92.

[28] See, e.g., Azzutti, Ringe, and Stiehl II, *supra* note 12 at 219.

[29] *Ibid*. at 220.

[30] In financial trading, the "black box" problem refers to AI systems whose internal workings are not visible or understandable by human experts, including the AI developers and human traders. This

financial trading, opacity in ML raises substantial issues of accountability and liability in cases of errors, misconduct, and resulting harm to third parties. Among other things, ensuring adequate levels of transparency, human agency and control is therefore deemed necessary for the trustworthy adoption of ML.[31]

ML financial applications encompass a highly diverse and heterogeneous category of computational methods grounded in mathematics that may involve different modes of human involvement.[32] In "*supervised learning*" (SL), ML models learn to generalize a function that maps input to output data pre-labelled by human experts. An SL trading algorithm, for instance, can learn from financial data (e.g., price time series, technical indicators, etc.) to forecast or classify data points, which can be used for subsequent trading decisions.[33] In contrast, "*unsupervised learning*" (UL) involves ML models performing clustering tasks without requiring labeled data from human experts. Within a given system, SL and UL methods can be complementarily integrated at various stages of the trading cycle to leverage the benefits of both approaches.[34]

"*Reinforcement learning*" (RL) represents the third main ML paradigm, which has a broad scope of application in financial trading. This class of ML methods deserves particular attention. In essence, RL enables the creation of software agents that achieve pre-defined goals in a given environment by learning from feedback on their actions (i.e. rewards and punishments). Through "trial and error", RL agents "explore" different strategies and "exploit" the best ones to maximize rewards.[35] In financial trading, RL methods can optimize narrow tasks, such as best execution or order routing, or be employed to research end-to-end trading systems (i.e. "artificial trading agents").[36]

With the advent of the first ML era, technological complexity has increased. AI trading systems must thus be regarded as complex ecosystems of algorithms capable of handling a growing number of tasks.[37] As these systems become more sophisticated, their trustworthy adoption requires appropriate governance throughout the entire AI lifecycle.

(iii) "Deep Computational Finance"

The latest AI generation in financial trading applications has been referred to as "Deep Computational Finance",[38] which is an umbrella term encompasses a vast and ever-expanding range of advanced applications based on deep learning and other innovative ML methods.[39] Some of the most attention-grabbing innovations in this space include "*deep reinforcement learning*" (DRL) and the most recent AI subfield of Generative AI (GenAI) methods.

---

makes it difficult to interpret how a given trading decisions has been generated. See Azzutti, Ringe, and Stiehl I, *supra* note 12 at 90.

[31] See, e.g., Azzutti, Ringe, and Stiehl II, *supra* note 12 at 221-222.

[32] *Ibid*. at 204.

[33] See, e.g., Azzutti, Ringe, and Stiehl I, *supra* note 12 at 86.

[34] *Ibid*.

[35] See *ibid*. at 88.

[36] See *ibid*. at 89.

[37] E.g., Azzutti I, *supra* note 12 at 4.

[38] Azzutti, Ringe, and Stiehl II, *supra* note 12 at 218.

[39] For an overview of the various ML methods and their respective applications for various tasks in financial trading and beyond, see Longbing Cao, "AI in Finance: Challenges, Techniques, and Opportunities" (2022) 55:3 ACM Computing Surveys, Article No. 64.

DRL methods enable human experts to research artificial trading agents able to overcome many of the techno-methodical limitations that plague other ML methods.[40] By combining the upsides of deep *and* reinforcement learning, DRL agents are capable of (i) identifying profitable trading opportunities and strategies through deep learning by processing vast datasets across several assets and trading venues, and (ii) experiment and dynamically learn optimal trading decisions through RL to achieve pre-defined business goals — most likely some profit-maximization function under risk control.[41] Despite their potential, a number of techno-methodical challenges remains to ensure trustworthy DRL application due to the inherent difficulty of dealing with the behavior of capital markets.[42]

As the latest breakthroughs in the AI field, the advent and improvement of "*Transformer architectures*"[43] have led to the emergence of GenAI methods, particularly "*Large Language Models*" (LLMs) and "*Foundation models*",[44] which hold potential for a wide range of applications. In the first place, LLMs can be employed by human experts in writing programming code (e.g., in Python) for developing trading software.[45] More importantly, numerous research projects are currently focused on leveraging GenAI to support financial decision-making. An important distinction exists between proprietary models, such as Bloomberg's BloombergGPT,[46] and open-source models. Many initiatives in the latter category involve adapting — e.g., via fine-tuning — generic pretrained models such as "*Generative Pretrained Transformers*" (GPT) *à la* ChatGPT.[47] In addition, GenAI models can be categorized based on their data processing modalities into two main types. Unimodal models can process only a single type or dimension of data (e.g., text),[48] while multimodal models can handle multiple data formats, such as text, numerical data, and images.[49] In practical applications, GenAI may be used for financial forecasting and trading signal generation based on

---

[40] For an introduction to DRL-based methods in financial trading, see Azzutti, Ringe, and Stiehl I, *supra* note 12 at 90-92.

[41] *Ibid*.

[42] See *ibid*. at 92-94.

[43] See Ashish Vaswani et al., "Attention Is All You Need" (2017) online (arXiv): *31st Conference on Neural Information Processing Systems (NIPS 2017), Long Beach, CA, USA*.

[44] For a definition of LLMs and Foundation model, see Helen Toner, "What Are Generative AI, Large Language Models, and Foundation Models?" (12 May 2023), online: *Center for Security and Emerging Technology* <https://cset.georgetown.edu/article/what-are-generative-ai-large-language-models-and-foundation-models>.

[45] Miquel Noguer i Alondo and Hanane Dupouy, "Evaluating LLMs in Financial Tasks – Code Generation in Trading Strategies" (2024) SSRN preprint 1; but see Samia Kabir et al., "Is Stack Overflow Obsolete? An Empirical Study of the Characteristics of ChatGPT Answers to Stack Overflow Questions", in Florian Floyd Mueller et al., eds, *CHI '24: Proceedings of the CHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery, 2024) Article No. 935, who estimate that use of ChatGPT in programming tasks can often result in errors (in 52 percent of cases).

[46] Shijie Wu et al., "BloombergGPT: A Large Language Model for Finance" (2023) arXiv preprint 1.

[47] For instance, FinGPT is an open source LLM for various tasks in financial trading that employs RLHF to fine-tune general LLMs like ChatGPT. Hongyang (Bruce) Yang, Xiao-Yang Liu, and Christina Dan Wang, "FinGPT: Open-Source Financial Large Language Models" (2023) arXiv preprint 1.

[48] For instance, FinBERT is a LLM based on BERT for NLP financial tasks, particularly sentiment analysis. Dogu Tan Araci, "FinBERT: Financial Sentiment Analysis with Pre-trained Language Models" (2019) arXiv preprint 1.

[49] One example is FinTral, a multimodal LLMs for financial analysis which supports financial decision-making tasks. See Gagan Bhatia et al., "FinTral: A Family of GPT-4 Level Multimodal Financial Large Language Models" (2024) arXiv preprint 1.

market sentiment[50] or technical analysis[51]. More sophisticated approaches involve the creation of GenAI-based end-to-end trading agents.[52] Moreover, LLMs may help establish multi-agent frameworks to support financial decision-making,[53] which might also be integrated with artificial trading agents.[54] Like DRL, GenAI methods remain largely experimental and lack thorough scientific validation despite ongoing research to benchmark and compare applications.[55] However, experts believe GenAI could revolutionize financial research and practice in the future.[56]

Beyond mere task automation, "Deep Computational Finance" and its advanced ML methods drive additional technological complexity in capital markets, which tend to be complex anyway. These next-generation AI systems are expected to enhance human cognitive and decision-making capabilities further, opening up to a symbiotic and synergistic relationship between human experts and complex computational systems. The advent of so-called "augmented financial intelligence"[57] also introduces potential negative consequences, some of which will be explored in Section III from a market conduct perspective.

(b) AI-Induced Complexity Relevant To Capital Markets Regulation

The evolution in technological complexity punctuated by the three AI generations described above has spurred increasing levels of "complexity" in the capital markets system.[58] All this complexity, which poses great challenges for financial regulators, manifests through three interrelated dimensions: (a) the actors, (b) their market behavior, and (c) the interactions among them, which collectively determine overall system behavior.[59]

---

[50] See, e.g., Wei Luo and Dihong Gong, "Pre-trained Large Language Models for Financial Sentiment Analysis" (2024) arXiv preprint 1, who develop an LLM models adapted on pretrained LLaMa-7B with supervised fine-tuning techniques for financial sentiment analysis.

[51] For instance, BreakGPT is a LLM specifically tailored to the analysis of trading range breakouts. Kang Zhang, Osamu Yoshie, and Weiran Huang, "BreakGPT: A Large Language Model with Multi-stage Structure for Financial Breakout Detection" (2024) arXiv preprint 1.

[52] FinAgent is a multimodal foundational agent for trading able to process a diverse range of data to analyse markets. It integrates established trading strategies and human experts' insights. Wentao Zhang et al., "A Multimodal Foundation Agent for Financial Trading: Tool-Augmented, Diversified, and Generalist" (2024) arXiv preprint 1.

[53] For instance, FinRobot is an open-source AI agent platform supporting multiple specialized AI agents powered by LLM for financial analysis tasks. According to its creators, it is proposed to democratize access to AI tools and promoting wider AI adoption. Hongyang Yang et al., "FinRoboT: An Open-Source AI Agent Platform for Financial Applications using Large Language Models" (2024) arXiv preprint 1.

[54] For instance, TradingGPT is a LLM multi-agent framework suited for trading and investment. It can be used to support decision-making for artificial trading agents. Yang Li et al., "TradingGPT: Multi-Agent System with Layered Memory and Distinct Characters for Enhanced Financial Trading Performance" (2023) arXiv preprint 1.

[55] Qianqian Xie, "The FinBen: A Holistic Financial Benchmark for Large Language Models" (2024) arXiv preprint 1.

[56] Xiaolong Zhen et al., "New Paradigm for Economic and Financial Research with Generative AI: Impact and Perspective" (2024) 11:3 IEEE Transactions on Computational Social Systems 3457.

[57] Mihov, Firoozye, and Treleaven, *supra* note 16.

[58] A growing number of scholars regard "complexity" as a major challenge for the effective regulation and governance of the financial system. For an early contribution in this field, see Cheng-Yun Tsang, "Rethinking Modern Financial Ecology and Its Regulatory Implications" (2017) 32:3 Banking & Finance Law Review 461.

[59] Azzutti, Ringe, and Stiehl II, *supra* note 12 at 202.

First, AI adoption impacts the identity and composition of market participants.[60] In particular, it affects their business operations, investment priorities, and strategic vision. AI systems also emerge as new "actors" themselves,[61] as well illustrated in the case of artificial trading agents that will be discussed later. Second, AI systems alter the market behavior of their deployers. By delegating decision-making tasks to "intelligent" machines, market participants seek to optimize their trading strategies and may develop new ones.[62] As ML-powered trading systems become more advanced, autonomous, and often operate as black-boxes, they inevitably impact market behaviors in fast-paced, interconnected markets. Lastly, the interactions among market participants take on new forms, and this has a strong impact on the collective behavior of the system.[63] Actually, since the advent of algorithmic trading, new market phenomena, such as technical errors, flash crashes and other disruptions have occurred.[64] While ML methods are employed to manage and interpret market uncertainty, they simultaneously introduce their own model-related uncertainties.[65] Additionally, the widespread and sophisticated adoption of AI is likely to further redefine the spatiotemporal dimensions of market events.[66]

All the above underscores the growing difficulties in ensuring the controlled deployment of AI technology in financial markets and raise questions of liability should something go wrong. AI-spurred complexity introduces new risks to the integrity — and stability — of capital markets. Understanding the determinants of this complexity is necessary for developing innovative and effective approaches for the governance of its inherent financial and technological risks.[67] The next section elaborates on market manipulation as a case study.

3. AI, MARKET MANIPULATION, AND COLLUSION ON CAPITAL MARKETS: CHALLENGES TO CURRENT REGULATORY FRAMEWORKS

As an expression of the parallel and intertwined increase in technological and overall system complexity, new and heightened risks to market integrity emerge. Because of the *dual-use* nature of AI, its use, misuse, and abuse can result in market misconduct and harm, even apart from specific human intent.[68] On this premise, this section has two main objectives. First, it aims to conceptualize the new market manipulation scenarios made possible by the succession of the three AI generations described earlier. Second, it highlights the growing deficiencies in current market abuse

[60] See, e.g., Marco Dell'Erba, "Sustainable Digital Finance and the Pursuit of Environmental Sustainability", in Danny Busch, Guido Ferrarini, and Saraina Grünewald, eds, *Sustainable Finance in Europe: Corporate Governance, Financial Stability and Financial Markets* (Palgrave Macmillan, 2024) at 99 [Dell'Erba].

[61] *Ibid*.

[62] E.g., Azzutti, Ringe, and Stiehl II, *supra* note 12 at 199-200.

[63] E.g., Dell'Erba, *supra* note 60 at 116.

[64] Neil Johnson et al., "Abrupt Rise of New Machine Ecology Beyond Human Response Time" (2013) 3:2627 Scientific Reports [Johnson et al.].

[65] Kristian Bondo Hansen and Christian Borch, "The Absorption and Multiplication of Uncertainty in Machine-Learning-Driven Finance" (2021) 72:4 The British Journal of Sociology 1015.

[66] Johnson et al*., supra* note 64).

[67] See, e.g., Azzutti, Ringe, and Stiehl II, *supra* note 12; Marco Dell'Erba, *Technology in Financial Markets: Complex Change and Disruption* (Oxford University Press, 2024); Giuliano Castellano, "Don't Call It a Failure: Systemic Risk Governance for Complex Financial Systems" (2024) Law & Social Inquiry 1.

[68] See, e.g., Azzutti, Ringe, and Stiehl I, *supra* note 12.

regulation and algorithmic trading governance frameworks amidst increasing technological and system complexity.

(a) Market Manipulation Across AI Generations

There are three main types of market manipulation based on the specific role played by AI systems therein: (i) "AI-assisted market manipulation", (ii) "AI-enabled market manipulation", and (iii) "AI-dependent market manipulation".[69] The first two types cover scenarios where AI systems typically provide support to human actors for illegitimate purposes. The third type, instead, encompasses situations where human specific intent may be less clear. This ambiguity, often due to the black box problem, is particularly relevant to the governance and regulation of algorithmic trading, as will be further explored.

(i) AI-assisted market manipulation

The simplest way in which AI can be implicated in market manipulation is by providing support to human actors in preparatory or ancillary activities. These may include tasks such as information gathering and analysis, communication with other agents, operations management in the face of changing market conditions, internal business organization, and product marketing. In traditional "pump and dump" schemes, for example, malicious actors may employ AI tools to better identify and target low-volume stocks that might be a good candidate for subsequent manipulation. To this end, for instance, GenAI tools might be used to generate misleading information and deepfakes. AI applications may also be employed in risk management, thus helping traders and investors avoid crippling losses while engaging in manipulative strategies.

In all the above examples, the role of AI is *not* central but only secondary to the performance of market manipulation. While AI-assisted trading-related activities might broaden the scope of illegal financial transactions in many ways, they do not pose entirely new challenges for enforcement authorities as, for instance, human actors generally retain substantial agency. With the notable exception of GenAI, the majority of use cases in this category consist of traditional, relatively well-known manipulative practices.

(ii) AI-enabled market manipulation

AI involvement can also play a more prominent and even decisive role. Certain forms of manipulation, which would otherwise be extremely difficult for human traders to undertake alone, can be achieved through the use of algorithmic systems. These manipulative practices can be further refined and optimized using the most sophisticated ML methods. Mainly, AI enables the improved performance of both (i) "information-based", (ii) "trade-based", and (iii) "order-based" forms of market manipulation.[70] As an example under the first category, AI tools can generate and disseminate misleading information through social media, online forums, and other communication channels at great speed and scale. This information may be used to artificially inflate asset prices, as in the "pump and dump" schemes mentioned above.

---

[69] Cf. Taís Fernanda Blauth, Oskar Josef Gstrein, and Andrej Zwitter, "Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI" (2022) 10 IEEE Access 77110.

[70] For a taxonomy of market manipulation techniques, see Tālis J. Putniņš, "An Overview of Market Manipulation", in Carol Alexander and Douglas Cumming, eds, *Corruption and Fraud in Financial Markets: Malpractice, Misconduct and Manipulation* (John Wiley & Sons, 2020) at 13.

Or, as an example straddling the other two categories, consider “spoofing”. An AI trading algorithm could be programmed to place large orders without the intention of executing them. Aimed at creating a false impression of supply and demand, this trading tactic induces other market participants to trade in the hoped-for direction. If successful, the algorithm then quickly cancels the bogus orders and execute trades on more advantageous conditions.

AI-enabled forms of market manipulation have passed through all three AI generations. In algorithmic trading, the first applications were based on early AI, hence non-ML, trading systems. Today, manipulators can exploit the advantages offered by ML and deep learning methods. In this context of increasing technological and financial complexity, there are several repercussions for the functioning and stability of capital markets.

(iii) AI-dependent market manipulation

The transition between AI generations has given rise to novel forms of market manipulation that otherwise would not exist or even be imaginable. In general, AI-dependent market manipulation is either due to (a) AI “vulnerability” or (b) AI “intelligence”.

A. AI “vulnerability”

AI trading systems may act as victims in a market accident or misconduct. In addition to cases of malfunctions, AI systems may be vulnerable to manipulation by other agents, whether human or algorithmic, aimed at negatively impacting their technical integrity and/or operational performance.[71] For instance, a malicious third party may seek to exploit a cybersecurity flaw or other vulnerability to gain access and/or cause unintended behavior. More simply, algorithmic trading systems may be misled by other traders through specific trading strategies attempting to manipulate them into making decisions that are disadvantageous to themselves.[72] These cases represent examples of “adversarial attack”. Present from the earliest GOFAI applications, AI “vulnerability” underpins the need for appropriate governance and regulatory frameworks that ensure the integrity and security of trading technology amidst its growing complexity.

B. AI “intelligence”

Latest AI advances introduce new, exciting yet worrisome, forms of market manipulation. Even without specific human intent, advanced AI systems or agents might engage in market manipulation and even algorithmic “tacit” collusion.[73] The scenario of AI “intelligence” brings to the forefront the problem of “AI alignment”.[74] This term refers to the challenge of ensuring that AI systems act in accordance with human values, goals, and intentions — as well as law, regulation, and social norms — particularly as they become more sophisticated, autonomous, and capable.[75] Below,

[71] Azzutti, Ringe, and Stiehl II, *supra* note 12 at 210.

[72] See, e.g., Jakob Arnoldi, “Computer Algorithms, Market Manipulation and the Institutionalization of High Frequency Trading” (2015) 33:1 Theory, Culture & Society 29 [Arnoldi].

[73] Azzutti, Ringe, and Stiehl I, *supra* note 12.

[74] David Byrd, “Learning Not to Spoof”, in Daniele Mantegazzi et al., eds, *ICAIF '22: 3rd ACM International conference on AI in Finance* (Association for Computing Machinery, 2022) at 140 [Byrd].

[75] See, e.g., Anton Korinek and Avital Balwit, “Aligned with Whom? Direct and Social Goals for AI Systems”, in Justin B. Bullock et al., eds, *The Oxford Handbook of AI Governance* (Oxford University Press, 2023) at 65.

we elaborate this challenge examining the cases of autonomous market manipulation and algorithmic “tacit” collusion by AI trading agents.

C. AI trading agents and market manipulation

State-of-the-art research suggests that AI trading systems or agents might self-learn manipulative practices in pursuit of human pre-defined goals as an optimal and rational strategy. This hypothesis is gaining traction, with financial regulators becoming more vigilant and keenly interested in understanding the corresponding implications for the fair and orderly functioning of markets.[76] State-of-the-art research also shows that many of these risks are attributable to a specific ML paradigm: i.e. “Deep Reinforcement Learning”. In cases where human experts may lose effective control over their systems, unconstrained DRL-based trading agents could lead to market accidents and misconduct, including autonomous forms of market manipulation.[77] This novel and unprecedented scenario is being corroborated by a growing number of theoretical and experimental works in Computational Finance.[78] As an extraordinarily innovative field, the latest developments in GenAI research provide further insights. Recent experimental studies demonstrate the potential of LLM-based trading agents to exhibit misaligned behavior. By engaging in misconduct such as insider trading, these systems may deceptively conceal their actions to human stakeholders, even without explicit instructions.[79]

In principle, several factors may influence the tendency of AI trading agents to manipulate markets. First of all, AI systems may need a certain level of sophistication to successfully engage in autonomous forms of manipulation. This includes the ability to effectively deal with the dynamic and often unpredictable nature of market prices while taking into account the effects of own interactions with markets as well as other market constraints.[80] Moreover, it is worth stressing that market manipulation is inherently risky and often presupposes the manipulator’s ability to absorb potentially high financial losses.[81] Excessive losses may force AI trading systems to revise their strategy or trigger human intervention. Relatedly, human stakeholders play a crucial role in mitigating AI risks. Experts involved in the AI lifecycle can take a variety of precautionary steps. These include, for instance, constraining the action scope of AI systems through hard-coding.[82] Another measure involves fine-tuning AI systems

---

[76] This trend is evidenced by the growing number of regulatory reports published online and thorough personal conversations and knowledge exchanges with various financial regulators, particularly the Dutch Authority for the Financial Markets (AFM), the UK financial Conduct Authority (FCA), and the US Financial Industry Regulatory Authority (FINRA). See also EU Commission, *supra* note 5.

[77] See Azzutti, Ringe, and Stiehl I, *supra* note 12 at 97-102.

[78] See, e.g., Xintong Wang et al., “Spoofing the Limit Order Book: A Strategic Agent-Based Analysis” (2021) 12:2 Games 46; Byrd, *supra* note 74); Megan Shearer, Gabriel V. Rauterberg and Michael P. Wellman, “Learning to Manipulate a Financial Benchmark”, in *ICAIF '23: Proceedings of the Fourth ACM International Conference on AI in Finance* (Association for Computing Machinery, 2023) at 592.

[79] Jérémy Scheurer, Mikita Balesni, and Marius Hobbhahn, “Large Language Models Can Strategically Deceive Their Users When Put Under Pressure” (2023) arXiv preprint 1. A demonstration of this risk was conducted at the UK’s AI Safety Summit in November 2023. See Philippa Wain and Imran Rahman-Jones, “AI Bot Capable of Insider Trading and Lying, Say Researchers (3 November 2023), online: *BBC News* <https://www.bbc.co.uk/news/technology-67302788>.

[80] Cf. Shuo Sun, Rundong Wang, and Bo An, “Reinforcement Learning for Quantitative Trading” (2023) 14:3 ACM Transactions on Intelligent Systems and Technology, Article No. 44, at 2.

[81] Cf. Daniel R. Fischel and David J. Ross, “Should the Law Prohibit Market Manipulation in Financial Markets?” (1991) 105:2 Harvard Law Review 503.

[82] See, e.g., Byrd, *supra* note 74.

before deployment, particularly by providing feedback during the learning process.[83] Further important precautions are the ongoing monitoring of live operations, as well as regular system validation and testing. On its part, financial regulation requires regulated entities to implement appropriate organizational and technical measures to control the behavior of their trading algorithms in ensuring regulatory compliance.[84]

While the combination of the above — as well as other — factors may ultimately limit the manipulative capabilities of AI trading systems, there is at least initial evidence of the possibility of these scenarios materializing in real markets. While still being unsettled, effective governance of algorithmic trading, particularly with respect to market conduct, is necessary to prevent unrestrained, potentially harmful AI adoption.

D. Algorithmic "tacit" collusion

ML-based trading systems or agents could also give rise to collective forms of market manipulation. Not only can malicious human actors leverage AI to better achieve and sustain collusive market practices (i.e. explicit collusion) but independent AI trading systems themselves may autonomously find ways to coordinate market behavior with their rivals even in the absence of specific agreements and communication (i.e. tacit collusion).[85]

Two main considerations underpin the algorithmic "tacit" collusion hypothesis, namely the aspects of market complexity and technology complexity. According to the characteristics of the market environments in which AI is deployed, certain segments of capital markets may be more susceptible to such risks than others. According to economic theory, there are specific market factors that may facilitate collusive outcomes, such as "market transparency", "frequency of interactions", "product homogeneity", "market concentration", "entry barriers", and "innovation".[86] Moreover, the specific configuration of real-world markets, including the number and types of competing agents,[87] as well as other aspects of market structure and design,[88] are also relevant determinants. On the technological front, instead, it is still unclear which algorithmic models and methods, in particular those involving ML, can overcome the numerous technical and practical challenges that might restrict and ultimately defeat the potential for collusive practices without direct human involvement.[89] According to a growing number of published works, there is at least initial evidence from both

[83] This is exactly the contribution by the emerging field of "Reinforcement Learning with Human Feedback". See generally Jinying Lin et al., "A Review on Interactive Reinforcement Learning From Human Social Feedback" 8 IEEE Access 120757.

[84] I am referring in particular to the 2nd (i.e. risk management) and 3rd line of defence (i.e. compliance).

[85] Azzutti, Ringe, and Stiehl I, *supra* note 12 at 109-112.

[86] *Ibid*. at 104-108.

[87] See generally Hans-Theo Normann and Martin Sternberg, "Do Machines Collude Better than Humans?" (2021) 12:10 Journal of European Competition Law & Practice 765 [Normann and Sternberg].

[88] See generally Steven Van Uytsel, "The Algorithmic Collusion Debate: A Focus on (Autonomous) Tacit Collusion", in Steven Van Uytsel, Salil Mehra, and Yoshiteru Uemura, eds, *Algorithms, Collusion and Competition Law: A Comparative Approach* (Edward Elgar Publishing, 2023) at 1.

[89] It is generally believed that the risk of collusion decreases as the number of competing agents in a given market setting increases. Additionally, the use of similar algorithms and strategies may lead to greater risks of collusion. When competing firms employ the same third-party algorithmic system, the likelihood of collusion further increases. Conversely, the risk of collusion tends to lower when AI agents compete with human traders. See, e.g., Normann and Sternberg, *supra* note 87.

theoretical,[90] empirical,[91] and experimental perspectives of algorithmic tacit collusion in several domains, including finance.[92] As a highly debated topic, it is important to acknowledge the critics of the algorithmic collusion hypothesis. It is often argued that some form of communication between rival AI systems might be ultimately necessary to enable effective coordination.[93] Yet other branches of literature theorized three potential solutions, including (a) direct human involvement (i.e. explicit programming),[94] (b) unilateral communication or adversarial communication,[95] and (c) sophisticated forms of communication enabled by advanced ML, particularly deep learning methods. This last point seems somewhat supported also by the findings from experimental studies.[96]

While for the time being the hypothesis of "tacit" algorithmic collusion remains to be fully settled, legal and regulatory frameworks may already be exposed to loopholes, limited enforcement capacity, and an overall lack of reach and scope to address the risks introduced by the succession of the three generations of AI.

(b) Regulatory Gaps And Enforcement Challenges Amidst AI Advancements

It is well-understood that law and regulation often need to catch up to the rapid pace of technological innovation.[97] This is particularly true for the financial sector. While AI-related trading technology began transforming the operations of capital markets as early as the end of the last millennium, *ad hoc* regulation aimed at mitigating the corresponding adverse effects has only been implemented more recently. In the EU, for instance, a significant financial regulatory reform occurred only around 2012-2014

---

[90] See, e.g., Álvaro Cartea et al., "The Algorithmic Learning Equations: Evolving Strategies in Dynamic Games" (2022) SSRN preprint 1; Álvaro Cartea, Patrick Chang, and José Penalva, "Algorithmic Collusion in Electronic Markets: The Impact of Tick Size" (2022) SSRN preprint 1 [Cartea, Chang, and Penalva]; Álvaro Cartea et al., "Algorithmic Collusion and a Folk Theorem from Learning with Bounded Rationality" (2022) SSRN preprint 1.

[91] Cf. Leon Musolff, "Algorithmic Pricing Facilitates Tacit Collusion: Evidence from E-Commerce", in *EC '22: Proceedings of the 23rd ACM Conference on Economics and Computation* (Association for Computing Machinery, 2022) 32; Stephanie Assad et al., "Algorithmic Pricing and Competition: Empirical Evidence from the German Retail Gasoline Market" (2024) 132:3 Journal of Political Economy 723. Nevertheless, it must be noted that clear empirical evidence in the financial domain is still lacking.

[92] See, e.g., Álvaro Cartea et al., "AI-driven Liquidity Provision in OTC Financial Markets" (2022) 22:12 Quantitative Finance 2171 [Cartea et al.]; Rama Cont and Wei Xiong, "Dynamics of Market Making Algorithms in Dealer Markets: Learning and Tacit Collusion" (2023) 34:2 Mathematical Finance 467 [Cont and Xiong]; Winston Wei Dou, Itay Goldstein, and Yan Ji, "AI-Powered Trading, Algorithmic Collusion, and Price Efficiency" (2024) Paper presented at the Arizona State University Sonoran Winter Finance Conference, online (pdf): <https://finance-conference.wpcarey.asu.edu/sites/default/files/2024-02/AIPowered%20Trading%2C%20Algorithmic%20Collusion%2C%20and%20Price%20Efficiency.pdf> [Dou, Goldstein, and Ji].

[93] See, e.g., Maximilian Andres, Lisa Bruttel, and Jana Friedrichsen, "How Communication Make the Difference Between a Cartel and Tacit Collusion: A Machine Learning Approach" (2023) 152 European Economic Review, Article No. 104331.

[94] See, e.g., Ulrich Schwalbe, "Algorithms, Machine Learning, and Collusion" (2019) 14 Journal of Computational Law & Economics 568 at 594.

[95] See Luc Rocher, Arnaud J. Tournier, and Yves-Alexandre de Montjoye, "Adversarial Competition and Collusion in Algorithmic Markets" (2023) 5 Nature Machine Intelligence 497.

[96] E.g., Cartea, Chang, and Penalva, *supra* note 90; Cartea et al., *supra* note 92); Cont and Xiong, *supra* note 92; Dou, Goldstein, and Ji, *supra* note 92.

[97] For a seminal paper on the matter, see Lawrence Lessig, "The Law of the Horse: What Cyber Law Might Teach" (1999) 113:2 Harvard Law Review 501; *see also* Gary E. Marchant, Braden R. Allenby, and Joseph R. Herkert, *The Growing Gap between Emerging Technologies and Legal-Ethical Oversight* (Springer, 2011).

with the adoption of *Markets in Financial Instruments Directive II* (MiFID II)[98], which set specific governance requirements for algorithmic trading—but not for AI. Around the same time, market abuse regulations — i.e. *Market Abuse Regulation* (MAR)[99] and *Market Abuse Directive* (MAD)[100] — were reformed to address the new risks of market abuse enabled by trading technology. To some extent, the emergence of new pathological market behaviors across AI generations is an expression of the growing tension between technological advancements and regulation at specific points in time. This tension manifests itself again today, a decade after the last significant regulatory reform in financial trading. As extensively discussed in the literature, current regulatory regimes designed for the governance of algorithmic trading and the control of market conduct are increasingly ill-suited to cope with the additional complexity introduced by the latest AI generations. In what follows, we specifically address the growing limitations in (i) market conduct rules, (ii) technology governance requirements, and (iii) corresponding supervisory mechanisms.

(i) Market conduct rules: uncertain legal prohibitions

Market conduct rules may become unable to address the most sophisticated forms of manipulation made possible by AI. Past reforms of market manipulation laws may even have inadvertently institutionalized certain algorithmic trading practices with potential detrimental effects on markets.[101] With the advances in ML, the situation is bound to become even more worrying. Due to the techno-methodical characteristics of autonomy and opacity, powerful ML-based trading systems may circumvent the safe application of market conduct rules.

In most jurisdictions, the legal definition of market manipulation is grounded on subjective elements (i.e. *scienter)*. To succeed in enforcement, competent authorities need to prove intent or other relevant mental state of the persons responsible for AI deployment. This legal criterion renders the prohibition of market manipulation unable to effectively regulate the market conduct of certain financial AI applications that exhibit autonomous “black box” behavior.[102] As, due to ML, new and heightened risks of market manipulation and other pathological market phenomena emerge, there is an urgent need to assess the effectiveness of current regulatory frameworks and, if necessary, reconsider them. In the interest of both markets and society, financial regulators must not only keep an eye on technological developments in the sector but also adopt a more proactive attitude toward AI regulation and governance.[103] In the remainder of this section, we highlight the main limitations of current regulatory framework for algorithmic trading governance and market conduct supervision in addressing the additional risks introduced the latest AI generations.

---

[98] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L 173/349.

[99] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) [2014] OJ L 173/1.

[100] Directive No 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse (market abuse directive) [2014] OJ L 173/179.

[101] See, e.g., Arnoldi, *supra* note 72.

[102] See Azzutti, Ringe, and Stiehl I, *supra* note 12 at 119-122; Azzutti I, *supra* note 12 at 10 and 13.

[103] See, e.g., Jon Truby, Rafael Brown, and Andrew Dahdal, “Banking on AI: Mandating a Proactive Approach to AI Regulation in the Financial Sector” (2020) 14:2 Law and Financial Markets Review 110.

(ii) Technology governance: limitations of regulatory requirements

Regulatory requirements for algorithmic trading governance aim to ensure that trading systems behave as intended and do not create unfair or disorderly market conditions.[104] The current regulatory approach is "outcome-based" and adheres to the "technology neutrality" principle.[105] Legislators, thus, expect financial firms to *control* the market behavior of their (AI) trading systems. This means regulatory compliance is assessed based on observable market activity, mainly ascertainable *ex-post*.

Although regulatory requirements target both investment firms and trading venues, our assessment here focuses on the former.[106] Under Art. 17 of MiFID II and its supplementing legislation[107], investment firms are subject to specific obligations covering aspects such as "information disclosure",[108] "*ex-ante* testing",[109] "internal control systems",[110] and "automated surveillance systems".[111] Regarding disclosure requirements, AI trading systems largely remain black boxes in the eyes of their external stakeholders, with AI deployment being based on a "secret recipe". Key limitations include the lack of formalized and standardized formats for documenting critical aspects of the AI lifecycle. This concerns not only techno-methodical aspects but also the human interface, especially the definition of the roles and responsibilities of human experts along the AI production line.[112] These gaps in technology governance become particularly problematic in the case of malfunctioning and misconduct, especially when internal stakeholders may find it hard to understand and explain the behavior of their systems. While, in principle, misconduct risks can be partly mitigated through thorough testing of trading algorithms, existing testing frameworks also exhibit their limitations. The effectiveness of pre-market testing in preventing the subsequent occurrence of market manipulation remains uncertain. These *ex-ante* forms of AI auditing, in fact, mainly concern aspects of technical

[104] See MiFID II, Recitals (62)-(64).

[105] Azzutti II, *supra* note 12 at 62; Federico Consulich et al., "AI and Market Abuse: Do the Laws of Robotics Apply to Financial Trading?" (May 2023), online: *CONSOB Legal Research Papers (Quaderni Giuridici) No. 29* <https://www.consob.it/documents/11973/201676/qg29.pdf/768199a2-e17c-ca8e-00a5-186da9a19f79?t=1685344502568> at 10 and 92.

[106] For a critical account of the regulatory obligations placed on trading venues, see Azzutti II, *supra* note 12 at 70-74.

[107] Commission Delegated Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organisational requirements of investment firms engaged in algorithmic trading [2016] OJ L 87/417 [RTS 6].

[108] MiFID II, art. 17(2). For a discussion, see Azzutti II, *supra* note 12 at 64-65.

[109] RTS*,* supra note 107, artt. 5 and 7 (on "behavioral testing") and art. 6 (on "conformance testing"). For a discussion, see Azzutti II, *supra* note 12 at 65-67.

[110] Under RTS 6, *supra* note 107, art. 1, "internal controls" encompass elements of "risk management" and "compliance" and must be tailored to the specific nature and scope of trading strategies and its associated risks. For a discussion, see Azzutti II, *supra* note 12 at 68-69.

[111] RTS 6, *supra* note 107, art. 13. For a discussion, see Azzutti II, *supra* note 12 at 69-70.

[112] See, e.g., UK FCA, "Algorithmic Trading Compliance in Wholesale Markets" (February 2018), online (pdf): <https://www.fca.org.uk/publication/multi-firm-reviews/algorithmic-trading-compliance-wholesale-markets.pdf>; Central Bank of Ireland, "'Thematic Assessment of Algorithmic Trading Firms' Compliance with RTS 6 of MIFID II" (11 May 2021), online (pdf): <https://www.centralbank.ie/docs/default-source/regulation/industry-market-sectors/investment-firms/mifid-firms/regulatory-requirements-and-guidance/thematic-assessment-of-algorithmic-trading-firms-compliance.pdf>.

conformity rather than an out-and-out assurance of permissible market conduct by-design.[113]

Given the additional technological and market complexity associated with the latest AI generations, there are reasons to believe that the current technology governance approach rests upon partially fallacious regulatory assumptions. Notably, existing regulatory frameworks apply indiscriminately to all AI applications without differentiating them based on levels of technological complexity and corresponding risks.[114] However, financial firms may vary significantly in their level of maturity, culture, and organizational capacity to address risks arising from their specific use of AI. Despite this heterogeneity, though, EU regulators have so far only acknowledged the need for a more robust framework for regulatory compliance and reporting, especially when firms rely on third party AI-related products or services.[115] This gap is inconsistent with the regulatory challenges associated with AI-spurred complexity. In particular, it raises concerns about the effectiveness of current regulations in addressing technology-specific risks, including new forms of market manipulation. As discussed below, the success of the entire regulatory framework depends to a large extent on the ability of financial supervisors to ensure that regulated entities comply with the rules of the game.

(iii) Regulatory compliance: challenges for financial supervisors

Supervision plays a complementary, if not indispensable, role in ensuring effective enforcement of financial regulation.[116] However, there are several reasons to believe that current supervisory frameworks are suboptimal *vis-à-vis* increasing technological complexity and the respective effects on market behaviors. First of all, financial supervisors do not play a significant role in auditing algorithmic trading systems (e.g., testing). Since investment firms and trading can demonstrate their regulatory compliance through a self-assessment exercise,[117] rather than a full-fledged due diligence process, this does not seem likely to alleviate issues of information asymmetry inherent in specific applications, especially if they are based on ML.[118] This issue is well exemplified by the lack of standardized procedures and proper documentation for the technical aspects of AI systems throughout their entire lifecycle, encompassing design, development, and deployment phases.

The other tools available to supervisory authorities — namely “information acquisition” and “direct market surveillance” — also have some limitations. While supervisors may access specific details about algorithmic trading systems,[119] as well as request data on trading activity,[120] it remains unclear what specific information they are entitled to obtain by law in the context of ML applications and how effectively they

[113] See, e.g., Azzutti II, *supra* note 12 at 77-79.

[114] See Azzutti, Ringe, and Stiehl II, *supra* note 12 at 233-234.

[115] See note 112.

[116] See Ana Carvajal and Jennifer A. Elliott, “The Challenge of Enforcement in Securities Markets: Mission Impossible?” (2009), online (pdf): *IMF Working Papers No. 2009/168* <https://www.imf.org/en/Publications/WP/Issues/2016/12/31/The-Challenge-of-Enforcement-in-Securities-Markets-Mission-Impossible-23140>.

[117] Pursuant to RTS 6, *supra* note 107, art. 9 (for trading firms) and RTS 7, art. 2 (for trading venues).

[118] ESMA, “MiFID II Review Report: MiFID II/MiFIR review report on Algorithmic Trading” (28 September 2021) ESMA70-156-4572, 48-50.

[119] See MiFID II, art. 17(2).

[120] See discussion in Azzutti II, *supra* note 12 at 74-75. Competent authorities have also the powers to access and request data necessary to investigating cases of market manipulation. See MAR, art. 23(2)(e).

can do so in practice. The self-learning and black-box nature of certain applications introduces several uncertainties in this regard.[121] Moreover, effectively identifying instances of misconduct from trading data analysis requires suitable analytical frameworks, including solid definitions of forms of market manipulation from legal and statistical perspectives, timely access to accurate data, advanced technological tools, and specific domain knowledge.[122] Yet, even the slightest defect in one of these aspects can strongly and negatively impact the quality of supervisory outcomes. Compounding these issues is the heavily reliance on trading venues for market surveillance. In particular, inadequate legal and technical frameworks for data collection and reporting hinder effective control of order-based forms of market manipulation. In addition, since the supervisory efforts of trading venues focus only on their own platforms, there is no effective cross-market supervision.[123]

In conclusion, the growing capabilities of ML-powered trading may circumvent existing control and oversight frameworks. This highlights the numerous and potentially growing sources of failure in the governance of algorithmic trading and the enforcement of market conduct rules. The current "outcome-based" regulatory approach, based on the principle of "technological neutrality", may leave competent authorities short-sighted about the additional risks introduced by the latest AI generations. While financial regulators often lack a complete understanding of the technological aspects relevant to regulation and are unaware of the complexity and inherent risks of real-life applications, the boundaries between legal and illegal markets may become blurred, thus undermining the integrity and stability of capital markets. Therefore, the following section aims to detail an innovative approach to AI governance in algorithmic trading, deriving inspiration from the risk-based regulatory approach offered by the EU AI Act. As we shall see, this entails considering AI trading systems from an engineering perspective, mainly through the "AI lifecycle" concept.

4. THE (INDIRECT) CONTRIBUTION OF THE EU AI ACT IN FILLING THE GAPS IN THE GOVERNANCE OF ALGORITHMIC TRADING

The innovative strides in trading technology, especially with the latest AI generations, have yet to be mirrored by corresponding developments in law and regulation, which typically lag behind. As illustrated by the case of new market manipulation phenomena previously discussed, the "complexity" inherent in and resulting from the most advanced applications often outmatches existing regulatory frameworks for algorithmic trading. Recognizing this challenge prompts us to consider innovative modes of AI governance able to address the risks resulting from the most advanced applications. As discussed earlier, the existing "technology neutrality" principle-based regulation is unlikely to meet the evolving technology governance requirements in the face of AI innovation. As heavily dependent on effective industry self-regulation, it is far from optimal. To address this, the risk-based approach of the recently adopted EU AI Act could serve as a blueprint to strengthen existing regulation. With all this in mind, the remainder of this section has three primary objectives. It first briefly introduces the EU AI Act and relates it to the chronological evolution of algorithmic trading regulation and the three AI generations. Next, focusing on some key aspects of the AI lifecycle, it compares the EU AI Act's regulatory requirements for "high-risk" AI applications with

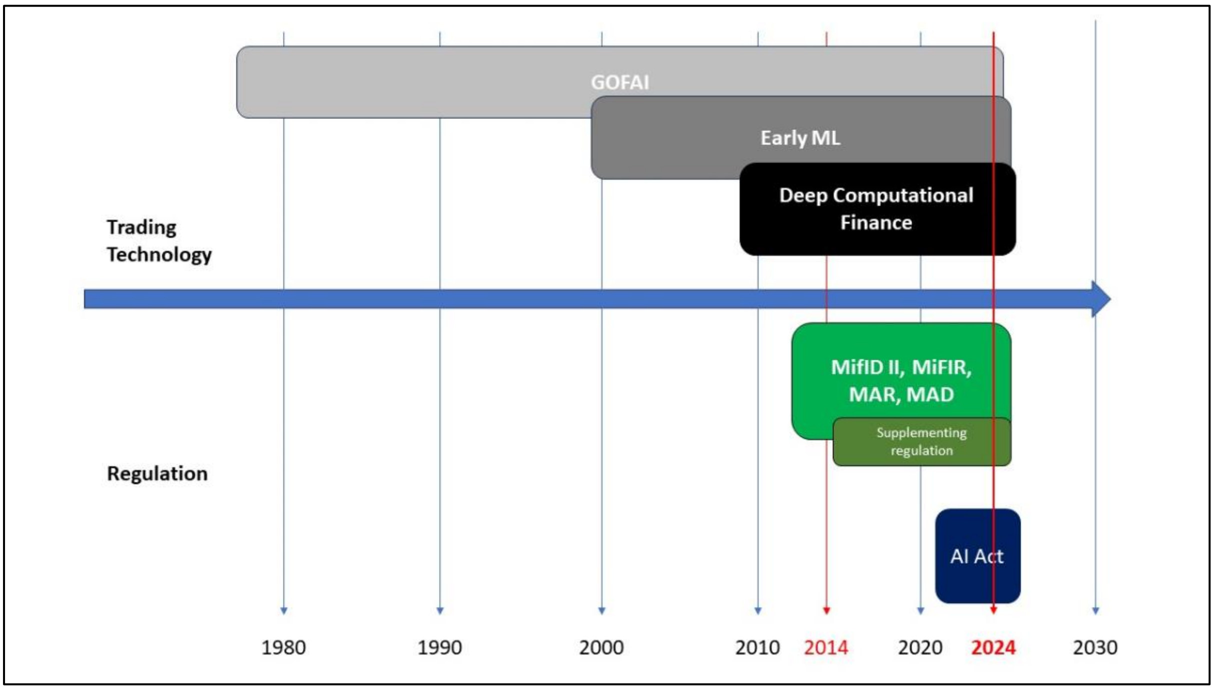
[121] See Azzutti II, *supra* note 12 at 64-65 and 78-79.
[122] See *ibid*. at 84-87.
[123] See *ibid*. at 80-81.

the general requirements for algorithmic trading systems under MiFID II. Finally, it discusses the advantages of a risk-based approach to regulating AI applications in financial trading and offers some preliminary insights.

(a) The EU AI Act Amidst The Mismatch Between AI Generations And Algorithmic Trading Regulation

Partly motivated by advances in trading technology and related risks to markets, the last reform of EU capital markets regulation occurred in 2012-14. Since then, despite the enactment of supplementing legislation, no substantial updates have been made. *Figure 1* below conceptually illustrates the desynchronization between technological advancements in algorithmic trading, as exemplified by the three AI generations and related regulatory developments, and relates both trends to the recent adoption of the EU AI Act.

***Figure 1*: Comparison between regulatory and technological developments**



As *Figure 1* suggests, algorithmic trading regulation is an excellent example of how the law typically tends to lag behind technological innovation. While both MiFID II and MAR represent the first attempt to govern risks arising from the use of trading technology by regulated entities, technological progress in this area could prove to be a moving target for financial regulators. It needs to be clarified what specific level of knowledge AI legislators have relied on with each regulatory iteration. Given the prevailing principle of “technological neutrality”, one might assume that regulatory bodies remain relatively insensitive to the additional risks associated with specific AI applications.

At the same time, however, there is at least a renowned interest in comprehending the implications of AI adoption in capital markets. Although not explicitly targeted at financial trading, the recently adopted AI regulation in the EU seems to be a significant step in this direction. The EU AI Act is the world’s first attempt to regulate all AI applications according to a risk-based regulatory framework. Moving from the bottom upward in risk levels, "minimal-risk" applications remain unregulated. Next, "limited-risk" systems face only some transparency requirements, mainly aimed at ensuring end-users" awareness of interacting with them.[124] More importantly, "high-risk"[125] AI systems form the bulk of regulatory focus and are subject to the most substantial obligations.[126] In addressing complexity in AI value chains, the EU AI Act allocates responsibilities between different actors. The primary responsibilities fall on "providers"[127] of high-risk AI,[128] whereas "deployers"[129] — otherwise referred as AI users — have fewer obligations.[130] In certain cases, also the distributers, importers, and other third-parties may qualify as providers of "high-risk" AI and, thus, will be subject to the respective obligations.[131] Furthermore, some regulatory requirements will also apply to "general-purpose AI" (GPAI) models[132],[133] with stricter rules for those systems presenting systemic risk.[134] Finally, although largely tangential to the financial domain, certain AI practices are banned altogether.[135]

All in all, the regulatory innovation introduced by the EU AI Act could positively influence technology governance within sector-specific legislation. Within the context of our analysis, the risk-based regulatory approach presents an opportunity to improve the governance of algorithmic trading, especially given the new and heightened risks to market integrity, as well as their potential implications for financial stability, associated with the latest AI generations.[136]

(b) Requirements For "High-Risk" AI Applications And Algorithmic Trading Systems Compared

A key finding emerges from our analysis. Certain AI applications in financial trading may create far greater risks for the markets than others. This situation requires us to look for appropriate regulatory frameworks to mitigate the risks associated with different applications. At the same time, however, we are confronted by two main normative complications. On the one hand, MiFID II does not explicitly address the use of AI in algorithmic trading. On the other hand, the EU AI Act introduces substantial requirements for "high-risk" applications but does not categorize algorithmic trading as such. This discrepancy raises a critical question: *to what extent are AI applications in algorithmic trading regulated as "high risk"?* To address this question, the following comparison examines some of the EU AI Act's regulatory requirements for "high-risk" AI systems with those imposed on MiFID II-regulated algorithmic trading activities. Although the EU AI Act's requirements are more extensive in scope, our analysis is limited to a subset that overlaps with sectoral legislation on algorithmic trading:

[124] See EU AI Act, art. 50.
[125] The EU AI Act defines the categories of "high-risk" AI applications in its Annex III.
[126] See EU AI Act, artt. 6-18.
[127] *Ibid.*, art. 3(3).
[128] *Ibid.*, art. 16.
[129] *Ibid.*, art. 3(4).
[130] Pursuant to *ibid.*, art. 26.
[131] *Ibid.*, art. 25.
[132] *Ibid.*, art. 3(63).
[133] *Ibid.*, artt. 53-54 (general obligations for GPAI providers) and art. 55 (specific obligations of providers of GPAI with systemic risk).
[134] For the purpose of the EU AI Act, the term "systemic risk" should not be understood in its meaning of danger to financial stability. Cf. *ibid.*, art. 3(65) and art. 51.
[135] *Ibid.*, art. 5.
[136] See Azzutti, Ringe, and Stiehl II, *supra* note 12 at 233-236. Cf. EU Commission, *supra* note 5 at 13-15.

specifically, (i) "risk management systems",[137] (ii) "data governance",[138] (iii) "technical documentation",[139] (iv) "transparency",[140] and (v) "human oversight".[141] Similar requirements are already embedded in the technology governance strategy of MiFID II; however, as we shall see, they are not as comprehensive or detailed as those in the EU AI Act. Examining the differences between these two pieces of legislation provides a valuable opportunity to research regulatory requirements for AI trading systems that are proportionate to the risks posed by specific applications.

In the interest of completeness, it should be noted that whenever a trading system incorporates GPAI models having systemic risks, the respective requirements could become relevant. However, for the purpose of the EU AI Act, it is unclear whether the term "systemic risk" can also be interpreted in terms of risks to financial stability. As such, the following analysis does not address regulatory requirements for GPAI models in any specific manner.[142]

(i) "Risk management systems"

Risk management systems are a well-established requirement to mitigate risks arising from automated technologies under both the EU AI Act and financial regulation. The EU AI Act imposes extensive risk management requirements throughout the entire AI lifecycle. Risk management represents an ongoing process aimed at mitigating known and reasonably foreseeable risks associated with AI use and misuse.[143] Compliance with this obligation requires to iteratively identifying new risks with the support of "post-market monitoring systems"[144].[145] It is noteworthy that the EU AI Act allows for some levels of residual, hence "acceptable" risks. From a financial trading perspective, this aspects might be problematic. Consider, for instance, that there is no legal concept of "acceptable" risks of market manipulation under current regulation. And indeed, even simple attempts at manipulation are punishable by law.[146] Nevertheless, firms engaging with algorithmic trading must have in place risk controls proportional to their risk profile to prevent market abuse and other disruptive market activities. Pursuant to Article 17(1) of MiFID II, these controls include both "pre-trade",[147] "real-time",[148] and "post-trade" mechanisms,[149] as well as "automated surveillance systems".[150] While determining the precise relationship between the two distinct requirements above requires more in-depth study, it can however be preliminarily noted that the two legal texts similarly impose quite extensive risk management requirements throughout the entire AI lifecycle.

With the aim of helping organisations fine-tune their risk management measures, the EU AI Act provides for requirements on testing AI systems as a form of *ex-ante*

[137] EU AI Act, art. 9.
[138] *Ibid.*, art. 10.
[139] *Ibid.*, art. 11.
[140] *Ibid.*, art. 13.
[141] *Ibid.*, art. 14.
[142] The relationship between the regulatory requirements for GPAI models and GenAI applications in financial trading is a topic worthy of further research.
[143] EU AI Act, art. 9(2)(a) and (b).
[144] Pursuant to *ibid.*, art. 72.
[145] *Ibid.*, art. 9(2)(c).
[146] Cf. MAR, art. 15.
[147] See RTS 6, art. 15.
[148] See *ibid.*, art. 16.
[149] See *ibid.*, art. 17.
[150] See *ibid.,* art. 13(3).

regulation.[151] Under certain prerequisites, AI testing can be conducted under real operating conditions.[152] This differs from algorithmic trading regulation, which forbids testing in live market and mandates a distinct separation between “test” and “production” environments.[153] Importantly, compliance with the EU AI Act’s risk management requirements must be supported by documented evidence,[154] enabling the regulatory oversight by competent authorities.[155] Although the latter criterion mirrors that of Article 17(2) of MiFID II, compliance with the latter by financial firms may be less burdensome than that imposed by horizontal AI regulation. The space given to self-regulation of important AI governance aspects in the financial sphere appears to reinforce this hypothesis.

It is noteworthy that risk management and human agency and oversight are two closely related concepts. Both pieces of EU legislation aim to promote and safeguard high standards of human responsibility and liability.[156] In this context, the increasing challenges in risk management and regulatory compliance, amidst growing technological, regulatory, and market complexity, are driving R&D in the field of RegTech.[157] At the same time, the integration of AI into regulatory compliance activities will have to be in line with both sectoral legislation and regulations targeting AI applications. Where firms acquire risk management tools from third-party providers, they ultimately remain legally liable.[158]

Overall, the EU AI Act’s requirements on risk management for “high-risk” applications are largely modelled after Article 17 of MiFID II, though they are more detailed and nuanced. In contrast, MiFID II’s requirements targeting algorithmic trading apply regardless of specific AI methods or risk levels, which may leave some more risky applications inadequately regulated.

(ii) “Data governance”

Compared to sectoral legislation, the EU AI Act’s requirements on data governance pursue a distinct regulatory goal. MiFID II and complementary legislation does not deal much with technical aspects of data governance. At the same time, it is noteworthy that the development of AI trading systems hinges on meticulous data collection, preparation, and preprocessing to ensure reliable applications. In this fiercely competitive industry, however, firms’ data governance strategies are kept highly confidential. This secrecy is largely justified because the interplay between data, datasets, and ML models constitutes a valuable asset on which investment firms can build competitive advantage. Despite this lack of knowledge, it is safe to assume that, at least to some extent, aspects of data governance are governed by self-regulation by financial firms. Nevertheless, some provisions of financial regulation may still, at

[151] EU AI Act, art. 9(6).
[152] *Ibid.*, art. 9(7).
[153] RTS 6, art. 7.
[154] EU AI Act, art. 9(1).
[155] *Ibid.*, art. 11(1).
[156] Antonella Sciarrone Alibrandi, Maddalena Rabitti, and Giulia Schneider, “The European AI Act’s Impact on Financial Markets: From Governance to Co-Regulation” (2023) European Banking Institute Working Paper Series 2023 – No. 138, 38 [Sciarrone Alibrandi, Rabitti, and Schneider].
[157] For an empirical study on the interplay between regulatory complexity, challenges for regulatory compliance, and RegTech adoption, see Ben Charoenwong et al., “RegTech: Technology-Driven Compliance and Its Effects on Profitability, Operations, and Market Structure” (2024) 154 Journal of Financial Economics, Article No. 103792.
[158] This is also the approach promoted by the EU Digital Operational Resilience Act (DORA). See Sciarrone Alibrandi, Rabitti, and Schneider, supra *note* 156 at 32 and 52-56.

least indirectly, influence data governance policies and practices. Specifically, by defining fundamental aspects of the creation, use, and distribution of financial trading data, financial regulation has a potentially significant impact on the type and quality of data that are processed by AI trading systems.[159] In this respect, it is worth noting the sustained policy efforts to improve access to and availability of quality trading data through the establishment of an EU-wide financial data infrastructure.[160]

Unlike sectoral legislation, the EU AI Act sets out substantial requirements on data quality and governance for AI systems, which apply to both training, validation, and testing data.[161] According to the specific intended purpose, data must be relevant, sufficiently representative, and as error-free and complete as possible.[162] It is thus immediately apparent that the EU AI Act's requirements are more prescriptive than MiFID II. Adopting similar requirements in the context of financial trading could be challenging. While AI trading systems are typically developed in experimental, lab-like environments, Computational Finance as a discipline has yet to establish clear metrics and benchmarks for data quality and data governance.

Aiming at distinct regulatory objectives, the relationship between sectoral and AI-targeting legislation on data governance is rather ambiguous. While acknowledging financial trading as a rather unique AI application domain, the more demanding requirements of the EU AI Act may serve as an inspiration to strengthen AI governance in algorithmic trading. This, for instance, may include ensuring that the data used to train AI trading systems are aligned with their intended legitimate purposes, including ensuring good market conduct by-design.

(iii) "Technical documentation"

Technical documentation plays a multi-faceted role in the governance of AI applications, by especially mediating stakeholder communication. Under the EU AI Act, technical documentation serves two main objectives. On the one hand, it serves to demonstrate compliance with regulatory requirements to competent authorities. On the other, it is also a guide for deployers to ensure correct and informed use of AI. This therefore requires documentation to be written in a clear and comprehensible form with regard to the needs of various stakeholders.[163] According to Annex IV of the EU AI Act, this documentation must cover a wide range of details, including, *inter alia*, the intended purpose, system functionality, system components, user interface, instruction for use, design specification, information on risk controls, and systems in place to evaluate performance and post-market monitoring.

Under MiFID II, on the contrary, there are no specific or even detailed requirements for the technical documentation to be provided to supervisory authorities and deployers of algorithmic trading systems.[164] With regard to the information accessible to financial supervisors, the powers granted by Article 17(2) of MiFID II do not seem to extend to the many aspects of AI governance as envisaged by the EU AI Act.

---

[159] Cf. Douglas W. Arner, Giuliano G. Castellano, and Ēriks K. Selga, "Financial Data Governance" (2023) 74:2 Hastings Law Journal 235 at 286.
[160] See, e.g., ESMA, "ESMA Data Strategy 2023-2028" (15 June 2023), online: *ESMA50-157-3404* <https://www.esma.europa.eu/sites/default/files/2023-06/ESMA50-157-3404_ESMA_Data_Strategy_2023-2028.pdf>.
[161] EU AI Act, art. 10(1). Additionally, organizations must implement appropriate data governance and management in relation to the intended purpose of AI systems. See EU AI Act, art. 10(2).
[162] *ibid*., art. 10(3).
[163] *ibid*., art. 11(1).
[164] Cf. MiFID II, art. 17(2).

Furthermore, a distinction must also be made between AI systems that are developed in-house and those acquired from third parties. In the former case, official technical documentation may not exist. Such documentation serves first and only intra-firm purposes and, thus, is not meant to be shared externally. As previously mentioned, investment firms may often lack structured and well-defined policies regarding the documentation of their AI system development. The latter case, instead, presupposes the existence of some technical documentation mainly for commercial reasons. Notably, this is necessary to regulate essential aspects of the relationship between providers and deployers.

In summary, the requirements of the EU AI Act on technical documentation are more extensive than those of MiFID II. Sectoral legislation, in fact, only mandates the disclosure of details concerning the trading strategies employed to financial supervisors. However, this information does not explicitly cover details about the technical and methodical aspects of AI systems. An improved version of this technical documentation could cover information about the various technical measures implemented through the AI lifecycle to prevent the occurrence of risks, including market manipulation. Enhanced disclosure can lead to higher standards of human accountability and better ensure human liability for cases of AI errors, misuses, and abuses.

(iv) "Transparency"

Ensuring high levels of transparency in AI systems is key for trustworthy adoption. The EU AI Act's transparency requirements, which are more detailed than those in MiFID II, need to be addressed from the early stages of the AI lifecycle. This "technical transparency" aims to ensure that AI systems are used appropriately by deployers and remain compliant with regulation for both providers and deployers.[165] To this end, the EU AI Act mandates detailed information and instructions,[166] with a focus on AI "explainability". This information must cover the technical capabilities and characteristics of AI systems, enabling human experts to interpret and explain AI outputs.[167] Additionally, this form of technical transparency should detail the human-machine interfaces designed to facilitate interpretability/explainability.[168]

By contrast, MiFID II does not stipulate equally detailed transparency requirements. However, it is reasonable to assume that when investment firms use third-party software or AI components, some of this information would typically be included in the instructions for use or other documents. Financial firms retain legal responsibility and, thus, must possess sufficient knowledge and documentation to ensure regulatory compliance when procuring or outsourcing AI-related products or services.[169]

Transparency requirements are only effective if stakeholders have an adequate level of AI literacy. The EU AI Act addresses this by establishing requirements for staff involved in the operation and use of AI systems.[170] This requirement is similarly reflected in sectoral legislation. For instance, compliance staff are required to possess a general understanding of how trading systems work and maintain regular contact with specialized staff members who have domain-specific expertise.[171]

[165] EU AI Act, art. 13(1).
[166] See *ibid*., art. 13(2) and (3)
[167] See *ibid*., art. 13(3)(b)(iv) and (vii).
[168] See *ibid*., art. 13(3)(d).
[169] See RTS 6, art. 4.
[170] Cf. EU AI Act, art. 4.
[171] RTS 6, art. 2(1).

Overall, similar to the EU AI Act, MiFID II mandates *strong* "transparency" requirements for AI trading systems *de jure*.[172] Yet, these high standards of transparency may actually be only marginally enforced *de facto*.[173] This is primarily due the outcome-based nature of algorithmic trading regulation, which focuses on observable market conduct rather than ensuring effective transparency and explainability of AI systems throughout the AI lifecycle.

(v) "Human oversight"

Fundamentally, the "human oversight" requirements in both pieces of EU legislation share the same objective: namely, ensuring that AI deployers are in a position to understand, interpret, and control the behavior of their AI systems. Under the EU AI Act, human oversight must be meaningful and aimed at mitigating risks from AI use and misuse. The intensity of oversight should be proportional to the nature, complexity, and the inherent risks of specific applications. Among other things, control systems should empower human experts to monitor AI operations,[174] address "automation bias",[175] interpret AI outcomes,[176] and, if necessary, take control and interrupt the systems as a last resort.[177]

MiFID II has similar requirements, incorporating the "human-on-the-loop"[178] approach as a minimum standard. Human oversight is implemented through various systems and controls. For instance, to prevent market manipulation, investment firms are required to monitor trading activity using automated surveillance systems. These systems must generate alerts and reports, provide actionable insights also through visualization tools, and facilitate subsequent investigation and corrective measures.[179] Additionally, staff overseeing trading activities must always be able to promptly halt trading to avert market disturbances (i.e. kill functionality).[180] While these control systems may mitigate some of the more obvious market harms, they may not be sufficient to prevent the subtler instances of market manipulation made possible by advanced ML methods. In regulating the relationship between providers and deployers of AI systems, the EU AI Act requires providers to provide information and technical documentation to ensure meaningful human control and human-computer interaction.

All in all, the EU AI Act's approach to human oversight draws inspiration from algorithmic trading regulation but is more detailed due to its broader protective scope. While MiFID II focuses on preventing AI systems from exceeding limits related to market risk and conduct, it follows an outcome-based approach. Thus, firms in algorithmic trading are not mandated to provide detailed documentation on human oversight unless requested by competent authorities. By contrast, the EU AI Act

[172] See Adrien Bibal et al., "Legal Requirements on Explainability in Machine Learning" (2021) 29 Artificial Intelligence and Law 149, 164.

[173] Azzutti, Ringe, and Stiehl I, *supra* note 12 at 126.

[174] EU AI Act, art. 14(4)(a).

[175] *Ibid*., art. 14(4)(b).

[176] *Ibid*., art. 14(4)(c).

[177] *Ibid*., art. 14(4)(e).

[178] The term "human-on-the-loop" describes AI applications where humans monitor and can intervene in automated processes, such as stopping the systems when necessary. For a discussion of the various approaches to human oversight of AI systems and their relationship to the EU AI Act, see Lena Enqvist, "'Human Oversight' in the EU Artificial Intelligence Act: What, When and by Whom?" (2023) 15:2 Law, Innovation and Technology 508.

[179] See RTS 6, art. 13.

[180] See *ibid*., art. 12.

mandates comprehensive documentation and proactive measure to ensure effective human oversight.

(c) Toward A Risk-Based Regulation Of AI Trading Systems

Recognizing that algorithmic trading regulation may have yet to keep pace with the rapid advancements in AI technology, the question remains how to bridge this gap. Our comparison above reveals that the EU AI Act's regulatory requirements for *providers* of "high-risk" AI systems are more prescriptive than those for *deployers* of algorithmic trading under MiFID II. Given the specific characteristics of the financial trading sector, not all of the EU AI Act's requirements may be suited to algorithmic trading. However, some provisions could benchmark future regulatory improvements or at least inform regulatory compliance guidance set by financial regulators, particularly in cases where financial firms develop their AI systems in-house. In instances where AI trading systems, or significant components thereof, are provided by third-party vendors, the relevant requirements could also extend to these entities.

Nevertheless, as a first step, one should determine to what extent AI applications in financial trading can be considered "high-risk". In the EU AI Act, indeed, financial trading is not classified as a "high-risk" domain. This is primarily justified by the fact that financial AI applications involve purely economic risks, which hence are beyond the regulatory scope of the EU AI Act.[181] Some scholars contend that the definition of "high-risk" AI systems is under-inclusive and problematic, as it omits certain AI applications in areas of high societal risk. Due to their potential risks to financial stability, AI applications in capital markets clearly exemplify this concern.[182]

A combined reading of the goals pursued by the EU AI Act with those of EU financial regulation may support a new regulatory approach to AI governance in finance.[183] However, it is prudent to refrain from categorizing all AI applications in financial trading as "high-risk" for at least three reasons. First, not all applications present the same risks. The riskiness of AI trading systems varies according to their specific techno-methodic characteristics (e.g., autonomy and opacity) and their actual market operating capabilities.[184] Second, a one-size-fits-all regulatory approach would unnecessarily increase compliance costs for all applications, discourage AI use, and reduce competition, leading to market concentration and negatively affecting market participation and efficiency. Third, implementing stricter regulations for all AI trading systems would place a heavier burden on competent authorities, potentially leading to a significant depletion of already limited enforcement resources.[185] Regulators tend, in fact, to concentrate on a select number of high-risk activities rather than spreading their resources thinly across numerous lower-risk ones.

Therefore, an innovative and more appropriate regulatory framework for AI in specific application domains, such as financial trading, should be based on a risk-based approach.[186] In other words, instead of classifying only certain domains as "high-risk", a more practical alternative would be to fractally replicate the EU AI Act's

[181] See Sciarrone Alibrandi, Rabitti, and Schneider, supra *note* 156 at 18.

[182] Anat Keller, Clara Martins Pereira, and Martinho Lucas Pires, "The European Union's Approach to Artificial Intelligence and the Challenges of Financial Systemic Risk", in Henrique Sousa Antunes et al., eds, *Multidisciplinary Perspectives on Artificial Intelligence and the Law* (Springer, 2024) at 415.

[183] See, e.g., Sciarrone Alibrandi, Rabitti, and Schneider, supra *note* 156 at 32.

[184] Azzutti, Ringe, and Stiehl II, *supra* note 12 at 234.

[185] Cf. Julia Black and Robert Baldwin, "Really Responsive Risk-Based Regulation" (2010) 32:2 Law & Policy 181.

[186] This approach was first proposed in Azzutti, Ringe, and Stiehl II, *supra* note 12.

risk-based approach within individual application domains. In addition to financial trading, this concept has also gained ground in other contexts.[187] Yet, the initial challenge for regulators will be to establish a comprehensive framework to effectively differentiate AI applications based on their specific risk levels. This is by no means an easy task. A potential approach, however, could be to classify financial AI applications using a three-dimensional framework based on (i) the specific ML methods involved in an AI system ("*Methods*"), (ii) the system's capabilities to interact with the market environment ("*Capability*"), and (iii) the resulting risks in terms of market misconduct, market disruption, and financial stability ("*Materiality*").[188] The riskiness of a given application would therefore depends on the specific combination of these three factors, each of which may assume different dimensions according to a pre-defined measuring system. To illustrate, when considering the "*Methods*", regulators must understand the underlying technology and grade different ML methods in terms of riskiness (e.g., in terms of autonomy, levels of opacity, etc.). In evaluating the "*Capabilities*", regulators should assign different risk weights to the various tasks that AI systems may perform. For instance, an AI system that only "senses" the world without making final financial decisions could generally be perceived as less risky than an end-to-end AI system. Lastly, when addressing "*Materiality*", regulators must identify and evaluate the characteristics of risks related to specific applications (e.g., considering factors such as trading strategies, market access, risk management, etc.). Accordingly, the overall level of riskiness of a given AI application will result from the precise combination of the three risk factors and their corresponding weights.

Admittedly, this is only a preliminary proposal; numerous other possible alternatives are undoubtedly available. Given its rudimentary nature, the proposed framework aims to initiate debate and raise awareness within the regulatory community rather than offer a universal and definitive solution. Nonetheless, if an appropriate and reliable classification framework can be established, adequately calibrated regulatory requirements could be applied proportionately to different financial AI applications according to their risks. While current technology governance frameworks may suffice for less risky AI trading systems, they fall short for higher-risk ones. As shown in this Article, the EU AI Act's regulatory requirements for "high-risk" applications could serve as a blueprint for strengthening the regulation of riskier AI trading systems to the extent that they contribute to safeguarding high standards of transparency, auditability, human agency and accountability.

Ultimately, the proposed risk-based regulatory involves leveraging tailored rules, instead of principles alone, to ensure trustworthy AI adoption in financial trading. If done right, this improved form of "technology governance by regulation" could address and even anticipate potential market failures associated with the latest AI generations. Based on standard economic theory, the proposed approach is intended to tackle three main types of market failures: (i) negative externalities (e.g., market manipulation), (ii) information asymmetries (e.g., due to lack of AI

---

[187] See Claudio Novelli et al., "Taking AI Risks Seriously: A New Assessment Model for the AI Act" (2023) AI & Society; Claudio Novelli, "AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act" (2024) 3:13 Digital society 1; Alessio Azzutti, Pedro Magalhães Batista, and Wolf-Georg Ringe, "Good Administration in AI-Enhanced Banking Supervision: A Risk-Based Approach" (2024) Columbia Journal of European Law (forthcoming), working paper version (27 April 2023) available at: https://dx.doi.org/10.2139/ssrn.4430642.

[188] Azzutti, Ringe, and Stiehl II, *supra* note 12 at 237-238, building upon the proposal by Thomas Schmid et al., "The AI Methods, Capabilities and Criticality Grid" (2021) 35 KI – Künstliche Intelligenz 425.

transparency/explainability), and (iii) moral hazard (e.g., by AI providers and deployers).

5. CONCLUSION

This Article explores the ongoing struggle between law and technology through the lens of AI adoption within the domain of algorithmic trading. By conceptualizing three main AI generations characterized by increasing technological complexity, it examines how advances in financial AI research and practice have amplified the complexity of capital markets. This AI-spurred complexity exposes markets to new risks and poses significant challenges for regulatory frameworks. To exemplify these challenges, the Article addresses the new and heightened risks of market manipulation and even algorithmic collusion due to innovative ML approaches. Considering these risks, it identifies the main shortcomings of existing regulatory frameworks for ensuring effective AI governance.

Addressing these limitations, this Article underscores the necessity for regulations to keep pace with the increasing complexity of technology and capital markets. It advocates for complexity-informed AI regulation in financial trading. This approach does not mean more complicated rules but instead rules deeply rooted in a comprehensive understanding of AI, its real-world applications, and the related capabilities and associated risks. In this context, the Article argues that, compared to the EU AI Act, MiFID II's requirements on algorithmic governance may not fully address the risks posed by specific AI applications in high-risk domains like capital markets. Therefore, inspired by the risk-based regulatory approach of the EU AI Act, this Article proposes a fractal replication of risk-based regulation to the algorithmic trading domain, hence mandating more prescriptive requirements for those AI trading systems that present higher risks to markets.

Overall, the insights offered by this Article, coupled with the momentum around AI regulation, offer an opportunity to strengthen financial regulation, especially in the highly AI-dependent domain of algorithmic trading. However, whether financial regulators alone can undertake this task remains to be determined. Enhanced collaboration between financial and technology regulators will likely become essential to tackle the seemingly insurmountable challenges of AI governance in finance.