Azzutti, Alessio

Working Paper

AI-driven Market Manipulation and Limits of the EU law enforcement regime to credible deterrence

ILE Working Paper Series, No. 54

Provided in Cooperation with:
University of Hamburg, Institute of Law and Economics (ILE)

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

FAKULTÄT
FÜR RECHTSWISSENSCHAFT

INSTITUTE OF LAW AND ECONOMICS
WORKING PAPER SERIES

AI-driven Market Manipulation and Limits of the EU law enforcement regime to credible deterrence

Alessio Azzutti

Working Paper 2022 No. 54

January 2022

Photo by UHH/RRZ/Mentz

AI-driven Market Manipulation and Limits of the EU law enforcement regime to credible deterrence

Alessio Azzutti [*]

Abstract

As in many other sectors of EU economies, 'artificial intelligence' (AI) has entered the scene of the financial services industry as a game-changer. Trading on capital markets is undoubtedly one of the most promising AI application domains. A growing number of financial market players have in fact been adopting AI tools within the ramification of algorithmic trading. While AI trading is expected to deliver several efficiency gains, it can also bring unprecedented risks due to the technical specificities and related additional uncertainties of specific 'machine learning' methods.

With a focus on new and emerging risks of AI-driven market manipulation, this study critically assesses the ability of the EU anti-manipulation law and enforcement regime to achieve credible deterrence. It argues that AI trading is currently left operating within a (quasi-)lawless market environment with the ultimate risk of jeopardising EU capital markets' integrity and stability. It shows how 'deterrence theory' can serve as a normative framework to think of innovative solutions for fixing the many shortcomings of the current EU legal framework in the fight against AI-driven market manipulation.

In concluding, this study suggests improving the existing EU anti-manipulation law and enforcement with a number of policy proposals. Namely, (i) an improved, 'harm-centric' definition of manipulation; (ii) an improved, 'multi-layered' liability regime for AI-driven manipulation; and (iii) a novel, 'hybrid' public-private enforcement institutional architecture through the introduction of market manipulation 'bounty-hunters'.

Keywords: algorithmic trading; artificial intelligence; market manipulation; market integrity; effective enforcement; credible deterrence.

JEL Codes: G18, G28, G38, K14, K22, K42, O33, O38

[*] PhD Candidate in Law at *Universität Hamburg*. Corresponding author at: Johnsallee 35, 20148, Hamburg, Germany. *E-mail address:* alessio.azzutti@ile-hamburg.de

1. Introduction

Regulatory struggle to keep up with the pace of technological innovation is a phenomenon that has always been present in the world of finance.[1] With technological innovation moving faster than legal and regulatory reform, lawmakers' capability to safely regulate disruptive technology without stifling innovation becomes questionable.[2] As a recent market development, challenges inherent in regulating algorithmic trading clearly show this fundamental tension between law and technology in finance.[3] Exactly under this lens, this paper aims at demonstrating how core legal instruments of EU capital markets law, such as the MAR[4]/MAD[5] legislations, can become obsolete as algorithmic trading technology evolves in sophistication and complexity thanks to constant and spectacular progress in the field of artificial intelligence (AI). Undoubtedly, AI is considered the main game-changer in today's socio-economic system. But both misuses of and unintended consequences from using AI raise several ethical and legal questions, which require careful consideration and may even justify some precautionary regulatory intervention.[6] In finance, for instance, AI approaches to algorithmic trading can expose markets to new and emerging risks, including novel forms of market manipulation.[7] Yet whenever market manipulation passes undetected and thus is left unprosecuted, it can ultimately jeopardise markets' safety and integrity, thus impairing investor protections and confidence until the point of putting the stability of the global financial system at risk.[8]

While algorithmic trading can contribute to market quality through different channels,[9] its impact on market integrity is still a legal and regulatory conundrum. Specifically, a growing number of scholars claim, on different grounds, that financial law and regulation still lack behind actual technological developments within the ramification of algorithmic trading.[10] In the same vein, this paper addresses critical legal issues arising from new and emerging threats to capital markets' integrity led by the most advanced AI approaches to financial trading. Algorithmic market manipulation is generally a somewhat complex financial crime to regulate, detect and prosecute. Whereas supervisors' lack of resources and expertise can hamper their ability to detect market abuse, prosecution becomes ineffective if it cannot target responsible individuals. In this last regard, establishing individuals' exact liability contribution might be tricky for misconduct and harm by algorithmic trading. AI agency further exacerbates already well-known issues in the enforcement of market conduct rules. As it will be argued, whenever not adequately developed, tested, and supervised by human experts, AI trading can lead to a number of unintended consequences, including optimised forms of market manipulation, which can ultimately undermine capital markets' stability and integrity.

---

[1] cf Dan Awrey and Kathryne Judge, 'Why Financial Regulation Keeps Falling Short' (2020) 61 Boston College Law Review 2295.

[2] See, e.g., Mark D. Fenwick, Wulf A. Kaal and Erik P.M. Vermeulen, 'Regulation Tomorrow: What Happens When Technology Is Faster than the Law?' (2017) 6 American University Business Law Review 561.

[3] See Tom C.W. Lin, 'The New Financial Industry' (2014) 65 Alabama Law Review 567.

[4] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC [2014] OJ L173/1 [hereinafter MAR].

[5] Directive 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 L173/179 [hereinafter MAD].

[6] Roger Clarke, 'Regulatory Alternatives for AI' (2019) 35 Computer Law & Security Review 389.

[7] Alessio Azzutti, Wolf-Georg Ringe and H. Siegfried Stiehl, 'Machine Learning, Market Manipulation and Collusion on Capital Markets: Why the "Black Box" Matters' (2021) 43 University of Pennsylvania Journal of International Law 79.

[8] See Gina-Gail Fletcher, 'Macroeconomic Consequences of Market Manipulation' (2020) 83 Law and Contemporary Problems 123.

[9] Ekkehart Boehmer, Kingsley Fong and Juan (Julie) Wu, 'Algorithmic Trading and Market Quality: International Evidence' (2020) 56 Journal of Financial and Quantitative Analysis 2659.

[10] For some recent studies addressing the challenges of the EU capital markets law in regulating algorithmic trading, see: Carsten Gerner-Beuerle, 'Algorithmic Trading and the Limits of Securities Regulation' in Emilios Avgouleas and Heikki Marjosola (eds), *Digital Finance in Europe: Law, Regulation, and Governance* (De Gruyter 2022) 109; Patrick Raschner, 'Algorithms put to test: Control of algorithms in securities trading through mandatory market simulations?' (2021) European Banking Institute Working Paper Series 2021 - no. 87 <https://ssrn.com/abstract=3807935> accessed 16 January 2022; Clara Martins Pereira, 'Unregulated Algorithmic Trading: Testing the Boundaries of the European Algorithmic Trading Regime' (2021) 6 Journal of Financial Regulation 270; Matteo Gargantini, *The European Regulation of Securities Exchanges: Regulated Markets in an Evolving Technological and Legal Context* (Giappichelli Editore, 2021).

With all these risks in mind, this paper aims to critically evaluate the effectiveness of the current EU anti-manipulation legal framework *vis-à-vis* novel forms of AI-driven manipulation. The main goal is to identify the shortcomings in the EU enforcement regime to credibly deter and effectively punish AI trading misconduct and harm. We proceed as follows. From a high-level perspective, **Section 1** discusses how constant progress in AI techniques and ML methods revolutionise today the financial trading industry and highlights the main technical specificities of the most promising AI trading systems and strategies based on ML. It shows how AI-driven trading can lead to additional uncertainty for financial regulators in pursuing their institutional mandate, focusing on enforcement issues of market conduct rules. Next, **Section 2** examines the current EU anti-manipulation law applied to algorithmic trading. It assesses possible sources of regulatory failures in achieving effective enforcement due to AI trading operating within highly fragmented EU capital markets, characterised by enhanced cross-border activity. Borrowing from the law and economics scholarship, **Section 3** applies 'deterrence theory' to the law enforcement puzzle led by AI-driven market manipulation. It shows how deterrence theory can serve as a practical normative framework for evaluating the limits of the EU anti-manipulation enforcement regime's effectiveness. Hence, **Section 4** explores some reform ideas to enhance and improve EU instruments in the fight against AI trading manipulation to achieve credible deterrence within increasingly digital, integrated, but fragmented EU capital markets. **Section 5** concludes.

2. AI trading and market manipulation: a primer

In the current hype about the promises of technological innovation, AI is often presented as the real game-changer for many sectors of the economy. There is, in fact, enormous and growing enthusiasm for the potential that AI proposes to offer, mainly for reasons of greater economic efficiency as well as wider socio-economic benefits.[11] This is undoubtedly also the case for the financial services sector. Indeed, there is increasing evidence that a growing number of organisations have been researching, developing and deploying AI solutions for a wide-ranging number of business tasks.[12] Mainly, the benefits led by AI approaches to financial trading are twofold. On the one hand, the use of AI can ensure that companies deploy their resources and make decisions under conditions of uncertainty in a more operationally efficient manner.[13] On the other, the competitive edge offered by AI can translate into more favourable market conditions and increased allocative efficiency for consumers, investors, and society.[14] Not surprisingly, therefore, AI solutions are expected to widespread among investment firms, asset management firms, credit institutions, and other financial organisations alike.

Yet, delegating cognitive agency and decision-making tasks to increasingly *intelligent*[15] and autonomous machines brings with it a whole set of new risks and related ethical and legal questions that regulators urge to consider to pursue their institutional mandates effectively while avoiding to stifle social welfare-enhancing innovation. In the financial trading context, this means that innovation in AI can deliver expected benefits without jeopardising capital markets' safety and integrity.

---

[11] See generally James Eager et al, 'Opportunities of Artificial Intelligence' (2020) Study Requested by the ITRE committee, European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies, DG for Internal Policies, PE 652 713, 35-45 <www.europarl.europa.eu/RegData/etudes/STUD/2020/652713/IPOL_STU(2020)652713_EN.pdf> accessed 16 January 2022.

[12] See Bank of England and U.K. Financial Conduct Authority, *Machine learning in UK financial services* (2019) <www.bankofengland.co.uk/-/media/boe/files/report/2019/machine-learning-in-uk-financial-services.pdf> accessed 16 January 2022; IOSCO, *The use of artificial intelligence and machine learning by market intermediaries and asset managers* (2021) <www.iosco.org/library/pubdocs/pdf/IOSCOPD684.pdf> accessed 16 January 2022.

[13] See Financial Stability Board, *Artificial intelligence and machine learning in financial services* (2017) 24-25 <www.fsb.org/wp-content/uploads/P011117.pdf> accessed 16 January 2022.

[14] ibid, 25-27.

[15] With the term 'intelligence', this study does not refer to general human or animal intelligence but instead to the computational ability of a specific AI system or agent to self-learn and adapt autonomously to its environment through its own experience while pursuing a pre-defined business goal. For a discussion on the difference between human, animal and artificial forms of intelligence, their complementarities and possibilities for combination, see Dominik Dellermann, Philipp Ebel and Jan Marco Leimesiter, 'Hybrid Intelligence' (2019) 61 Business & Information Systems Engineering 637.

2.1 Algorithmic trading and AI

From a historical perspective, algorithmic trading can be seen as one of the first use cases where some AI techniques were first implemented.[16] In general, algorithmic trading refers to technologically-enabled modes of financial trading leveraging the use of computer algorithms to automate fully, or only in part, tasks within the trading cycle.[17] AI approaches to algorithmic trading can apply to several tasks, such as pre-trade analytics, trading strategy selection, order routing and execution management, as well as post-trade analytics.[18] At their origin, however, algorithmic trading entailed basic AI techniques, known as 'expert systems'. This first generation of AI-empowered trading algorithms was rather rudimental in their algorithmic inner functioning. The beauty – but, at the same time, their principal limit – relied on a very deterministic approach to assist human experts in financial decision-making. Specifically, 'expert systems', also known as 'knowledge-based' AI, were profoundly constrained by human experts' knowledge and assumptions about and within a particular application domain. Their operations worked according to pre-defined and straightforward commands and heuristics, such as "*if/then*".[19] However elementary these first generations of AI-driven trading had been, those were still able to complicate the work of public authorities in the oversight and enforcement of market conduct rules. Even if one could grasp human developers' true motives by observing algorithms' operations and gaining insights from their inner functioning (*i.e.*, the code), the fact that algorithmic trading systems always operate within highly complex and interconnected market environments makes traditional legal concepts of liability (such as 'intent', 'causation' and 'foreseeability') not entirely applicable.[20] Most advanced AI approaches can only be expected to complicate this issue further.

Thanks to increased data availability, in both quantity and quality, and progress in computational power, a new generation of AI algorithms has emerged, among which 'machine learning' (ML) methods have gained a prominent role. In simple terms, ML is a sub-field of AI comprising different learning paradigms.[21] Without the need to enter too much into technical details, it may suffice to say that, thanks to ML methods, most-advanced trading algorithms are able today to self-learn from input data without constant human control and oversight. According to the specific ML methods employed, self-learning can occur via training by human experts and/or through own interaction within a specific market environment. For instance, some ML methods (*e.g.*, 'deep reinforcement learning') allow for establishing artificial agents that, by trial and error, can autonomously find the best way to optimise a pre-defined objective – most likely a profit-maximisation one under some risk constraints – without necessarily requiring any specific prior knowledge about the environment in which they are called to operate.[22] ML methods are generally proposed to augment human capabilities in detecting patterns and meaningful correlations from data used for subsequent financial decision-making.[23] In highly fragmented and increasingly digital markets, finding profitable trading opportunities requires delving into an increasingly abundant bunch of data of a very different quality to get a competitive advantage over the crowd and, thus, ensure 'alpha' returns. As a solution, humans can create algorithmic

[16] cf Dave Cliff, Dan Brown and Philip Treleaven, 'Technology Trends in the Financial Markets: A 2020 Vision' (UK Government Office for Science, 2011) <www.bis.gov.uk/assets/bispartners/foresight/docs/computer-trading/11-1222-dr3-technology-trends-in-financial-markets.pdf> accessed 16 January 2022.

[17] Andrei A. Kirilenko and Andrew W. Lo, 'Moore's Law versus Murphy's Law: Algorithmic Trading and Its Discontents' (2013) 27 Journal of Economic Perspectives 51, 52 ("the use of mathematical models, computers, and telecommunications networks to automate the buying and selling of financial securities").

[18] See Fethi A. Rahbi, Nikolay 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 Financial Industry, 10th International Workshop, FinanceCom 2020, Helsinki, Finland, August 18, 2020* (Springer 2020).

[19] See Philip Treleaven, Michal Galas and Vidhi Lalchand, 'Algorithmic Trading Review' (2013) 56(11) Communications of the ACM 76 <https://cacm.acm.org/magazines/2013/11/169035-algorithmic-trading-review/pdf> accessed 16 January 2022.

[20] Yesha Yadav, 'The Failure of Liability in Modern Markets' (2016) 102 Virginia Law Review 1031.

[21] For a first introduction to different machine learning models and their respective applications in algorithmic trading, see Adriano Koshiyama, Nick Firoozye and Philip Treleaven, 'Algorithms in Future Capital Markets' (2020) Proceedings of ACM ICAIF '20 <https://dl.acm.org/doi/pdf/10.1145/3383455.3422539> accessed 16 January 2022.

[22] Azzutti, Ringe, and Stiehl (n 7) 90-92.

[23] ibid, 86-90.

trading systems and strategies able to explore and find, with increased autonomy, profitable investment and trading opportunities, which are no more intelligible by the sole human mind.[24]

- ***AI trading technical specificities and additional risks***

Notwithstanding all expected benefits for private firms, their clients and society at large, real-life AI applications can also entail significant side effects as long as their development and implementation are not supported by sound regulation given emerging risks to people safety and fundamental rights.[25] Indeed, the most powerful and promising ML methods can lead to additional uncertainties and risks, especially whenever implemented in *high-risk* domains such as capital markets.[26] For instance, whenever AI results in wrongdoing and harm, fundamental ethical and legal questions of liability arise. Importantly, these additional risks are intimately linked to specific ML methods' very technical specificities, which read as follows.

- *'Complexity' and 'connectivity'*. Increased complexity and connectivity are both general problems relating to IT systems.[27] Today, most advanced algorithmic trading systems ought to be conceived as real *ecosystems* of algorithms.[28] Different software components run and interact in AI ecosystems thanks to and on complex nets of IT hardware elements. Together, they work to operationalise partly or the whole trading cycle, according to pre-set specific business goals. Building such algorithmic ecosystems requires a vast amount of specific domain knowledge, including, *inter alia*, data science, computer programming, financial theory and capital markets law and regulation. Thus, it usually involves a relatively vast number of human experts from very different professional backgrounds that, only by joining forces, can put together all the skills required to assemble and deploy profitable trading systems and strategies successfully and reliably. However, the more complex and interconnected an AI system is, the more likely it could behave in unexpected ways even when users act with due care.[29] Thus, whenever something goes wrong and results in harm to others, substantial legal issues of liability arise.
- *'Correlation' versus 'causation'*. ML methods are data-driven empirical techniques that establish knowledge by induction from data correlations identified within a given dataset. Instead of enquiring about causation among parameters, ML approaches are called to look for patterns and statistical correlations in the data. This significant paradigm change in financial practice fuelled by ML approaches to data analysis could lead to a fundamental shift in financial theory from 'causation' to 'correlation'.[30] While focusing on correlation can provide fast and cost-saving approaches to data analysis, informing decision-making without any causation enquiry (*i.e.*, without being supported by a reliable and robust mathematical theory) can negatively affect the quality of the AI process and result in unintended consequences or other biased outcomes.[31] Moreover, the widespread adoption of ML applied to algorithmic trading could even revolutionise both financial and statistical theory underlying financial decision-making under uncertainty.[32]
- *'Autonomy'*. Since the emergence of electronic trading, algorithmic trading systems have shown growing levels of autonomy. Thanks to ML methods and techniques, algorithmic trading enjoy today an even greater level of system autonomy until the point that, thanks to constant progress in AI, truly

---

[24] ibid, 85.

[25] See generally Daron Acemoglu, 'Harms of AI' (2021) NBER Working Paper 29247 <www.nber.org/papers/w29247> accessed 16 January 2022.

[26] To note, however, the business of financial trading is not labelled as a 'high-risk' AI application by the recently proposed EU approach to regulating AI. See Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act)' COM/2021/206 final.

[27] Martin Ebers, 'Regulating AI and Robotics: Ethical and Legal Challenges' in Martin Ebers and Susana Navas (eds) *Algorithms and Law* (CUP 2020) 44.

[28] cf Koshiyama, Firoozye and Treleaven (n 21).

[29] Yadav (n 20) 1059 and 1077-1079.

[30] cf Ebers (n 27) 45.

[31] ibid, 46.

[32] cf Stefan Nagel, *Machine Learning in Asset Pricing* (PUP 2021) (discussing how the application of ML methods in asset pricing can foster advances in theoretical modelling o financial markets).

autonomous AI trading systems and agents will emerge.[33] However, with increased autonomy, algorithmic trading raises severe questions of liability for market misconduct and harm. Traditional legal concepts of liability such as 'intent', 'causation' or 'foreseeability' can find no safe application from both a conceptual and legal point of view. Due to self-learning capabilities, AI trading can indeed pose severe challenges to guaranteeing accountability and assigning responsibility, as human experts do not explicitly program the AI behaviour anymore. In fact, AI trading behaviour is trained and learned on a vast amount of training data to develop autonomously by learning from historical examples or own experience within a specific market environment. Therefore, autonomous and self-learning AI trading raises serious questions about liability for misconduct and harm. This is mainly because enforcement bodies would potentially need to ascertain liability among a relatively significant number of human experts. Each of which share some responsibility for designing, developing, using, and monitoring the AI trading systems, thus, rendering enforcement action practically not feasible.[34]

- *'Opacity' (or the "black-box" problem).* One much-debated concern proper to most advanced ML methods and techniques refers to the opacity of specific algorithmic decision-making systems. Specifically, the so-called 'black box' problem can arise whenever human experts cannot fully predict, understand and explain why and how their algorithms have reached a particular solution/decision given specific data input.[35] Very diverse, however, can be the causes for opacity in various ML methods.[36] At the very basic level, opacity can be the result of a design choice by firms using AI to keep secret the details about the inner functioning of their trading algorithms to guarantee themselves a competitive advantage.[37] Alternatively, opacity can be an unintended consequence because of a lack of specialised skills for the design and development of AI systems.[38] Finally, opacity can be an unavoidable consequence due to the high degree of system complexity of specific ML methods (*e.g.*, deep learning), allowing for algorithmic trading systems that can dynamically learn.[39] While these ML methods can allow for powerful optimisations and improved accuracy, their outcome and behaviour can be highly opaque.

Overall, because of specific ML methods' technical specificities, AI agency can lead to 'accountability gaps' for algorithmic trading misconduct and harm. Whenever most advanced AI trading systems learn to misbehave and cause harm to others in the course of their autonomous activity, traditional liability rules will fail to apply safely. In effect, AI-driven misconduct and harm can either result from humans' flawless development of AI, be an unintended consequence due to the system's interaction with different agents, both human and algorithmic, in a complex and interconnected environment such as global capital markets, or even due to autonomous behaviour of increasingly intelligent AI systems able to self-learn.

2.2 AI-driven market manipulation: mapping the risks

As an economic phenomenon, market manipulation refers to any market conduct aiming at influencing natural market forces of supply and demand, or the price of a given (or more) financial instrument(s), in a non-natural way, through a deliberate attempt to impact those forces.[40] Because market manipulation has the effect of undermining the informativeness of market prices and the fair functioning of markets, it constitutes a form of market failure that leads to an inefficient allocation of resources.[41] As such, market manipulation creates negative externalities, the harmful effects of which cannot be eliminated by market forces alone. For these reasons, in most-advanced jurisdictions, market manipulation is generally prohibited and often criminally prosecuted as a form of market abuse. Nevertheless, AI trading can alter traditional crime scenes of market

[33] Azzutti, Ringe, and Stiehl (n 7) 90-92.

[34] ibid, 121-22.

[35] ibid, 89-90.

[36] Jenna Burrell, 'How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms' (2016) 3 Big Data & Society <https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512> accessed 16 January 2022.

[37] ibid, 3.

[38] ibid, 4.

[39] ibid, 4-5.

[40] Emilios Avgouleas, *The Mechanics and Regulation of Market Abuse: A Legal and Economic Analysis* (OUP 2005) 107.

[41] ibid, 4 ("[i]t is widely admitted that no behaviour is a more potent enemy of market efficiency and bigger destroyer of investor confidence than market abuse").

manipulation. Not only AI trading can optimise old-fashioned manipulative strategies by making their economic performance faster, cheaper and more secure; but, thanks to AI greater analytical power and enhanced connectivity, it can also lead to new and more complex forms of manipulation.[42] In the following, we examine these risks.

- ***Scenarios of AI-driven manipulation***

In principle, there are at least four different scenarios in which an AI system can be involved in misconduct or crime – like market manipulation. **First**, AI can be part of an accident or a crime as victim itself.[43] Imagine, for instance, the case of a cybersecurity breach where a third-party malicious actor (*e.g.*, a terrorist group) seeks to sabotage the ordinary functioning of an AI trading system as to damage society. AI hacking could either be done by exploiting its technical vulnerabilities (*e.g.*, through corrupting the training dataset) or disenabling some of the AI functionalities.[44] As a result, the AI system can thus fail to achieve its pre-defined business goals and/or be induced to commit a crime itself, independently from the willingness of the AI developers and users. **Second**, an AI system can work in unexpected ways even when its developers and users take due care. For instance, AI unexpected behaviour could be due to a mere operational failure such as a bug in the system. Under this scenario, AI could therefore cause market disruptions or even 'mistakenly' engage in some forms of manipulation.[45] **Third**, also malicious human actors can consciously design, develop, and use AI trading to put in place profitable financial crime such as a manipulative scheme.[46] In these cases, assessing liability for AI misconduct and harm can be difficult, as it requires enforcement authorities being equipped with adequate tools, resources, and expertise. Finally, there is also a **fourth** and more problematic scenario, which can complicate the work of both enforcement authorities, which are in charge of protecting markets from abuses, and investment firms alike, which instead need to comply with market conduct rules. Under this trickiest scenario, AI algorithmic trading systems are so advanced that they can discover ways to game market rules autonomously while pursuing a pre-defined business goal, regardless of human intent. This way, manipulation can occur thanks to AI self-learning from own experience through the observation of and trading activity on markets.[47]

- ***AI-driven manipulative strategies***

As the core of AI is about solving optimisation problems mathematically, it is envisaged that AI will well serve the purpose of malicious actors looking for ways to optimise their manipulative algorithmic strategies to the detriment of other market participants. However, AI trading can also learn to misbehave autonomously in a rational way regardless of human intent and even negligence while pursuing its pre-set trading objectives. Overall, distinguishing between these two scenarios will be increasingly challenging for enforcement bodies and victims alike. Whenever this is the case, malicious or negligent actors will so externalise to other market participants and society as a whole the costs of their practices. Indeed, there is growing evidence of the possibility to use AI methods to optimise some algorithmic and particularly high-frequency trading (HFT) forms of manipulation. Without pretending of being exhaustive, examples can include: (*i*) *deceptive* strategies,

[42] Azzutti, Ringe, and Stiehl (n 7) 118.

[43] See generally Lorenzo Pupillo, Stefano Fantin, Afonso Ferreira and Carolina Polito, 'Artificial Intelligence and Cybersecurity: Technology, Governance and Policy Challenges' (2021) CEPS Task Force Report, Brussels, 57-59 <www.ceps.eu/download/publication/?id=33262&pdf=CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf> accessed 16 January 2022.

[44] ibid, 59-62.

[45] Azzutti, Ringe, and Stiehl (n 7) 116-17.

[46] ibid, 117-18.

[47] ibid, 118-19.

such as 'spoofing'[48], but also (*ii*) *aggressive* strategies, such 'pinging'[49] and 'momentum ignition'[50].[51] Moreover, thanks to enhanced analytical capabilities, and equipped with the ability to monitor and act on very different venues at the same time, AI trading can optimise and so better implement forms of 'cross-asset' and 'cross-market' manipulation.[52] To go even further, AI trading could also lead to new and more sophisticated forms of manipulation, by combining for instance elements of different strategies. Moreover, the widespread adoption by competing investment firms of AI trading agents has already warned policy-makers and academic scholars alike on emerging risks of herding behaviours and one-way markets, given the high degree of interconnectedness among algorithmic trading agents within digital capital markets.[53] It is believed that competing trading algorithms could more likely lead to the emergence of cartel-like behaviours in a novel fashion. Whereas in the past, competitors needed some form of 'explicit' communication to coordinate their behaviours, delegating decision-making tasks to AI agents can pave the way to 'tacit' forms of collusion. Particularly, competing algorithms could ultimately be able to reach sub-optimal market equilibria without any need for communication by solely relying on their superior analytical capabilities.[54] Some recent studies claim that, according to the specific techno-economic features of a given market segment, AI forms of collusion can occur whenever some conducive market factors for algorithmic forms of collusion to emerge are present.[55]

More generally, with greater analytical capabilities, speed of action, and market ubiquity, specific AI approaches to algorithmic trading can alter the traditional contours of manipulation. Specifically, it is envisaged that AI trading will change the spatio-temporal dimension of market events, such as flash-crashes, market manipulation, and their contagion effects. For instance, the fast and interconnected nature that characterises algorithmic trading can lead to ultrafast extreme events, including a number of instances of 'micro-manipulation'.[56] This way, AI can render easier and profitable those manipulative strategies, until now thought hard to accomplish, without facing substantial risks of being detected and punished. Conversely, this likely translates into insurmountable problems for regulators, supervisors, and enforcement authorities, with the effect of leaving markets exposed to abuse and harmed parties unable to protect their economic interests.

3. The EU anti-manipulation law and enforcement regime for algorithmic trading

The current EU anti-manipulation law is in its second generation.[57] It now consists of two legal instruments: namely (*i*) the MAR, establishing a common legal framework for the EU Member States on the prohibition of market abuse[58], complemented by (*ii*) the MAD, providing minimum harmonised rules for criminal sanctions targeting most serious cases of manipulation. Despite having it been largely reformed to address major market developments, including the 2007-8 global financial crisis and technological developments within the ramification of algorithmic trading,[59] there are several reasons to believe that the EU anti-manipulation

[48] 'Spoofing' refers to manipulative practices involving the submission and cancellation of trading orders without the real intention of execution with the effect of misleading other market participants as to the natural trading interest in a specific financial instrument.

[49] 'Pinging' refers to the strategy of placing small tradable orders to discover the presence of large hidden orders resting in deeper levels of the electronic book in a dark pool or exchange.

[50] 'Momentum refers to manipulative practices involving several trading orders with the aim of initiating or inflating a price trend on a financial instrument in order to encourage other market participants to trade in the same direction before opening/closing a position on more favourable terms.

[51] Azzutti, Ringe, and Stiehl (n 7) 98-100.

[52] ibid, 100-101.

[53] See OECD, *Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers* (2021) <www.oecd.org/finance/artificial-intelligence-machine-learning-big-data-in-finance.htm> accessed 16 January 2022.

[54] Azzutti, Ringe, and Stiehl (n 7) 109-12 (discussing 'reinforcement learning' algorithms as a case study).

[55] ibid, 104-08.

[56] cf Neil Johnson et al, 'Abrupt rise of new machine ecology beyond human response time' (2013) 3 Science Report 2627 <www.nature.com/articles/srep02627.pdf> accessed 16 January 2022.

[57] Sofie Cools, 'Public Enforcement of the Market Abuse Regulation' in Marco Ventoruzzo and Sebastian Mock (eds) *Market Abuse Regulation: Commentary and Annotated Guide* (OUP 2017) 64-70.

[58] According to the EU taxonomy, market abuse includes economic wrong phenomena such as insider dealing (MAR artt 8 and 14), unlawful disclosure of insider dealing (MAR artt 10 and 14), and market manipulation (MAR artt 12 and 15).

[59] See MAR, recital (38).

framework is ineffective in dealing with novel risks led by advances in AI. This section addresses the scope of the EU prohibitions, liability rules and respective sanctions for algorithmic trading manipulation to highlight possible sources of enforcement failures.

3.1 The prohibition of algorithmic market manipulation

On a very general level, algorithmic forms of manipulation, such as 'trade-based'[60] and 'order-based'[61] manipulation, are covered by the legal definitions given by the EU MAR, defining market manipulation as a 'multi-layer' phenomenon.[62] Albeit not providing for a uniform and comprehensive legal definition, Article 12 MAR provides for a list of trading activities and behaviours that the EU legislator rules out and, by its enforcement, punishes as being highly detrimental to the integrity of EU capital markets. In addition, because the EU prohibition not only targets – and as such aims to deter – traders from engaging in manipulative practices but also outlaws any mere attempt to it,[63] the EU MAR seems seeking to solve the problem of deterrence at its very root. In other words, the deterrence effect of EU anti-manipulation law appears strengthened by putting every manipulative scheme on an equal footing, regardless of their actual economically successful implementation. At least in principle, thus, any attempt to distort natural market forces of demand and supply or market prices is strictly prohibited and punished.

Most-known algorithmic trading manipulative practices fall within the meaning of Article 12(1)(a). This provision refers to any trading conduct (*i.e.*, entering in a transaction, placing an order to trade or any other behaviours) that have, or is likely to have, the effect of either: (*i*) deceiving other market participants, by giving false or misleading signals as to the natural forces of supply and demand of a given financial instrument; or (*ii*) securing the price of one or more financial instruments at abnormal or artificial prices. Accordingly, the EU anti-manipulation law bans those algorithmic strategies that can cause distortions to natural market forces of supply and demand or market prices. As long as algorithmic trading strategies employ some sort of "fictitious device, or any other form of deception or contrivance", the above prohibition can overlap with the one given by Article 12(1)(b).[64] Arguably, the effective contours of market manipulation under MAR appear not clearly defined, with the risk of leaving markets with an uncertain legal prohibition,[65] especially when confronted with some algorithmic forms of manipulation. In principle, the MAR legal definition of market manipulation only includes objective elements: the EU legislator opted for some sort of 'effect-based' definition.[66] In effect, to count as an administrative offence, a given trading conduct only suffices to have a "likely" possibility to create a market distortion, the magnitude of which is, however, not clearly specified by law. Moreover, the extension in time of market distortion, at least regarding the prohibition of securing prices at abnormal or artificial levels, is *per se* irrelevant as interpreted by recent case law.[67] This interpretation seems somewhat to provide further legal certainty for those algorithmic trading strategies (i.e. HFT) that, because happening at the speed of light, can affect the genuine functioning of markets even for very short spans of time.

While the MAR definition entails a relatively interpretable objective element, it does not encompass any subjective element. Unlike the criminal prohibition under MAD, the administrative offence of market manipulation does not depend, at least in principle, on the specific intention of the manipulator to distort natural

---

[60] 'Trade-based' manipulation refers to manipulative conducts that take place by simply buying and selling activities on a given financial instrument. See Franklin Allen and Douglas Gale, 'Stock-Price Manipulation' (1992) 5 The Review of Financial Studies 503, 505-06.

[61] 'Order-based' manipulation refers to those strategies leveraging relatively high rates of orders' submission, modification and cancellation to deceive other market participants. See Viktoria Dalko and Michael H. Wang, 'High-Frequency Trading: Order-Based Innovation or Manipulation?' (2020) 21 Journal of Banking Regulation 289, 290-92.

[62] Sebastian Mock, 'The Concept of Market Manipulation' in Ventoruzzo and Mock (n 57) 36.

[63] MAR art 15.

[64] For a discussion on this issue, see Carsten Gerner-Beuerle, 'Article 12: Market Manipulation' in Matthias Lehmann and Christoph Kumpan (eds), *European Financial Services Law: Article-By-Article Commentary* (Nomos 2019) 748-750.

[65] For more on the issue as well as regarding the ability of a trading behaviour to be 'likely' to create a market distortion, see ibid 735-36.

[66] For a taxonomy of different regulatory approaches to the definition of the prohibition of market manipulation, see Avgouleas (n 40) 107-108.

[67] See Case C-445/09 *IMC Securities BV v Stichting Autoriteit Financiële Markten*, [2011] ECR I-05917, paras 26-27.

market conditions.[68] Altogether, the absence of any reference to subjective elements combined with a pretty vague formulation of the objective component can arguably lead to a lack of predictability and legal certainty, which could undermine both supervisors and prosecutors' ability in dealing with algorithmic forms of market manipulation. Indeed, discerning between legitimate and unlawful trading behaviours can amount to a puzzling exercise for market conduct supervisors.[69] Thus, a comprehensive assessment of the real motives behind a given algorithmic trading behaviour is usually necessary to ascertain manipulation cases and attribute liability for misconduct.[70] For instance, this can be accomplished by inferring some manipulative intent from observing trading patterns via sophisticated market surveillance systems, which however requires supervisors to be equipped with adequate technological equipment to detect suspicious activity. But this also underpins their need and ability to develop statistical methodologies to effectively recognize and clearly distinguish different manipulative strategies.

In the attempt to elucidate particularly harmful trading conducts, Article 12(2) provides a non-exhaustive list of examples of manipulation. Accordingly, algorithmic traders must be aware that specific trading strategies such as, for instance, 'abusive squeeze'[71] or 'banging the close'[72] are already well understood and clearly defined by the EU legislator as forms of manipulation. Furthermore, the EU anti-manipulation law also directly targets some forms of disruptive and manipulative behaviours made possible by trading technology, including HFT strategies such as spoofing.[73] Nevertheless, Article 12 should be read in conjunction with Annex I of MAR, which lists a number of indicators to consider in ascertaining market manipulation cases that, when being met, can raise a presumption of manipulation.[74] Also, under Article 12(5) MAR, the EU Commission used its powers to amend Annex I with a delegated act that provides a more detailed, although non-exhaustive, list of technical indicators to assist enforcement bodies in detecting and assessing suspected cases of market manipulation.[75]

Overall, while aiming at fighting against algorithmic forms of manipulation, the EU legal definition of manipulation seems not to provide adequate legal certainty. Notably, it can be doubtful whether such vagueness, which leaves ample room for legal interpretation, can safely apply to and regulate most-sophisticated forms of AI trading manipulation. Unlike manipulative strategies from more "analogic" times, algorithmic trading manipulation generally burdens enforcement authorities to succeed in prosecution. Indeed, enforcers may still need to prove with documented evidence the actual motifs behind a given suspicious trading activity, or at the very least, demonstrate a negligent use of algorithmic trading.

3.2 Liability framework and sanctions regime for algorithmic market manipulation

The EU MAR/MAD legal framework provides a 'dual-track' system of liability for market manipulation. Violations of market conduct rules can either give rise to administrative or criminal liability depending on the seriousness of offences, meaning they must be evaluated case-by-case by supervisors.

---

[68] See Gerner-Beuerle (n 64).

[69] Daniel R. Fischer and David J. Ross, 'Should the Law Prohibit Manipulation in Financial Markets?' 105 Harvard Law Review 503.

[70] Gerner-Beuerle (n 64) 736.

[71] This behaviour involves the abuse of a dominant position in such a way as to significantly distort the price at which other participants are obliged to trade in order to fulfil their contractual obligations in respect of the underlying financial instrument. See MAR art 12(2)(a).

[72] A practice that refers to buying/selling heavily a given financial instrument during the close of trading to benefit from an even larger position in a derivative contract that is cash-settled based on the price of the same financial instrument on that day. See MAR art 12(2)(b).

[73] See MAR art 12(2)(c).

[74] MAR art 12(3).

[75] See Commission Delegated Regulation 2016/522 of 17 December 2015 supplementing Regulation (EU) No 596/2014 of the European Parliament and of the Council as regards an exemption for certain third countries public bodies and central banks, the indicators of market manipulation, the disclosure thresholds, the competent authority for notifications of delays, the permission for trading during closed periods and types of notifiable managers' transactions, [2016] OJ L 88/1. To note, the EU Commission has the competence to rectify and update the list of technical indicators of market manipulation as both technological innovation and market developments may require.

- ***Administrative liability and sanctions***

Violations of the MAR prohibitions give rise to administrative liability and are enforced by each national competent authority (NCA) according to their jurisdictional competence.[76] Administrative liability can be attributable to both individuals and legal persons. In the latter case, liability can also be extended to all natural persons within an organisation who *participate* in the decision to carry out a manipulative, thus prohibited, conduct.[77] As for the case of the prohibition of insider dealing,[78] the provision applies to both legal persons, their agents, and other natural persons acting on behalf of a legal person.[79] However, if an individual (*e.g.*, an employee) acts on behalf of a legal person (*i.e.*, the investment firm) can only be assessed according to Member States' legal systems,[80] and particularly to their specific rules of agency in both an employment and criminal law contexts.[81] However, the term generally refers to any individual that enjoy powers of legal representation, the authority to take decisions on behalf of a legal person, or to exercise control within a legal person.[82] Yet, although individual responsibilities and tasks are generally well defined within private organisations such as investment firms, it can still be hard to attribute liability for misconduct by a given algorithmic trading system, especially when the latter entails most-sophisticated AI approaches.

To tackle administrative violations of market abuse, Article 30 MAR defines the 'minimum harmonised' arsenal of administrative sanctions and other legal measures at disposal of NCAs.[83] Member States are, however, left with the discretion to adopt administrative sanctions against infringements listed in Article 30(1)(a),[84] but also for failure to cooperate or to comply with an investigation, inspection, or request as provided for by Article 23(2) MAR[85],[86] where the same infringement is already subject to a criminal sanction in the same jurisdiction. In fact, if a Member State has opted for criminal sanctions for MAR infringements by 3 July 2016, it is free to decide not to apply any of the administrative sanctions.[87] As a rule, both administrative and criminal sanctions can jointly apply to the extent that the administrative proceeding does not qualify as criminal in nature. If a Member State has opted to inflict both administrative and criminal sanctions for the

[76] See MAR art 22.

[77] MAR art 12(4).

[78] For a legal definition of 'insider dealing', see MAR art 8.

[79] Gerner-Beuerle (n 64) 757.

[80] MAR art 8(5).

[81] See Carsten Gerner-Beuerle, 'Article 8: Insider Dealing' in Lehmann and Kumpan (n 64) 705.

[82] cf MAD art 8(1).

[83] Pursuant to Article 30(2) of MAR, each Member State is required to confer upon or make available to the respective NCA the power to impose a number of 'minimum harmonised' administrative sanctions and other measures against violations of market manipulation, Those include: (*a*) ordering to cease unlawful behaviours; (*b*) ordering the disgorgement of profits or avoided losses; (*c*) issuing a public warning; (*d*) the withdrawal or suspension of authorisation to provide financial services; (*e*) ordering the ban of managerial or other responsibilities within an investment firm; (*f*) imposing administrative pecuniary sanctions.

[84] Specifically, administrative sanctions must be available, *inter alia*, in the event of market manipulation (MAR art 15) but also for ineffective prevention and detection of market manipulation (MAR art 6(1)) and failures to effectively report orders and transactions that could amount to market manipulation (MAR art 16(2)).

[85] According to Article 23(2) of MAR, each NCA should enjoy "**at least**" a number of supervisory and investigatory powers, including: (*a*) accessing any document and data in any form and receiving or taking a copy of those; (*b*) requiring or demanding information from any persons and their principals by, if necessary, summoning and questioning those persons to obtain such information; (*c*) requesting information, obtaining reports on transactions, and obtaining direct access to trading systems in relation to commodity derivatives; (*d*) carrying out on-site inspections and investigations; (*e*) entering the premises of natural and legal persons to seize documents or data that may be relevant for inspection or investigation to prove an infringement of market manipulation; (*f*) referring matters for criminal investigations; (*g*) requiring existing recordings of telephone conversation and other electronic communications or data traffic records; (*h*) requiring, to the extent that is permitted under national law, existing data records from telecommunications operators for investigations where there is a reasonable suspicion of infringements; (*i*) requesting the freezing or sequestration of assets, or both; (*j*) suspending trading of the financial instrument concerned; (k) requiring the temporary cessation of any practice contrary to MAR; (*l*) imposing a temporary prohibition on the exercise of professional activity; and (*m*) taking all necessary measures to ensure that the public is correctly informed about the abusive practice.

[86] MAR art 30(1)(b).

[87] MAR art 30(1) subpara 2.

same infringement, it must do so by ensuring consistency between the two alternatives and respect the so-called criminal law principle of '*ne bis in idem*'[88],[89] as well as the 'right to a fair trial'[90].[91]

- ***Criminal liability and sanctions***

With the last reform of the EU market abuse law, the MAD introduced common minimum rules on criminal liability and respective sanctions for market manipulation. Pursuant to Article 5 MAD, EU Member States must take all necessary steps to ensure that market manipulation constitutes a criminal offence, at least in serious cases and when committed intentionally.[92] Moreover, the MAD configures as a criminal offence the inciting, aiding and abetting of market manipulation,[93] as well as attempted market manipulation.[94] It also extends criminal liability for lack of supervision or control if these omissions facilitated the occurrence of market manipulation.[95] While the MAD definition of market manipulation largely mirrors the one given by MAR, there are also some important differences given the higher procedural guarantees under Member States' criminal laws. Specifically, an alleged manipulative conduct under criminal law must entail an *actual* adverse effect on the natural market forces of demand and supply or prices to count as a crime.[96] This way, the criminal offence is subject to higher evidentiary standards and burden of proof (*i.e.*, 'beyond a reasonable doubt' standard as opposed to 'a preponderance of the evidence' one). But, as for the case of the administrative prohibition, one possible line of defence for investment firms is to show that the alleged behaviour is legitimate[97] or in conformity with 'accepted market practices'[98]. In addition, of course, traditional line of defence under criminal law are also available to defendants.[99]

According to the MAD enforcement regime, criminal penalties against market manipulation requires punishment to be "effective, proportionate, and dissuasive".[100] Hence, for the criminal offence of market manipulation, even when carried out through algorithmic trading strategies, EU Member States must ensure that any such a conduct can be punishable with imprisonment for a maximum term of four years.[101] In this last

---

[88] According to this principle, a person cannot be subject of a criminal proceeding about the same facts for which he/she was already finally convicted or acquitted. For a recent study on the legal challenges for EU courts in the application of the '*ne bis in idem*' principle in relation to financial crimes, see Marina Matić Bošković and Jelena Kostić, 'The Application of the Ne Bis In Idem Related to Financial Offenses in the Jurisprudence of the European Courts' (2020) 25 NBP Journal of Criminalistic and Law 2, 67.

[89] See *Grande Stevens et al v Italy* (App Nos 18640/10, 18647/10, 18663/10, 18668/10 and 18698/10), ECtHR, 7 July 2014, paras 221-228.

[90] See European Convention on Human Rights art 6.

[91] See Matteo Gargantini, 'Public Enforcement of Market Abuse Bans. The ECtHR Grande Stevens Decision' (2015) 1 Journal of Financial Regulation 149.

[92] MAD art 5(1). To note, however, that the provision does not define when a case of manipulation is "serious", which is only specified by MAD recital (12) stating that:

> "*[M]arket manipulation should be deemed to be serious in cases such as those where the impact on the integrity of the market, the actual or potential profit derived or loss avoided, the level of damage caused to the market, the level of alteration of the value of the financial instrument or spot commodity contract, or the amount of funds originally used is high or where the manipulation is committed by a person employed or working in the financial sector or in a supervisory or regulatory authority.*"

[93] MAD art 6(1).

[94] MAD art 6(2).

[95] MAD art 8(2).

[96] Carsten Gerner-Beuerle, 'Market Abuse Directive (MAD) - Article 6: Inciting, aiding and abetting, and attempt' in Lehmann and Kumpan (n 64) 635.

[97] See ibid, 636 ("[b]ehaviour is carried out for a legitimate reason if it pursues a goal that is in line with the principles, structures, and mechanisms underpinning the operation of capital markets and is not detrimental to transparency, stability, and market integration in the EU").

[98] Demonstrating that a conduct follows an 'accepted market practice' by a NCA is a true line of defence for investment firms. The legal framework of 'accepted market practice' is provided by MAR art 13.

[99] For a theory of criminal liability applied to AI crime addressing the application of traditional lines of defence under criminal law, see Gabriel Hallevy, *Liability for Crimes Involving Artificial Intelligence Systems* (Springer 2015).

[100] MAD art 7(1).

[101] MAD art 7(2). To note, Member States are free to establish harsher sentences provided that those respect the proportionality principle as referred to in Article 7(1) MAD. Precisely, the maximum length of a prison term or the amount

regard, the MAD addresses not only natural ('individual criminal liability') but also legal person ('corporate criminal liability'). According to Article 8(1) MAD, liability can be extended to legal persons for offences committed for their benefit by one or more of its employees, which either acted individually or as member(s) of an organ of the legal person. In other words, albeit assessing the real motives behind a given algorithmic misconduct can be a serious challenge for enforcement authorities, at least in principle, investment firms and their employees cannot escape criminal liability for malicious uses of trading algorithms.

- ***Risks of regulatory arbitrage due to the problem of 'divided interpretation'***

The primary policy rationale of the EU MAR/MAD legal framework is to establish an "equal, strong and deterrent sanctions regime"[102] for EU Member States to fight algorithmic forms of market abuse. However, given persisting differences in Member States' national laws, the prohibitions under MAR/MAD risk being implemented in a non-uniform and consistent manner within the EU (*i.e.*, problem of "divided interpretation"[103]). In addition, at least in principle, the EU legal framework allows for both public and private enforcement of market conduct rules.[104] Yet, private enforcement of financial law is not well developed in the EU, especially when compared to the US case where instead private enforcement of market abuse has historically played a more prominent role.[105] As the EU framework does not directly deal with civil liability for market manipulation,[106] our focus here is on issues of liability from an administrative and criminal law perspective.

On the one hand, existing differences in Member States' administrative law can give rise to uneven legal treatments as to meet constitutional and other restrictions for administrative authorities.[107] On the other, also the legal treatments of the "intent" requirement by EU Member States' criminal law are far from being homogeneous.[108] In the literature, it has been argued that problems specific to the interpretation of the intent requirement for market manipulation ought to be solved within the legal context of the respective sanction.[109] Accordingly, for instance, administrative liability for market manipulation under EU law does not require proving manipulators' intent explicitly, thus leaving Member States' administrative codes to solve this interpretative puzzle.[110] By contrast, for criminal liability, the same MAD text leaves the regulation of the intent requirement to Member States' criminal codes.[111] As a consequence, heterogeneous legal treatments by Member States' legal systems of the prohibition of market manipulation do not lead to a level playing field across the EU, thus exposing EU capital markets to risks of 'regulatory arbitrage', which can easily translate in ineffective enforcement against most sophisticated and cross-border instances of manipulation led by AI.

3.3 Challenges from AI trading for law enforcement

Before outlining the challenges posed by AI-driven manipulation to achieve effective law enforcement, it should be mentioned that EU financial law provides other legal safeguards to limit the occurrence of unintended consequences and unlawful practices. These include, *inter alia*, legal frameworks on 'human

---

of a pecuniary fine must reflect the profits made or losses avoided, the damage caused to other market participants, and the offence's impact on the smooth and fair functioning of markets. See Gerner-Beuerle (n 96) 640.

[102] MAD recital (38).

[103] See Sebastian Mock, 'History, Application, Interpretation, and Legal Sources of the Market Abuse Regulation' in Ventoruzzo and Mock (n 57) 9.

[104] For an account of the role of private enforcement of EU financial laws and its relation with public enforcement, see Danny Busch, 'The Private Law Effect of MiFID: the Genil Case and Beyond' (2017) 13 European Review of Contract Law 70.

[105] See John C. Coffee, 'Law and the Market: the Impact of Enforcement' (2007) 156 University of Pennsylvania Law Review 229, 245.

[106] See Mock (n 62) 44.

[107] Mock (n 103) 8.

[108] Mock (n 62) 41.

[109] ibid.

[110] The same reasoning applies to civil liability for market manipulation. ibid, 42.

[111] ibid.

control'[112] and other organisational requirements relating to the governance of algorithmic trading (*e.g.*, testing; ongoing risk management; etc.),[113] as well as electronic trading platforms (*e.g.*, direct market interventions such as 'circuit-breakers'[114]). However, as our focus is on the limitations of the EU enforcement approach to market conduct rules, these other safeguards are not addressed here in a specific manner.

Despite the EU primary objective to establish a level playing field among Member states' law enforcers, there are several reasons to believe that whenever facing the technical specificities and additional risks posed by AI trading, the EU anti-manipulation law and its enforcement regime display a number of weak points to achieve credible deterrence. Whereas AI trading can enjoy market ubiquity, with cross-market and cross-border scope of action, Member States' interpretation and enforcement of liability rules for manipulation are not homogeneous. If compounded with a similarly de-centralised interpretation and implementation of MiFID II rules on the governance of algorithmic trading and electronic trading platforms,[115] all this raises serious doubts about the effectiveness of the EU approach to protect EU capital markets' integrity. The following provides a non-exhaustive list of causes for enforcement failures that can lead to sub-optimal, thus not credible deterrence of AI-driven manipulation.

First, AI trading can take advantage of uncertain legal prohibitions by optimising both old and new manipulation strategies that may fall outside the scope of EU anti-manipulation law. Different implementations of the prohibition of market manipulation among Member States' legal systems and the exclusion of certain financial instruments from the scope of MAR can both become a fertile ground for AI trading manipulation to occur. **Second**, as not all Member States adopted criminal law measures for serious manipulation cases, this can lead to different enforcement outcomes across the EU.[116] The uncertain equivalence of administrative and criminal sanctions can expose EU capital markets to enforcement discrepancies to the extent that criminal sanctions substitute administrative ones since criminal law enforcers lack some instruments that MAR defines as minimum administrative powers. In addition, the uncertain relationship between administrative and criminal law measures can hamper effective enforcement, especially against cross-border cases.[117] As another cause of enforcement asymmetry, not all Member States provide for 'corporate criminal liability' (*e.g.*, Germany), something that represents a fundamental tool to achieve effective enforcement as it can incentivise investment firms towards co-operating with enforcement bodies. **Third**, the existing EU supervisory architecture can lead to oversight failures as being inadequate to deal with the cross-market and cross-border nature of certain AI trading strategies. As private organisations operating within competitive markets, 'gatekeepers' (*i.e.*, trading venues), which are responsible for some delegated supervisory tasks, do not always face the right incentives to carry out effective oversight. In addition, their supervisory competence is only limited to their platforms ('single market' supervision). In fact, 'cross-market' supervision of EU markets has not been effectively implemented, something that could be in principle assigned to NCAs.[118] In this last regard, whereas the format of order book data to submit to NCAs is harmonised, there is no common standards relating to the scope of their communication between trading venues and NCAs.[119] Not only can this limit NCAs' ability to grasp a holistic picture about the supervisory landscape, but it can also undermine NCAs' easiness of coordinating and sharing information on time. More generally, NCAs suffer from a lack of technological expertise and tools to equate those of malicious market actors. **Fourth**, even assuming the ability of market supervisors to detect AI manipulation effectively, there persist fundamental legal problems as to attributing liability for AI misconduct. As seen, the self-learning and 'black-box' nature of specific ML methods call into question the suitability of

---

[112] See Joseph Lee and Lukas Schu, 'Regulating of Algorithmic Trading: Framework for Human Supervision and Direct Market Interventions (2021) European Business Law Review (forthcoming) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3765882> accessed 16 January 2022.

[113] See Raschner (n 10); Gerner-Beuerle (n 10).

[114] See Gerner-Beuerle (n 10); Lee and Schu (112)

[115] See Johannes Karremand and Magnus G. Schoeller, 'MiFID II between European rule-making and national market surveillance: the case of high-frequency trading' in Adrienne Héritier and Magnus G. Schoeller (eds) *Governing Finance in Europe: A Centralisation of Rulemaking?* (Edward Elgar Publishing 2020).

[116] See Andrea Perrone, 'EU Market Abuse Regulation: The Puzzle of Enforcement' (2020) European Business Organization Law Review 379.

[117] See Michiel Luchtman and John Vervaele, 'Enforcing the Market Abuse Regime: Towards an Integrated Model of Criminal and Administrative Law Enforcement in the European Union?' (2014) 5(2) New Journal of European Criminal Law 192.

[118] See ESMA, *MAR Review Report* (23 September 2020) ESMA70-156-2391, 128-134.

[119] ibid.

the current regulatory framework on testing and human oversight of algorithmic trading. For instance, the fact that both investment firms[120] and trading venues[121] were allowed to show, until now, their law compliance through an annual self-assessment would not seem entirely appropriate to ensure the safe and law compliant implementation of AI trading. As the frameworks of this self-assessment exercise are still not entirely harmonised at the EU level, divergences may also arise among different NCAs in checking for compliance.[122]

All the above raises several questions about the ability of the EU enforcement regime to credibly deter and effectively punish AI-driven manipulation. As the main takeaway, AI trading seems left operating in a (quasi-)lawless market environment to exploit regulatory arbitrage opportunities offered by the current EU anti-manipulation law and its enforcement, thus leading to 'forum-shopping' possibilities for AI traders.

4. The law & economics of deterring AI manipulation

Most sophisticated and profitable market manipulation cases usually occur as a 'white collar' crime. Through gimmicks, swindles and other deceiving strategies, malicious actors aim at extracting profits that would not otherwise be available to them. Traditionally, market manipulation has always been one of the most 'intractable' financial wrongs for enforcement authorities, given all the difficulties inherent in detecting, investigating, and prosecuting such cases.[123] As we have seen, these difficulties increase in algorithmic market manipulation and further compound in the presence of AI agency. Nevertheless, one of the primary goals of any enforcement regime against market manipulation is to put in place legal prohibitions, liability rules, and enforcement mechanisms able to credibly deter would-be manipulators.[124] With these goals in mind, this study proposes to analyse the enforcement puzzle of deterring AI-driven manipulation under the lens of 'deterrence theory', with the aim to provide normative interpretations and unlock valuable insights to think of new ideas to improve the effectiveness of the EU anti-manipulation law and its enforcement.

Within the law and economics scholarship, 'deterrence theory' is a branch of economic analysis of tort law and criminal law interested in analysing the interplay between different sanctions regimes and people behaviour in abiding by the law. In strictly utilitarian terms, deterrence theory generally posits that an individual will break the law if his/her expected utility, measured as the difference between total expected gains and costs from misconduct, is greater than not committing it.[125] In a financial trading context, deterrence theory would suggest that a rational human trader would not intentionally enter into unlawful conduct (such as manipulation) unless his or her expected benefits outweigh expected costs. To put it simply, whenever a human trader presumes to face greater risks of penalties than economic rewards, he/she can be deterred from engaging in manipulation. According to this school of thought, the law can deter would-be manipulators by altering the balance in their expected utility from manipulating markets. Therefore, by making market manipulation a costly and risky activity, the law can make such an offence less desirable to accomplish from an *ex-ante* perspective. That makes deterrence credible and law enforcement effective.

Under deterrence theory, two are the primary policy levers that the law can leverage to alter manipulators' utility functions. Namely, (*a*) the '*certainty of punishment*' (*e.g.*, the probability of being caught, investigated, prosecuted, and punished) and (*b*) the '*severity of punishment*'.[126] On the one hand, higher levels of deterrence can be achieved by increasing wrongdoers' perception about the certainty of being punished. To this end, there

[120] See 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 [2017] OJ L 87/417, art 9.

[121] See Commission Delegated Regulation (EU) 2017/584 of 14 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying organisational requirements of trading venues [2017] OJ L 87/350, art 2(1).

[122] cf ESMA, *MiFID II Review Report on Algorithmic Trading* (28 September 2021), ESMA70-156-4572, 47-50 (for investment firms) and 54-55 (for trading venues).

[123] Merritt B. Fox, Lawrence R. Glosten and Gabriel Rauterberg, 'Stock Market Manipulation and Its Regulation' (2018) 35 Yale Journal of Regulation 67.

[124] See Gina-Gail Fletcher, 'Deterring Algorithmic Manipulation' (2021) 74(2) Vanderbilt Law Review 101. To note, this sub-section extensively builds on this study.

[125] ibid. 268.

[126] See Raymond Paternoster, 'The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues' (1987) 4(2) Justice Quarterly 173.

are several alternatives for lawmakers. As a first condition, legal systems need to provide for clearly defined legal prohibitions,[127] which is a prerequisite to allowing would-be criminals to be aware of the precise boundaries between legitimate and unlawful behaviours. Legal un-certainty can in fact have the effect of impairing deterrence, thus allowing more offences to occur. In addition, credible deterrence is also strictly linked to enforcers' resources, tools and expertise, and not least the authority to address misconduct;[128] that is the ability of enforcement authorities to detect, investigate, and prosecute offenders. On the other hand, would-be criminals can more effectively be deterred through harsh punishments.[129] Indeed, the magnitude of sanctions that offenders risk facing, such as the length of sentences, monetary fines, or other measures (*e.g.*, a professional ban), have a relatively important deterrent effect.[130] Therefore, under this second lever, the law should set levels of punishment high enough to discourage misconduct.

Under simplistic assumptions about individuals' behaviours, as well as public authorities' ability to successfully prosecute and punish, classical models of deterrence would suggest leveraging the 'severity of punishment' to optimally deter would-be offenders by making their crime opportunity unprofitable from an *ex-ante* perspective.[131] According to this view, the law should aim at deterring financial crimes, such as market manipulation, by setting high enough fines (or other punishments). Yet, classical models often fail to adequately represent reality by dismissing specific behavioural aspects that influence individuals' motivations to commit crimes. Because of this limitation, more modern approaches should be preferred as being instead enriched by fundamental insights from behavioural economics' studies. In effect, behavioural considerations can help us shed some light on the interplay between certain subjective elements of crime and credible deterrence. For instance, it seems that would-be manipulators are more sensitive to an increase in the probability of being punished than to an increase in the magnitude of punishments. This effect is due, *inter alia*, to people's 'risk aversion' and 'time sensitivity to losses'.[132] Overall, recurring to deterrence theory, as a normative framework, can be a useful tool for designing effective liability rules and sanctions to shape individual preference towards crimes.[133] However rudimentary this conceptual framework seems to be, it can still offer a useful scientific mindset and conceptual toolkit towards approaching novel economic and legal problems, such as dealing with AI agency and market manipulation.

4.1 Algorithmic market manipulation as corporate crime

Although AI methods are increasingly accessible to the public, it is safe to believe that only well-resourced and professional traders can employ the most-advanced AI-driven trading strategies. Under this assumption, most-sophisticated forms of AI-driven market manipulation can be understood as particular cases of corporate financial crime. Corporate crimes usually involve one or more employees within an organisation that, within the scope of their employment, can be motivated to commit an offence by some intent to benefit that organisation. There are several causes for such pathological corporate behaviours to occur. For instance, market manipulation can be the by-product of firms' internal culture, given unethical senior management or other agency problems likely to emerge within any organisation.[134] Hence, unlike individual crime, the law needs other strategies to constrain people behaviours when they are part of an organisation (or 'corporate behaviour'). In principle, any firm can either induce crimes through compensation schemes, providing incentives for its employees to commit unlawful acts or conversely inhibit potential wrongdoers because of

---

[127] Fletcher (n 124) 269.

[128] Ana Carvajal and Jennifer Elliott, *The Challenges of Enforcement in Securities Markets: Mission Impossible?* IMF Working Paper (August 2009) WP/09/168, 4-5 <www.elibrary.imf.org/downloadpdf/journals/001/2009/168/001.2009.issue-168-en.xml> accessed 16 January 2022.

[129] IOSCO, *Credible Deterrence in the Enforcement of Securities Regulation* (2015) 35-40 <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD490.pdf> accessed 16 January 2022.

[130] See A. Mitchell Polinksy and Steven Shavell, 'The Optimal Use of Fines and Imprisonment' (1984) 24 Journal of Public Economics 89.

[131] See Gary S. Becker, 'Crime and Punishment: An Economic Approach' (1968) 76 Journal of Political Economy 169 (advancing an economic model for the analysis of criminal punishment in order to develop optimal public and private policies to fight illegal activities).

[132] Fletcher (n 124) 270-71.

[133] Becker (n 131).

[134] See Jennifer Arlen and William J. Carney, 'Vicarious Liability for Fraud on Securities Markets: Theory and Evidence' (1992) University of Illinois Law Review 691.

their potential ability to assist public authorities in enforcement. That is why some neoclassical theories emphasise the role of 'corporate criminal liability' to achieve greater deterrence by incentivising firms to cooperate with enforcement authorities. This view moves from the assumption that public authorities alone cannot prosecute all crimes by just setting fines high enough to daunt criminals, whereas law enforcement always entails some social costs.[135]

In deterrence terms, corporate criminal liability should be seen as a complementary tool for individual liability,[136] rather than a mere substitute.[137] Notably, also governments around the globe recognise the essential role that corporate criminal liability plays in combating complex economic crimes,[138] such as market manipulation. Corporate criminal liability aims to ensure that the same organisations, which benefit from crimes put in place by their employees, can be held responsible by making legal persons (corporations) possible law enforcement targets. This way, corporate criminal liability allows to subject corporations to investigations, judicial or administrative proceedings and ultimately sanctions whenever found responsible for economic crimes. The contribution of corporate criminal liability to law enforcement processes and outcomes is twofold. First, it allows public authorities to hold legal persons liable for certain wrongdoings either additionally or independently from any natural person involved in the offence. Second, the specific design of corporate criminal liability rules can create efficient incentives for private organisations to adopt virtuous and collaborative behaviours, which can support public authorities' tasks by reducing society's efforts in the detection, prevention, investigation and resolution of crimes.[139] We should, however, keep in mind that the goal of an efficient and credible deterrence regime should be also one of minimising the sum of all the costs associated with crime. Total costs include both the cost of harm to victims and the market and those that the same law enforcement entails (*i.e.* both direct costs faced by enforcement authorities and over-deterrence costs that society may face from inaccurate prosecution and other legal errors).[140]

Designing an effective enforcement regime to deter market manipulation needs to be a top priority in regulators' policy agenda.[141] Since ineffective enforcement exposes markets to market abuse such as manipulation, it can thus impose a substantially high deadweight loss on society. That is why legal systems need to provide their regulators with the necessary legal tools and resources to counterbalance the competitive advantage of the industry on technology.[142] Notwithstanding all the difficulties in implementing an effective enforcement regime against market manipulation, there is an international agreement among financial regulators on the importance of credible deterrence as a pillar of effective law enforcement of securities law.[143] In short, deterrence is credible if it can modify behaviours and reduce violations from an *ex-ante* perspective. In turn, law enforcement is effective if it guarantees detection, prosecution, and sanctioning of misconduct.

4.2 The feasibility to credibly deter and punish AI trading

AI trading potential for crime poses new and important questions on ensuring deterrence, structuring liability rules and relative sanctions. Whenever financial decision-making is delegated to increasingly autonomous, market ubiquitous, and often black-box AI trading systems, traditional crime scenarios of market manipulation

---

[135] See Jennifer Arlen, 'Corporate criminal liability: theory and evidence' in Alon Harel and Keith N. Hylton (eds) *Research Handbook on the Economics of Criminal Law* (Edward Elgar Publishing 2012) 144, 162-167.

[136] See ibid, 167-172.

[137] For a critical account on the scope of corporate criminal liability, see Vikramaditya S. Khanna, 'Corporate criminal liability: What purpose does it serve' (1995) Harvard Law Review 1477.

[138] See OECD, *The Liability of Legal Persons for Foreign Bribery: A Stocktaking Report* (2016) <https://www.oecd.org/daf/anti-bribery/Liability-Legal-Persons-Foreign-Bribery-Stocktaking.pdf> accessed 16 January 2022.

[139] ibid.

[140] See Amanda Rose, 'The Multienforcer Approach to Securities Fraud Deterrence: A Critical Analysis' (2010) 158 University of Pennsylvania Law Review 2173, 2183-2193 (discussing the main factor determining the magnitude of overdeterrence costs).

[141] Frank H. Easterbrook and Daniel R. Fischel, 'Mandatory Disclosure and the Protection of Investors' (1984) 70 Virginia Law Review 674 (arguing that legal rules against market abuse are more efficient than solely relying on market-based solutions).

[142] See, e.g., Ana Carvajal and Jennifer Elliott, *The Challenges of Enforcement in Securities Markets: Mission Impossible?* IMF Working Paper (August 2009) WP/09/168.

[143] See, e.g., IOSCO, *Credible Deterrence in the Enforcement of Securities Regulation* (2015) (highlighting the seven main factors to achieve credible deterrence).

become altered. To be precise, AI agency adds another layer of complexity for market abuse law enforcement and, specifically, for the safe application of traditional legal concepts of liability underpinning existing anti-manipulation law. As seen, AI trading can result in unintended consequences or be used intentionally by malicious actors to manipulate markets. Even more problematic, thanks to increasingly powerful ML methods, AI trading can autonomously engage by self-learning in manipulative conduct and harm markets.

As discussed above, enforcement is effective if its deterrent effect can convince market actors that it is better not to attempt manipulation by threatening them with sanctions or other punishments. Therefore, deterrence is credible if market participants are convinced that better not to use AI trading for unlawful purposes. Ideally, deterrence is credible when it can also induce investment firms to take all necessary precautions to avoid misconduct and support enforcement action when something wrong occurs. In addition, an effective enforcement regime reduces the risks of crime to optimal levels and, at the same time, minimise the societal costs of enforcement. In sum, efficiently structured liability rules can help ensure firms and their employees behave according to the law and take precautionary measures to avoid or, at least, limit AI forms of crime and harm. However, AI agency alters the fundamental problem inherent in deterring market manipulation in significant ways. Unlike humans, AI systems are somewhat unusual *animal* for the law to regulate. Most advanced AI algorithmic trading systems are complex 'human-machine' hybrid systems. Shaping AI behaviour entails a different problem than dealing with humans or organisations.[144] As a complex ecosystem of algorithms that can lead to 'black box' issues, AI shows a fundamentally different behaviour than humans.[145] For all these reasons, the law may lack the right tools to shape AI behaviour. Because of this 'knowledge gap', legal systems and regulators are exposed to significant risks of under-deterrence. In contrast, AI trading is left operating in a (quasi-)lawless environment, discovering manipulation with a high chance of getting off scot-free. As a result, some market players could more or less consciously externalise the costs of their manipulative conduct to society.

However tricky the additional uncertainties posed by AI are, deterrence theory can still provide a theoretical tool to think of innovative legal solutions to deal with the specificities of AI-driven market manipulation. Punishing and deterring AI itself could be a possibility to explore. In theory, deterring AI could be done via programming codes. As AI is proposed to solve optimisation problems subject to some constraints, one could think to directly programme the utility function of crime within the AI system to deter it from engaging in misconduct *ex-ante*. But this underpins the necessity of legal systems to provide a more objective and quantifiable definition of market manipulation. If this was not a practicable alternative, one could alternatively envisage punishing AI *ex-post*. Still, also this option would require some fundamental changes to the law, as AI agents do not enjoy legal personhood to be subject to prosecution and sanctions. Nevertheless, from a policy perspective, at least at this stage of AI technology, holding firms and individuals responsible for AI crime and related harm seems the most desirable and viable solution.

- ***Deterring AI 'ex-ante'***

Being able to directly deter AI behaviour by leveraging the same AI technical features is conceptually fascinating. As the core of AI is solving problems of a mathematical optimisation nature, there could be room to directly integrate a 'deterrence formula' as a code within AI inner functioning. The idea of constraining AI trading via directly programming market conduct rules in their models to teach how not to (learn to) misbehave is surely appealing. However, its feasibility needs to be verified as several technical and legal issues must be overcome. Let us, for a moment, suppose there was no technical or legal barrier to implementing such a solution via programming. It would still be hard to let autonomous and self-learning AI adapt to changing regulations and market dynamics to achieve deterrence in a dynamically credible way. Perhaps, thanks to continuous progress in dynamic programming and reinforcement learning, this is something that computer scientists could achieve. As a prerequisite, the move towards more 'machine readable' regulation to feed into AI models for subsequent learning and adaptation seems relevant. To this end, legal definitions of manipulation need to be re-written in more objective and quantifiable terms to be intelligible by AI. Unfortunately, current legal prohibitions of market manipulation seem too far from it. As characterised by a high degree of vagueness, they indeed leave ample room for legal interpretation and, as such, are not conducive for AI to calculate its utility from committing misconduct.

---

[144] See Iyad Rahwan et al, 'Machine Behaviour' (2019) 568 Nature 477.
[145] ibid, 483.

- ***Punishing AI 'ex-post'***

If we cannot deter AI *ex-ante*, can we still punish it *ex-post*? Questions relating to punishing AI agents for their crimes and related harm have also attracted intense scholarly attention.[146] For many commentators, the main obstacle to punishing AI agents relies in existing legal systems' impossibility to grant legal personhood to AI. As AI cannot enjoy legal personality, this argument acknowledges current legal systems' inability to enforce the law against AI itself.[147] However, let us suppose, only for a moment, that AI systems can be granted legal personality. In that case, general legal concepts of criminal and civil law can still hardly find safe application. For instance, one of the general criminal law requisites for crime, the criminal mind status (*i.e.*, the so-called *mens rea*) cannot be assessed easily in AI crimes,[148] such as serious manipulation cases. In addition, also other established legal concepts such as 'causation', which is applied in both criminal and civil law contexts, struggle to solve liability attribution issues for AI misconduct.[149]

Even after putting all these legal considerations aside, we would still face critical legal issues in designing a suitable punishment regime targeting AI systems or agents. Imagine, as a prosecutor, dealing with a criminal AI system. Punishment alternatives that usually address individuals, such as a prison term or a ban from professional activity, do not provide for analogous application in cases involving AI. Albeit surely fascinating, the idea of punishing AI systems or agents by a temporary ban of professional activity or even a prison sentence is not conceptually workable. As AI cannot be banned or jailed, analogous alternatives may entail switching off or suspending a specific AI model, software, or system from operations. Again, there are also quite a few problems with these policy options. Asking an investment firm to 'switch off' or temporarily suspend the use of its AI trading system does not seem to be a credible, let alone reasonable, alternative. One has only to think of the many technical possibilities to circumvent such a punishment: e.g. by simply modifying some AI components to pretend that a given AI system is now another one that complies with market conduct rules. Alternatively, one could think of ways to directly punish AI with monetary fines. Again, as long as AI cannot enjoy legal personality and thus hold assets, this is hardly a workable option.

Overall, AI punishment is hard to conceive within existing legal systems, as they do not allow granting AI legal personhood. Therefore, the law must continue targeting individuals and corporations designing, developing use, and benefiting from AI. While certainly representing a fascinating venue for future research, deterring AI (*e.g.*, via programming) seems not a workable solution. The main obstacles seem to rely on too vague legal definitions of manipulation. Hence, given the impossibility of deterring ex-ante and punishing AI *ex-post* directly, holding firms and individuals responsible for AI crime and harm is the only viable alternative from a policy perspective.

5. Filling the gaps in the EU anti-manipulation law enforcement regime to safeguard credible deterrence

As markets are increasingly digital and traders artificial, we need to rethink the assumptions and rules of existing financial law regulation as current legal systems fail to address some of the AI trading technical specificities and related additional risks. Precisely, the rise of AI algorithmic trading and its disruptive potential for market integrity calls into question the EU financial law ability to credibly deter AI-driven market manipulation. As AI trading is left operating in a (quasi-)lawless market environment, it can lead to rigged markets, thus also threatening the stability of the whole financial system given the high interconnectedness of markets and the speed at which contagion can take place in a global economy. All this urges EU regulators to carefully monitor developments in AI, start thinking of innovative solutions to enhance the governance of algorithmic trading, and improve the regulation over the prohibition of market manipulation. With all these risks in mind, this last section puts forward a number of policy proposals *de lege feranda*, as possible solutions to the deterrence puzzle of AI financial misconduct and crime under the current EU MAR/MAD enforcement regime for market manipulation.

---

[146] See, e.g., Ryan Abbott and Alex Sarch, 'Punishing Artificial Intelligence: Legal Fiction or Science Fiction' (2019) 53 University of California Davis Law Review 323.

[147] See Simon Chesterman, 'Artificial Intelligence and the Limits of Legal Personality' (2020) 69 International & Comparative Law Quarterly 819.

[148] See discussion in Abbott and Sarch (n 146), 349-360.

[149] Azzutti, Ringe, and Stiehl (n 7) 120-121.

5.1 An improved, 'harm-centric' definition of manipulation

For a long time now, existing definitions of market manipulation have attracted extensive criticism for their inability to ensure legal certainty as their safe application is encapsulated in the proof of the intent or other relevant mental state (*e.g.*, negligence) of wrongdoers.[150] Challenges to the enforcement of market conduct rules have always been present, even in times of human trading. Whereas proving intent is only expressively required by the MAD prohibitions, it may also be necessary as a discriminatory criterion in ascertaining administrative liability for algorithmic market manipulation. Now that algorithmic trading already counts for the vast majority of all market activity and therefore has overshadowed human traders' traditional role, the whole problem has taken on worrying proportions. Relying on existing liability tests can lead AI-driven trading to operate within a (quasi-)lawless market environment. Specifically, whenever AI trading results in misconduct and harm, it can circumvent the prohibitions set out in the EU MAR/MAD legal framework. For this reason, we urge EU regulators to reconsider existing anti-manipulation law to achieve credible deterrence.

Following some recent proposals from US scholars,[151] a starting point can be moving towards more precise and harm-centric definitions of market manipulation. An improved, 'harm-based' definition of manipulation would provide market actors and operators with more objective and quantifiable elements to discern unlawful from legitimate trading activity, thus allowing them to know the exact boundaries of prohibited trading conducts. In addition, once a harm-based definition is in place, enforcement authorities could rely on a more reliable legal framework and tests to detect, investigate and prosecute manipulation. At the same time, victims could find it easier to seek compensation for incurred losses as manipulation is easier to spot and measure. Moving to a harm-based definition of manipulation can have several advantages, but it also entails very delicate policy decisions by regulators. Most importantly, a specific framework would be needed to define manipulation from a harm-centric perspective. Some existing proposals generally seek to disentangle the economics of manipulation from any subjective element. For instance, a solution could be defining 'trade-based' market manipulation as any trading activity that puts an unjustified pressure on market prices because unsupported by sufficient information.[152] But this presupposes that regulators are able to provide compelling evidence that suspected parties did not possess sufficient information justifying a specific trading behaviour.[153] Specifically, it would be crucial for market supervisors to effectively identify and measure harm and attribute liability according to the exact contribution of any alleged wrongdoers. A 'harm-based' definition of manipulation can also have the effect of signalling to market participants what regulators and supervisors accept as lawful market conducts, thus exploiting the law's expressive role.[154] Reforming the definition of market manipulation with an improved version that focuses on the harm to markets, rather than relying on the real motives behind specific conducts, can serve the law enforcement objective to achieve credible deterrence of AI trading manipulation. With more objective and quantifiable definitions of manipulation, for instance, AI trading could be programmed in such a way to take into consideration the legal but numerical boundaries of an improved definition of manipulation while pursuing optimisation tasks given specific trading goals. With an improved and 'harm-based' definition of manipulation, it is envisaged that enforcement authorities could enjoy a more specific and safe legal framework for law enforcement.

Overall, essential questions remain on how regulators should reform the definition of manipulation in more objective and quantifiable terms to better deal with AI. While 'indicators' of manipulation, as defined by the EU Commission Delegated Regulation 2016/522, might be seen somewhat as the first step in this direction, more work needs certainly to be done.[155] Indeed, law and regulation should be based on the best available

---

[150] See Daniel R. Fischel and David J. Ross, 'Should the Law Prohibit 'Manipulation' in Financial Markets?' (1991) 105 Harvard Law Review 503.

[151] See Fletcher (n 124) 318-321.

[152] See Matthijs Nelemans, 'Redefining Trade-Based Market Manipulation' (2008) 42 Valparaiso University of Law Review 1169.

[153] ibid, 1183-1190 (explaining in more detail the relationship between trading, price pressure and price change, as well as how regulators could produce evidence about a given trading activity's exercising of unsupported price pressure).

[154] cf Nelemans (n 152) 1176.

[155] Whereas these 'indicators' of manipulation are not defined into numeric or statistical values, they are still valuable in providing examples of suspicious signs of different manipulative strategies.

knowledge about modern capital markets and their functioning.[156] To this end, financial regulators need all the necessary expertise, motivation and public support to understand complex network systems (such as global algorithmic capital markets) in a holistic but pragmatic fashion. But all this underpins the urgency to establish greater collaboration between the scientific fields of financial law, economics, and informatics.[157]

5.2 An improved, 'multi-layered' liability framework for AI trading misconduct and crime

Complementary to a 'harm-based' definition of manipulation, the merits of structuring new liability rules better tailored to the specifics of AI-driven manipulation should be explored. As seen, existing liability rules are not optimal to achieve credible deterrence of AI trading manipulation. AI agency adds, in fact, another layer of complexity, which translates into a 'knowledge gap' for enforcement authorities, thus leading to accountability gaps for AI misconduct and harm. In addition, while existing liability rules can have the effect of shaping human behaviour towards socially acceptable conduct, they fail to effectively deal with the specific features of AI misbehaviour. Therefore, the following proposes an improved 'multi-layered' liability framework for AI misconduct, providing for administrative and criminal liability, however differentiating liability rules and sanctions according to the different degrees of harm and human involvement. The proposed multi-layered liability framework, disentangling administrative and criminal liability aspects relating to AI misconduct, ought to achieve two complementary objectives. On the one hand, it should make sure that investment firms (and trading venues) conduct due diligence on the use of their AI trading systems and invest in precautionary measures. On the other, it must ensure that private organisations work closely with public authorities to avoid crime in the first place, and, whenever misconduct occurs, the improved framework should provide great incentives for collaborating in enforcement action.

- ***Criminal liability for AI manipulation***

Criminal liability must continue to apply for serious violations, either when committed under traditional manipulative schemes or by AI algorithmic trading strategies. However, as we cannot hold AI agents criminally liable, the question remains: whom to blame and hold responsible for AI misconduct and related harm?

Some authors argue that, in the fight against algorithmic trading manipulation, individual criminal liability is an adequate tool to regulate and forestall manipulation.[158] According to this view, there are two main reasons to adopt individual criminal liability and prefer it to corporate criminal liability. First, holding individual human experts, such as traders and those in charge of some control and risk management function, directly responsible for algorithmic trading misconduct would have a greater deterrence effect than relying on corporate criminal liability.[159] Second, because in a criminal proceeding, the burden of proof is higher than in administrative or civil trials, convicting an individual usually requires a high burden of proof. Hence, higher procedural standards would guarantee that prosecutors only target and punish extremely grave offences.[160] This argument, however, cannot fully convince as, for specific AI behaviours, ascertaining and attributing liability to the responsible individuals can be a very burdensome activity or just not feasible. Because AI systems are 'hybrid' human-machine systems that entail substantial complexity, AI trading behaviour is intricate to observe, regulate, and shape. Thus, a better and safer option is to attribute the implications of AI trading misconduct and its effect on markets directly to the investment firms using and benefitting from these systems. The law should therefore recognise AI trading conduct as a corporate action.[161] Just as employees' acts or omissions can be attributable to corporates, so should AI trading behaviour. However, even when

[156] David C. Donald, 'Regulating Market Manipulation through an Understanding of Price Creation (2011) 6 NTU Law Review 55, 82.

[157] Azzutti, Ringe, and Stiehl (n 7) 122.

[158] Orlando Cosme, 'Regulating High-Frequency Trading: The Case for Individual Criminal Liability' (2019) 109 Journal of Criminal Law and Criminology 365.

[159] ibid, 387-88.

[160] ibid, 383-85.

[161] See Mihailis Diamantis, 'Algorithms Acting Badly: A Solution From Corporate Law' (2021) 89 The George Washington Law Review 801.

imputing AI misconduct as a corporate action, a clear line must be drawn to determine which conducts give rise to criminal liability.

If, as amply discussed above, 'intent' as a legal standard does not fit well for attributing liability for AI-driven manipulation, other 'fault-based' liability standards such as 'recklessness' could better serve this purpose.[162] As a liability rule, a recklessness standard implies that liability arises when an individual has deliberately and unjustifiably pursued a course of action while consciously disregarding any risks flowing from such action. In establishing liability for AI manipulation, a recklessness standard can be used to assess the *means rea* element of a corporation, through its employees in some leading position, in charge of fundamental oversight and compliance functions, or as developers and users of a manipulating AI trading system. To appreciate the merits of a 'recklessness' standard, let us assume that market conduct supervisors have detected a suspicious case of manipulation put in place by sophisticated AI trading strategies of a given investment firm. To avoid liability, such a firm would need to explain the actual AI system behaviour that led to the alleged trading conduct resulting in a manipulative-like outcome. Therefore, a 'recklessness' standard could allow shifting the burden of proof from enforcement authorities to alleged malicious actors, thus providing the latter incentives to develop a legally-acceptable internal culture that promotes market quality and integrity.[163] However, three basic scenarios can be envisaged here.

In the **first** but perhaps unrealistic scenario, let us assume that the investment firm takes a collaborative approach. Herein, the firm can explain why its AI system behaved in a particular manipulative manner and that some of its employees knew about that possibility or just were negligent. This way, the threat of 'corporate criminal liability' is instrumental in leading the firm to assist public authorities in enforcement. As a next step, the question for the firm would then be how to ascertain liability among its employees according to their exact contribution to the AI production line. Under the **second** scenario, instead, the investment firm takes a less collaborative stance. It firmly believes that all the necessary precautionary measures were in place and that it can oversight and control AI trading in a compliant manner. The firm also believes its AI trading did not result in unlawful behaviour and that harm was somewhat due to complex interrelations happening on markets among competing algorithms. Under this scenario, public authorities would need to prove that the firm did not take the adequate 'duty of care' prior to and while using AI on markets, thus resulting in a reckless implementation of AI trading or some other negligent-like conduct. Herein, however, enforcers would need a well-defined measuring system to appreciate in relative terms the extent to which the alleged conduct was reckless. But again, the burden of proof could be shifted to investment firms. Finally, in the **third** scenario, the firm is not in the position to explain why and how its AI trading system has behaved in the alleged market misconduct. In this case, enforcement authorities would have no doubts about the firm's reckless use of its trading algorithms. And 'corporate criminal liability' will automatically apply. Undoubtedly, the most challenging case for effective enforcement is the second scenario. Here, we have a firm that pretends to understand and explain its (manipulative) AI system's behaviour, while at the same time it believes that the respective trading strategy conforms to EU market conduct rules. Under this scenario, for enforcement authorities, proving 'intent' could result in a *probatio diabolica*, resulting in a lengthy investigation that may ultimately fail to ascertain liability, thus leaving victims uncompensated and markets integrity exposed to AI trading manipulation.

In a nutshell, the above scenario analysis illustrates how '**recklessness**', as opposed to 'intent', can better serve the purpose of protecting market integrity from those market actors externalising the costs of their AI trading practices to others. Adopting a recklessness standard, which nevertheless is already applied to other forms of market abuse (*i.e.*, insider trading, information-based manipulation), could arguably allow to better preserving investor protection and confidence *vis-à-vis* AI-driven market manipulation.

- ***Administrative liability for AI manipulation***

Criminal liability helps ensure that investment firms and their employees can be more credibly deterred from attempting to manipulate markets through their AI systems. In contrast, a strong, smooth and efficient administrative sanctions regime would guarantee that investment firms take all the necessary steps to operate within the boundaries of permitted conduct.

---

[162] See Fletcher (n 124) 320-21. To note, the same MAD does not exclude this possibility. cf MAD recital (21).
[163] Fletcher (n 124) 321.

As seen, AI systems are complex ecosystems of algorithms, constituted by different software and hardware parts, which usually require several human experts internal to an organisation, plus some components and expertise acquired from third parties. Because of this, whenever something can go wrong, it may be impossible to assess the exact contribution in liability among a long list of individuals. While administrative sanctions can target both companies and individuals, this paper argues in favour of the establishment of a 'single point of access' to regulatory litigation. Under this lens, AI personhood or other solutions,[164] such as a 'risk management approach'[165] to liability, can be seen as innovative policy tools to promote credible deterrence and effective enforcement. In addition, the proposed framework envisages a 'strict' liability rule for violations of the administrative prohibition of manipulation.[166] With a single access point for enforcement authorities and plaintiffs alike, an administrative sanction regime would be more effective in sanctioning wrongdoers and eventually supporting private litigation for compensating victims. With a 'single access point' subject to '**strict**' liability rule, investment firms may explore the desirability to hedge their increased exposure to sanctions risks via newly established insurance regimes for AI trading.[167] However, this alternative presumes that an insurance market for AI systems can be developed, which underlies private insurance companies' ability and business interest to statistically calculate risks of manipulation arising from using AI and price premiums accordingly. Alternatively, one can envisage the establishment of a 'compensation fund' for harm caused by AI trading manipulation. This option requires careful considerations on how such a fund should be financed and how and under which circumstances to grant access to victims seeking compensation.[168] Under both alternatives, investment firms could know better the risks and limits of their potential liability for AI-driven manipulation from an *ex-ante* perspective. Victims' compensation would be safeguarded from an *ex-post* viewpoint by holding the respective investment firm responsible for paying damages. However, firms could hedge their liability risks via insurance premiums or participate via contributions to a compensation fund. Either way, the proposed framework shows several benefits, as investment firms are the best party placed to minimise costs and risks arising from AI and eventually acquire AI insurance coverage. Nevertheless, given the unintentional aspect of some AI-driven market manipulation, there may be a need to cap the amount of maximum fines and compensation. A solution could be to sanction investment firms by ordering the disgorgement of profits or losses avoided, thus allowing one of the least used administrative powers in the arsenal of NCAs to find a scope of application. Furthermore, also trading venues should be held liable whenever they fail to take due care concerning the many legal obligations they face regarding the governance of algorithmic trading on their electronic platforms. Accordingly, whenever enforcement authorities find trading venues at fault, the latter will be held liable together with the investment firms deploying a malicious AI trading system. As a liability rule, a 'contributory negligence'/'reckless' standard could be applied to hold trading venues liable for their omissions.

* * *

Overall, the proposed multi-layered liability framework for AI trading manipulation is expected to deliver several benefits, including making malicious or reckless market actors internalise the costs of their AI trading misconduct. At the same time, it can also steer technological innovation towards safer applications for markets, thus enhancing social welfare without necessarily stifling innovation itself. An improved liability regime could also support victims' compensation while making investment firms invest in precautionary measures to develop safe AI trading systems and espouse a good market conduct-oriented corporate culture. Finally, it can ensure that those who pollute market integrity could more efficiently and effectively be held liable for their pollutive activity.[169]

---

[164] For instance, AI could also be thought of as an 'agent'. See Anat Lior, 'AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy' (2020) 46 Mitchell Hamline Law Review 1043, 1065-1075

[165] See Andrea Bertolini and Massimo Riccaboni, 'Grounding the case for a European approach to the regulation of automated driving: the technology-selection effect of liability rules' (2021) 51 European Journal of Law and Economics 243.

[166] For a discussion on the merits of using a 'strict' liability regime for AI misconduct and harm, see Anat Lior, 'AI Strict Liability vis-à-vis AI Monopolization' (2020) 22 Columbia Science & Technology Law Review 90.

[167] cf Gregory Scopino, *Algo Bots and the Law: Technology, Automation, and the Regulation of Futures and Other Derivatives* (CUP 2020) 435-38.

[168] See ibid, 439-443.

[169] Here, an analogy is drawn with the so-called 'polluter-pays' principle related to ecological harm.

5.3 Towards an improved and 'hybrid' institutional architecture of enforcement

The current EU anti-manipulation law and related institutional architecture of enforcement are weakened by several shortcomings that can ultimately jeopardise EU capital markets' integrity. These fragilities are mainly due to AI trading market ubiquity, technical specificities, and related additional manipulation risks. Hence, the following discusses possible pathways to promote an improved and 'hybrid' institutional architecture through a novel interplay between public and private enforcement.

.

- **Strengthening the EU public enforcement institutional infrastructure**

Two main obstacles seem to limit the effectiveness of the EU public enforcement institutional infrastructure to achieve credible deterrence. These include: (*i*) a lack of cohesive supervision and enforcement at the EU level; and (*ii*) the technological position of disadvantage faced by EU regulators and supervisors *vis-à-vis* private market participants.

First, the EU lacks a centralised framework for market conduct supervision, whereas law enforcement is not fully harmonised given too many persisting differences in Member States' national legal systems. Decentralised supervision and not fully integrated enforcement can constitute the EU framework's main obstacle to achieving credible deterrence of AI trading manipulation. With an uneven regulatory and enforcement playing field, risks of regulatory arbitrage can emerge, thus facilitating AI-driven manipulation. As a first step, a greater approximation in Member States' national laws seems desirable, which can be achieved through further EU harmonising legal instruments. Besides, a greater degree of cooperation among NCAs is necessary to deal with complex cross-asset, cross-market and cross-border manipulation cases. On a similar note, some believe that the best way to accomplish a high degree of supervisory coordination among NCAs could be to grant more powers to ESMA, thus moving towards a more centralised framework of market conduct supervision and enforcement.[170] Complementary to greater coordination among NCAs or more centralisation of supervisory powers on ESMA, it is the need to establish a unified EU trading data platform. Such a common infrastructure to analyse trading data could allow for more real-time and cross-border market conduct supervision and make possible direct data sharing among NCAs, thus enhancing their coordinative capacities. In this last regard, for instance, the recent Commission's proposal to establish a *European Single Access Point* database for securities trading, although limited to specific categories of companies and trading data, seems to go in the right direction.[171]

Second, EU financial regulators and supervisors face a more general issue. Namely, they must keep up with private organisations in using AI technology. Public authorities generally lack far behind private organisations in terms of technological tools and expertise. Therefore, they should be granted more resources to develop, test, and use AI methods for pursuing their institutional mandates and related tasks, such as market surveillance. Several scholars have highlighted the urgency to fill the technological gap of regulators and supervisors. Indeed, a new scholarship emphasising the role of supervisory technology ('SupTech') has emerged only in the last few years.[172] Whether public authorities alone will enjoy the adequate mindset, tools, and resources to enhance their SupTech capabilities can be doubtful; but novel public-private partnerships could also arise whenever required. However, SupTech to be effective requires the availability of data to detect and investigate suspicious cases of manipulation and state-of-the-art AI systems able to cope with those of malicious private actors. For instance, on the first aspect, ESMA also evaluates the possibility of enhancing

[170] See, e.g., Karel Lanoo, 'MiFID II and the new market conduct rules for financial intermediaries: Will complexity bring transparency?' (2017) ECMI Policy Brief 24 <www.ecmi.eu/sites/default/files/ecmi_pb_no_24_kl_marketconductrules.pdf> accessed 16 January 2022.

[171] See EU Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing a European single access point providing centralised access to publicly available information of relevance to financial services, capital markets and sustainability' (25 November 2021) COM/2021/723 final.

[172] See, e.g., Stefan Zeranski and Ibrahim E. Sancak, 'Digitalization of Financial Supervision with Supervisory Technology' (2020) 8 Journal of International Banking Law & Regulation 309.

and further standardising data reporting frameworks relating to compliance exercises about algorithmic trading by market actors.

- **Enabling private enforcement: is there a role for market manipulation 'bounty hunters'?**

In concluding the round of proposals, this last part discusses the merits and legal feasibility of introducing a new market actor within the already complex population of financial institutions: *i.e.*, market manipulation' bounty hunters'.[173]

Given all the struggles public authorities face to detect even the more conventional algorithmic forms of manipulation, there is a need to think of new tools for detecting the most sophisticated AI-driven manipulations. In this vein, 'bounty hunters' can be an attractive market-based solution, which has been already explored for specific problems inherent to economic law and regulation, such as in the antitrust law domain.[174] In imagining how these new market actors will operate, licensed market manipulation 'bounty hunters' could be in charge of directly supervising capital markets in multiple jurisdictions. In return for remuneration, 'bounty hunters' will be incentivised to scan market data to identify unusual trading patterns and report to public authorities suspicious transactions.[175] Adding it to existing whistleblowers programmes, the institutionalisation of market manipulation 'bounty hunters' can provide private firms with economic incentives to actively monitor EU capital markets, especially to fight cross-market and cross-border manipulation.[176] To operationalise market manipulation 'bounty hunters', however, EU regulators would need to design a specific legal framework, which should cover, at least, critical legal aspects such as their 'licensing' and 'remuneration structure'.[177] 'Bounty hunters' are not *per se* panacea. EU regulators would need to consider all the possible risks and benefits led by private enforcers of market conduct rules. On the one hand, 'bounty hunters' can be expected to enhance enforcement effectiveness through increased geographical coverage in market surveillance, enhanced expertise, more dedicated resources, and positive incentives for detecting and reporting suspicious transactions.[178] All this is expected to deliver greater levels of "certainty of punishment" for AI misconduct, thus making deterrence more credible. On the other, 'bounty hunters' can also lead to new market and regulatory failures. Primarily, 'bounty hunters' activity could result in overdeterrence. They could, in fact, report to regulators more suspicious trading conducts than necessary or even engage in false reporting, thus exacerbating issues of false positives.[179] Because motivated by the search for profits, 'bounty hunters' might face significant incentives to catch even bland and insignificant cases of suspected manipulation. In addition, as for the case of public authorities or market actors with some delegated responsibilities (*e.g.*, trading venues), 'bounty hunters' are not immune from risks of 'regulatory capture' by both industry players and public authorities.[180]

Overall, introducing 'bounty hunters' within the EU enforcement game is undoubtedly a fascinating and innovative idea to enhance law enforcement. Imagining a challenge to the last algorithm between manipulators and 'bounty hunters' could help direct technological innovation towards economic objectives closer to the need of the EU society. Moreover, if supported by a sound legal framework, 'bounty hunters' can deliver many expected benefits without substantially adding new risks to market integrity. Significantly, 'bounty hunters' could help enhance the AI regulatory science of public authorities, as the latter would work closely with market

---

[173] To the best of the author's knowledge, this is the first paper to discuss 'bounty hunters' within the EU capital markets context. For a first exploration of the same idea from a global perspective, see Miles Kellerman, 'Surveillance Games: The International Political Economy of Combatting Transnational Market Abuse' (DPhil thesis, University of Oxford 2020) <https://ora.ox.ac.uk/objects/uuid:3f22ea5c-8ce3-4574-9ede-886c88aa0423/download_file?safe_filename=DPhil_Thesis_Miles_Kellerman_July2020.pdf> accessed 16 January 2022.

[174] See Aleksandra Lamontanaro, 'Bounty Hunters for Algorithmic Cartels: An Old Solution for a New Problem' (2020) 30 Fordham Intellectual Property, Media and Entertainment Law Journal 1259.

[175] Kellerman (n 173) 242.

[176] ibid, 243.

[177] ibid, 247.

[178] ibid, 248.

[179] ibid, 249.

[180] ibid, 250.

participant experts, thus gaining meaningful insights from their use of technology and related scientific mindset.

6. Conclusions

This study has shown the challenges for EU regulators, supervisors, enforcement authorities, and market participants brought about constant progress in AI/ML methods within the ramification of algorithmic trading. If not adequately regulated, AI trading can expose EU capital markets' integrity to new and emerging risks of algorithmic market manipulation. Specifically, established legal frameworks and law enforcement regimes on the prohibition of market manipulation can leave AI trading operating in a (quasi-)lawless market environment. Under the lens of deterrence theory, this study has investigated the ability of the EU MAR/MAD enforcement regime to deter AI misconduct and harm credibly. The assessment has revealed the many weaknesses of the EU anti-manipulation law and enforcement in dealing with AI trading technical specificities and related additional risks. Uncertain legal prohibitions, inefficient liability rules and their varying interpretation and implementation among Member states, coupled with a decentralised institutional architecture of enforcement, constitute the main obstacles to achieving credible deterrence of AI-driven manipulation. Therefore, this study puts forward a number of policy proposals, including: (i) an improved, 'harm-centric' definition of manipulation; (ii) an improved, 'multi-layered' liability framework disentangling administrative and criminal aspects of AI-driven manipulation; and (iii) a novel, 'hybrid' public-private enforcement institutional architecture with a role for market manipulation 'bounty hunters'. All this is expected to improve the ability of EU regulators and enforcers to safeguard enforcement effectiveness within AI trading-driven markets.

Acknowledgements

I am grateful for comments by Prof. Wolf-Georg Ringe, Prof. H. Siegfriend Stiehl, Prof. Christoph Kumpan, Prof. Andrea Bertolini, Prof. Matteo Gargantini, Pedro Batista, Maria Grigoropoulou, Clara Martins Pereira, Hashem Nabbas, Patrick Raschner, Christopher Ruof, Roee Sarel, Antonella Zarra, as well as participants at the Ankara Yıldırım Beyazıt University Faculty of Law's 4th International Symposium on commercial law, the Tilburg Institute for Law, Technology and Society & Tilburg Law and Economics Center's international workshop on digital markets and enforcement, the Masaryk University international conference on cyberspace and law, and the Italian Society of Law & Economics' 17th annual Conference on law & economics. Funding from the Hamburg "Law, Finance, and Technology" project, sponsored by Joachim Herz Foundation, is gratefully acknowledged (https://LFT.ile-hamburg.de).

References

Abbott R and Sarch A, 'Punishing Artificial Intelligence: Legal Fiction or Science Fiction' (2019) 53 University of California Davis Law Review 323

Acemoglu D, 'Harms of AI' (2021) NBER Working Paper 29247

Allen F and Gale D, 'Stock-Price Manipulation' (1992) 5 The Review of Financial Studies 503

Arlen J and Carney WJ, 'Vicarious Liability for Fraud on Securities Markets: Theory and Evidence' (1992) University of Illinois Law Review 691

Arlen J, 'Corporate criminal liability: theory and evidence' in Alon Harel and Keith N. Hylton (eds) *Research Handbook on the Economics of Criminal Law* (Edward Elgar Publishing 2012) 144

Avgouleas E, *The Mechanics and Regulation of Market Abuse: A Legal and Economic Analysis* (OUP 2005)

Awrey D and Judge K, 'Why Financial Regulation Keeps Falling Short' (2020) 61 Boston College Law Review 2295

Azzutti A, Ringe W-G and Stiehl HS, 'Machine Learning, Market Manipulation and Collusion on Capital Markets: Why The 'Black-Box' Matters' (2021) 43 University of Pennsylvania Journal of International Law

Bank of England and U.K. Financial Conduct Authority, *Machine learning in UK financial services* (2019)

Becker GS, 'Crime and Punishment: An Economic Approach' (1968) 76 Journal of Political Economy 169

Bertolini A and Riccaboni M, 'Grounding the case for a European approach to the regulation of automated driving: the technology-selection effect of liability rules' (2021) 51 European Journal of Law and Economics 243

Boehmer E, Fong K and Wu J, 'Algorithmic Trading and Market Quality: International Evidence' (2020) 56 Journal of Financial and Quantitative Analysis 2659

Burrell J, 'How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms' (2016) 3 Big Data & Society

Busch D, 'The Private Law Effect of MiFID: the Genil Case and Beyond' (2017) 13 European Review of Contract Law 70

Carvajal A and J Elliott, *The Challenges of Enforcement in Securities Markets: Mission Impossible?* IMF Working Paper (August 2009) WP/09/168

Chesterman S, 'Artificial Intelligence and the Limits of Legal Personality' (2020) 69 International & Comparative Law Quarterly 819

Clarke R, 'Regulatory Alternatives for AI' (2019) 35 Computer Law & Security Review 389

Cliff D, Brown D and Treleaven P, 'Technology Trends in the Financial Markets: A 2020 Vision' (UK Government Office for Science, 2011)

Coffee JC, 'Law and the Market: the Impact of Enforcement' (2007) 156 University of Pennsylvania Law Review 229

Cosme O, ‘Regulating High-Frequency Trading: The Case for Individual Criminal Liability’ (2019) 109 Journal of Criminal Law and Criminology 365

Dalko V and Wang MH, ‘High-Frequency Trading: Order-Based Innovation or Manipulation?’ (2020) 21 Journal of Banking Regulation 289

Dellermann D, Ebel P and Leimesiter JM, ‘Hybrid Intelligence’ (2019) 61 Business & Information Systems Engineering 637

Diamantis M, ‘Algorithms Acting Badly: A Solution From Corporate Law’ (2021) 89 The George Washington Law Review 801

Donald DC, ‘Regulating Market Manipulation trough an Understanding of Price Creation (2011) 6 NTU Law Review 55

Easterbrook FH and Fischel DR, ‘Mandatory Disclosure and the Protection of Investors’ (1984) 70 Virginia Law Review 674

Ebers M, ‘Regulating AI and Robotics: Ethical and Legal Challenges’ in Martin Ebers and Susana Navas (eds) *Algorithms and Law* (CUP 2020)

ESMA, *MAR Review Report* (23 September 2020) ESMA70-156-2391

ESMA, *MiFID II Review Report on Algorithmic Trading* (28 September 2021), ESMA70-156-4572

Fenwick MD, Kaal AW and Vermeulen EPM, ‘Regulation Tomorrow: What Happens When Technology Is Faster than the Law?’ (2017) 6 American University Business Law Review 561

Financial Stability Board, *Artificial intelligence and machine learning in financial services* (2017)

Fischel DR and Ross DJ, ‘Should the Law Prohibit ‘Manipulation’ in Financial Markets?’ (1991) 105 Harvard Law Review 503

Fletcher G-G, ‘Macroeconomic Consequences of Market Manipulation’ (2020) 83 Law and Contemporary Problems 123

Fletcher G-G, ‘Deterring Algorithmic Manipulation’ (2021) 74(2) Vanderbilt Law Review 101

Fox MB, Glosten LR and Rauterberg G, ‘Stock Market Manipulation and Its Regulation’ (2018) 35 Yale Journal of Regulation 67

Gargantini M, ‘Public Enforcement of Market Abuse Bans. The ECtHR Grande Stevens Decision’ (2015) 1 Journal of Financial Regulation 149

Gargantini M, *The European Regulation of Securities Exchanges: Regulated Markets in an Evolving Technological and Legal Context* (Giappichelli Editore, 2021)

Gerner-Beuerle C, ‘Algorithmic Trading and the Limits of Securities Regulation’ in Emilios Avgouleas and Heikki Marjosola (eds), *Digital Finance in Europe: Law, Regulation, and Governance* (De Gruyter 2022) 109

Hallevy G, *Liability for Crimes Involving Artificial Intelligence Systems* (Springer 2015)

IOSCO, *Credible Deterrence in the Enforcement of Securities Regulation* (2015)

IOSCO, *The use of artificial intelligence and machine learning by market intermediaries and asset managers* (2021)

Neil Johnson et al, ‘Abrupt rise of new machine ecology beyond human response time’ (2013) 3 Science Report 2627

Karremand J and Schoeller MG, ‘MiFID II between European rule-making and national market surveillance: the case of high-frequency trading’ in Adrienne Héritier and Magnus G. Schoeller (eds) *Governing Finance in Europe: A Centralisation of Rulemaking?* (Edward Elgar Publishing 2020)

Kellerman M, ‘Surveillance Games: The International Political Economy of Combatting Transnational Market Abuse’ (DPhil thesis, University of Oxford 2020)

Khanna VS, ‘Corporate criminal liability: What purpose does it serve’ (1995) Harvard Law Review 1477

Kirilenko AA and Lo AW, 'Moore's Law versus Murphy's Law: Algorithmic Trading and Its Discontents' (2013) 27 Journal of Economic Perspectives 51

Koshiyama A, Firoozye N and Treleaven P, 'Algorithms in Future Capital Markets' (2020) Proceedings of ACM ICAIF '20

Lamontanaro A, 'Bounty Hunters for Algorithmic Cartels: An Old Solution for a New Problem' (2020) 30 Fordham Intellectual Property, Media and Entertainment Law Journal 1259

Lanoo K, 'MiFID II and the new market conduct rules for financial intermediaries: Will complexity bring transparency?' (2017) ECMI Policy Brief 24

Lee J and Schu L, 'Regulating of Algorithmic Trading: Framework for Human Supervision and Direct Market Interventions (2021) European Business Law Review (forthcoming)

Lehmann M and Kumpan C, *European Financial Services Law: Article-By-Article Commentary* (Nomos 2019)

Lin TCW, 'The New Financial Industry' (2014) 65 Alabama Law Review 567

Lior A, 'AI Strict Liability vis-à-vis AI Monopolization' (2020) 22 Columbia Science & Technology Law Review 90

Lior A, 'AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy' (2020) 46 Mitchell Hamline Law Review 1043

Luchtman M and Vervaele J, 'Enforcing the Market Abuse Regime: Towards an Integrated Model of Criminal and Administrative Law Enforcement in the European Union?' (2014) 5(2) New Journal of European Criminal Law 192

Martins Pereira C, 'Unregulated Algorithmic Trading: Testing the Boundaries of the European Algorithmic Trading Regime' (2021) 6 Journal of Financial Regulation 270

Nagel S, *Machine Learning in Asset Pricing* (PUP 2021)

Nelemans M, 'Redefining Trade-Based Market Manipulation' (2008) 42 Valparaiso University of Law Review 1169

OECD, *The Liability of Legal Persons for Foreign Bribery: A Stocktaking Report* (2016)

OECD, *Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers* (2021)

Paternoster R, 'The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues' (1987) 4(2) Justice Quarterly 173

Perrone A, 'EU Market Abuse Regulation: The Puzzle of Enforcement' (2020) European Business Organization Law Review 379

Polinksy AM and Steven Shavell, 'The Optimal Use of Fines and Imprisonment' (1984) 24 Journal of Public Economics 89

Pupillo L, Fantin S, Ferreira A and Polito C, 'Artificial Intelligence and Cybersecurity: Technology, Governance and Policy Challenges' (2021) CEPS Task Force Report, Brussels

Rahbi FA, Mehandjiev N and Baghdadi A, '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 Financial Industry, 10th International Workshop, FinanceCom 2020, Helsinki, Finland, August 18, 2020* (Springer 2020)

Rahwan I et al, 'Machine Behaviour' (2019) 568 Nature 477

Raschner P, 'Algorithms put to test: Control of algorithms in securities trading through mandatory market simulations?' (2021) European Banking Institute Working Paper Series 2021 - no. 87

Rose A, 'The Multienforcer Approach to Securities Fraud Deterrence: A Critical Analysis' (2010) 158 University of Pennsylvania Law Review 2173

Scopino G, *Algo Bots and the Law: Technology, Automation, and the Regulation of Futures and Other Derivatives* (CUP 2020)

Senior Supervisors Group, *Algorithmic Trading, Briefing Note* (April 2015)

Treleaven P, Galas M and Lalchand V, 'Algorithmic Trading Review' (2013) 56(11) Communications of the ACM 76

Ventoruzzo M and Mock S, *Market Abuse Regulation: Commentary and Annotated Guide* (OUP 2017)

Yadav Y, 'The Failure of Liability Liability in Modern Markets' (2016) 102 Virginia Law Review 1031

Zeranski S and Sancak IE, 'Digitalization of Financial Supervision with Supervisory Technology' (2020) 8 Journal of International Banking Law & Regulation 309