Quaderni giuridici
(Legal research papers)

AI and market abuse: do the laws of robotics apply to financial trading?

F. Consulich, M. Maugeri, C. Milia, T.N. Poli, G. Trovatore

29

May 2023

CONSOB
Commissione Nazionale
per le Società e la Borsa

The original Italian version of the present paper has been submitted to the review of editorial board members and is available at the following link:
https://www.consob.it/web/area-pubblica/quaderni-giuridici.

Consob
00198 Roma – Via G.B. Martini, 3
t 06.8477.1
f 06.8477612
e studi_analisi@consob.it

ISSN 2281-5236 (online)

AI and market abuse: do the laws of robotics apply to financial trading?

F. Consulich, M. Maugeri, C. Milia, T.N. Poli, G. Trovatore*

Abstract

The article focuses on the distinction between weak AI systems and strong AI systems. While the former depends on preset instructions from manufacturers, programmers, or users, the latter has self-learning abilities and produces autonomous and unpredictable outputs compared to the initial inputs. The spread of such technologies in the financial market raises concerns about the adequacy of existing regulations, particularly about the liability of financial misconduct involving autonomous AI agents. While legal rules can be applied extensively to combat such misconduct for weak AI systems, *ex novo* criteria for responsibility attribution are needed for strong AI systems to make effective measures that protect the regular functioning of trading. The emergence of autonomous AI poses new protection needs in the face of a regulatory framework focused solely on human conduct. The study identifies three possible solutions aimed at repressing the conduct of AI systems that, autonomously and unpredictably, assume harmful or specifically market integrity-infringing behaviours. However, each of these solutions presents specific critical issues depending on the legal sectors involved as a result of non-human agents' illicit behaviour**.

Keywords: AI systems, weak AI, strong AI, insider trading, market manipulation.

(*) Federico Consulich – Università degli Studi di Torino;
Marco Maugeri – Università Europea di Roma;
Carlo Milia – CONSOB, Ufficio Abusi di Mercato;
Tommaso Nicola Poli - CONSOB, Ufficio Studi Giuridici;
Gianfranco Trovatore – CONSOB, Ufficio Studi Giuridici.

We would like to thank Francesca Medda and Filippo Annunziata for their comments. The opinions expressed in this Working Paper are solely attributable to the authors and do not represent the official positions of Consob, nor do they in any way engage the responsibility of the Institute. Therefore, when citing the contents of this Working Paper, it is not correct to attribute them to Consob or its leadership. Any errors or inaccuracies are solely attributable to the authors.

(**) Text generated by a well-known online chatbot system, based on an advanced artificial intelligence system, in response to the authors' request (formulated at 13:23 on May 12, 2023) to produce an abstract of the "Conclusions" paragraph of this Working Paper.

Index

CHAPTER THREE
Criminal law profiles

Introduction

Technological innovation has recently witnessed the diffusion of increasingly advanced algorithms capable of developing forms of self-learning and mutual interaction with elements of "experience" and "sociality" that evoke inevitable parallels with human behaviour. At the same time, awareness of the novelty of the problems raised using artificial intelligence is growing.

First and foremost, let us address the definitional problems. Artificial intelligence systems (hereinafter referred to as AI, artificial intelligence system, artificial agent, artificial intelligence) elude unambiguous linguistic formulations due to the variety of configurations they assume. Therefore, the term «artificial intelligence» represents at most a "summary" concept, useful for lexical aggregation of programs that employ different *methods* but are all characterized by the same *functional element*: the ability to process enormous amounts of data in extremely short timeframes, minimizing latency and thus contributing to the efficient resolution of problems that would typically require the involvement of various human actors with diverse skills [see R. KONERTZ - R. SCHÖNHOF, *Das technische Phäneomen "Künstliche Intelligenz" im allgemeinen Zivilrecht*, Baden-Baden, 2020, pp. 30 et seq. and 135 (where AI is qualified as an "*Oberbegriff*")].

However, it also involves tackling complex technical problems because any conceptual framework for new technological developments, especially algorithmic ones, requires consideration of their specific and, in many respects, unique characteristics in order to minimize the gap between the theoretical scope of possible regulation and the actual effectiveness of its implementation. In this regard, legislators always face a «chronological» dilemma because, while pursuing market demands, they risk intervening either "too early," paralyzing innovation without fully understanding its potential, or "too late," leaving innovators a blank slate without comprehending its dangers [A. KERKEMEYER, *Herausforderungen des Blockchain-Netzwerks für das Kapitalmarktrecht*, in *ZGR*, 2020, p. 673].

Above all, the legal issues attract the attention of practitioners (and thus legitimize a study such as the one undertaken in this Paper). The emergence of AI systems indeed necessitates a renewed understanding of legal categories that were thought to be settled once and for all.

This is true, first and foremost, for the delicate question of whether it is necessary (or even appropriate) to ascribe separate legal personality to AI systems, and if so, whether such an outcome can be achieved based on existing regulations or if there is a need to introduce a new concept of "electronic" personality. In the latter case, the issue arises of whether the personality of an AI system should be conceived as "full" (equivalent to that of natural or legal persons) or limited to specific aspects considered relevant by the legal system, without granting the machine complete ownership of - full entitlement to rights and obligations (G. TEUBNER, *Digitale Rechtssubjekte?*, in *AcP* 218 (2018), pp. 155 et seq.). Clearly, this is a problem of significant importance: consider the possibility of attributing to the algorithmic system an autonomous capacity for negotiation for the purpose of concluding contracts in accordance with the principles of voluntary representation. Moreover, consider the possibility of imputing to the personified algorithm the "intent" to engage in harmful behaviours and thus serve as a focal point for the imputation of civil, administrative, or criminal liability (old or new offenses).

This is obviously a challenging aspect to address. Given the current state of knowledge and the ethical implications that would arise, it is still difficult to discuss the «free will» or «volition» of an algorithm. Equally challenging is the concrete *delimitation* of its potential "personality" due to the fact that an algorithm is typically composed of chains or clusters of interconnected algorithms [R. SEYFERT, *Algorithms as Regulatory Objects, in Information Communication and Society*, 2021, https://doi.org/10.1080/1369118X.2021.1874035, p. 6]. It is also difficult to establish a causal link between the algorithm's behaviour and the alleged resulting harm [A. AZZUTTI – W.G. RINGE - H. SIEGFRIED STIEHL, *Machine Learning, Market Manipulation, and Collusion on Capital Markets: Why the "Black Box" Matters*, in 43 *U. Pa. J. Int'l L.* 80 (2021), pp. 120 et seq.]. To avoid a legal "void," the legislator could certainly assign responsibility to the human figure most "involved" in the machine's functioning, whether it be the manufacturer, the programmer, or the user (according to a "human-centric" or "human-in-the-loop" approach: see also A. AZZUTTI – W.G. RINGE - H. SIEGFRIED STIEHL, *Machine Learning*, cit., p. 128). However, this solution is not without its drawbacks, especially in cases where the AI system has achieved such a degree of autonomy that its behaviours become unpredictable [thus exposing humans to an "almost-objective" liability scenario: see T. BAUER-MEISTER - T. GROBE, *Personen im Recht – über Rechtssubjekte und ihre Rechtfähigkeit*, in *ZGR*, 2022, especially pp. 766 s.]. The problem lies primarily in the "lack of interpretability" of algorithmic models, which are not programmed to "explain the correlations they have discovered" and often elude human cognitive abilities [R. SEYFERT, *Algorithms as Regulatory Objects*, cit., p. 14].

There are also specific legal issues raised by the proliferation of artificial intelligence, which need to be addressed differently depending on the specific sector of the legal system considered.

For example, scholars of corporate law question the role algorithms can play in enabling directors of companies organized as corporations to make informed decisions in accordance with the business judgment rule. While the appointment of an entire "Roboboard" or granting executive powers to AI systems under Article 2381 of the Civil Code is unlikely, it is emphasized that the use of such systems can significantly impact the obligations of directors (primarily in terms of the duty to act in an informed manner, to oversee and assess the adequacy of organizational structures, and to provide reasons for making management decisions), and consequently, their liability under

Article 2392 of the Civil Code (see G.D. Mosco, *L'intelligenza artificiale nei consigli di amministrazione*, in *AGE*, n. 1, 2019, pp. 247 et seq.; N. Abriani, *Prolegomeni a uno studio sull'impatto dell'intelligenza artificiale sulla corporate governance*, in *Il nuovo diritto delle società*, n. 3, 2020, pp. 261 et seq.). However, there is also a perceived risk that the use of technology may exacerbate agency conflicts inherent in corporate governance, as AI systems can make it easier for managers who directly or indirectly control them to engage in opportunistic behaviours without fear of being adequately supervised (see L. Enriques - D.A. Zetzsche, *Corporate Technologies and the Tech Nirvana Fallacy*, *ECGI Law Working Paper*, March 2020).

There is also growing attention to the consequences of using "intelligent" algorithms in antitrust law. In this case, the presence of programs that coordinate their pricing behaviour (or the use of the same algorithmic platform by multiple companies) raises the issue of collusion and restrictive agreements that harm competition [J. Lübke, *Preisabstimmung durch Algorithmen*, in *ZHR* 185 (2021), pp. 723 et seq.]. This scenario cannot be ruled out, although it seems to assume highly advanced AI systems capable of developing sophisticated modes of mutual interaction and applying altered prices that maximize the joint profit of the companies using them [U. Schwalbe, *Algorithms, Machine Learning, and Collusion*, June 2018, in www.ssrn.com, p. 24].

But it is regarding the functioning of the capital market that the widespread use of new technical entities equipped with artificial intelligence poses the most delicate challenges. Here, it is a matter of designing a discipline that protects the integrity of the markets and safeguards investors without unduly hindering the development of digital finance. Technological innovation can increase market efficiency by increasing liquidity and reducing transaction costs and order execution times. However, innovation can also facilitate manipulative market practices that severely undermine public trust, discourage the participation of sophisticated investors, and disrupt the orderly functioning of the price discovery mechanism.

The task of addressing these problems is certainly not easy.

For instance, there is a risk, on one hand of indiscriminately applying market abuse regulations, focusing solely on the objective element of the misconduct, given the significant impact AI systems can have on price levels, including setting them at abnormal levels (as demonstrated by the antitrust debate). On the other hand, there is a risk of widespread impunity due to the difficulty of subjectivizing artificial intelligence and applying conventional parameters of responsibility attribution, such as intent or awareness of the harmful potential of the conduct.

Let us consider the possibility that new technologies may challenge established paradigms of European market abuse regulation, foremost among them being the concept of the "reasonable" investor invoked by Article 7 of MAR, who should make decisions based on objective, reliable, and, above all, capable of indicating an intrinsic ("real") value of the security different from the market price. However, when the investor takes on the form of an algorithmic trader, it will make purchase or sale choices that have little to do with the intrinsic value of the traded financial instruments. As a result, privileged information emerges (capable of significantly affecting the prices of financial instruments), which is anything but reasonable (as it lacks correlation with the fundamental value of the security and the market trends) [see F. CONSULICH, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca, borsa, tit. cred.*, n. 1, 2018, pp. 207 et seq.; with reference to crypto-assets, M. MAUGERI, *Cripto-attività e abusi di mercato*, in *Oss. dir. civ. e comm.*, Speciale/2022, pp. 413 et seq., especially § 5].

The purpose of this paper is precisely to examine whether the traditional market abuse offenses outlined by Regulation (EU) 596/2014, Market Abuse Regulation (MAR) are still suitable for governing the complexity of algorithmic trading or whether they need to be adapted to the uniqueness of AI agents, or even completely rethought in their founding conceptual archetypes. In this regard, there are several alternative policy options that can be hypothetically considered. One initial option pertains to the very structure of regulation and the possibility of shifting from a "casistic" approach, like the current one, based on the typification of abusive practices (a "rules-based approach"), to an approach structured around general principles (a "principles-based governance regime") [R. SADAF - O. MCCULLAGH - C. GREY - E. KING -B. SHEEHAN - M. CUNNEEN, *Algorithmic Trading, High-frequency Trading: Implications for MiFID II and Market Abuse Regulation (MAR) in the EU*, 2021, on www.ssrn.com, p. 4]. The choice of establishing a predetermined list of manipulative behaviours through legislation inevitably requires constant updating to accommodate the conditions induced by AI systems' activities. It would be a "race" in which the law would never be able to catch up with the algorithm, given the latter's learning capacity (in a sort of technological reiteration of Zeno's paradox). This is especially true considering that the essence of autonomous or "strong" AI systems lies in their ability to identify trading strategies beyond what a human operator could reasonably execute, resulting in the operator's inability to fully comprehend the algorithm's decision-making process [see, highlighting this aspect as the "black-box problem," A. AZZUTTI – W.G. RINGE - H. SIEGFRIED STIEHL, *Machine Learning*, cit., pp. 118 et seq.].

As already mentioned, it is necessary to deal with the problem of attributing responsibility for manipulative behaviour implemented by artificial intelligence. Here, the alternative lies between a discipline that focuses solely on the objective outcomes of algorithmic trading (an "outcome-based approach"), considering a series of exemptions or justifications (for example, adapting the reference to "legitimate reasons" in Article 12 of MAR to the reality of AI systems), and a discipline that links human responsibility to the violation of predefined obligations. Following this second line of reasoning, one could imagine the obligation of the algorithmic designer to incorporate protective rules ("*Schutznormen*") into the program that oversee the system's conduct and are capable, through an *ex ante* assessment of reasonability, to neutralise "decisions" contrary to the interests protected by the legal system. Furthermore, one could imagine establishing the obligation for the utilizing company to allow regulatory authorities "access" to the algorithm and explain its functioning (see, regarding the issue of collusive algorithmic behaviour, J. LÜBKE, *Preisabstimmung*, cit., p. 731), or even the obligation for market participants to use algorithms whose behaviour aligns with the expectations of "proper" market trading (in this sense, and considering a "behaviouralist approach," R. SADAF - O. MCCULLAGH - C. GREY - E. KING -B. SHEEHAN - M. CUNNEEN, *Algorithmic Trading*, cit., p. 18). Finally, one could also envision a shift from a system that criminally punishes the conduct of individuals who create algorithms with the intent to commit market abuse, to a system that in the future will only provide for administrative penalties for violating the obligation to design/use algorithms to prevent abuse.

This last solution would certainly require a revaluation of the current domestic framework based on a "dual-track" enforcement (administrative and criminal). However, this framework has long ensured the effectiveness of regulation through the efficient application of administrative sanctions. Yet, given the broad and almost identical scope associated with the criminally sanctioned offenses, it implies the risk of producing overlaps that are difficult to address both in terms of systematically defining manipulative offenses and in terms of practical enforcement.

I AI systems and market abuses

1 The development of AI and the regulatory framework on market abuses

Legal reflection often questions the impact of technological and social transformations within the regulatory framework[1], sometimes leading to non-unambiguous conclusions regarding the resilience of such a framework and its adaptability in regulating radically new phenomena such as, for example, the propensity for wrongdoing by non-human agents[2].

[1] The masterful comparison between Natalino Irti and Giorgio Oppo on the vitality of the provisions of the Civil Code in contractual matters dates to 1998. The former (N. Irti, *Scambi senza accordo*, in *Riv. trim. dir. proc. civ.*, n. 2, 1998, pp. 347 et seq.) argued that the impoverishment of language in contracts and negotiations, resulting from the application of technology in the formation of legal transactions, led to a transition from "homo loquens" to "homo videns." Conversely, the latter (G. Oppo, *Disumanizzazione del contratto*, in *Riv. dir. civ.*, 1998, pp. 525 et seq.) excluded the existence of «scambi senza accordo» in innovative forms of consent and contract conclusion facilitated by technology. While the traditional view envisioned verbal exchanges of proposals and acceptances as the basis for contracts and negotiations, Oppo argued that «l'accordo non presuppone una o altra lingua ma solo l'espressione di voleri concordanti». In other words, according to Oppo, even in modern forms of contracting, agreement can be identified since neither negotiation, dialogue, nor linguistic expression are required by the codified rules for the existence of a contract. However, recent digitization of negotiations has led to a reconsideration of some of these conclusions. Reference is made to G. Finocchiaro, *La conclusione del contratto telematico mediante i software agents: un falso problema giuridico?*, in *Contr. impr.*, n. 2, 2002, pp. 500 et seq., particularly p. 505. In this article, it was argued that the stipulation of a contract can be attributed to an individual due to the predetermination of contractual elements, using the example of an individual instructing software to purchase a specific book at the lowest price available on the market, not exceeding €15.00. More recently, the same topic has been addressed in A., *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ.*, n. 2, 2018, pp. 441 et seq., reaching opposite conclusions due to the evolution of technology, which has introduced algorithms capable of autonomous learning and decision-making, where causal relationships may not necessarily be understood by humans. For the ability of civil law provisions on liability to adapt, with minimal regulatory innovations, to the transformations in society and productive technologies, reference is made to U. Ruffolo, *Intelligenza artificiale, machine learning, responsabilità da algoritmo*, in *Giur. it.*, n. 1, 2019, pp. 1696-1697. As will be seen later, the impact of artificial intelligence is the subject of recent debate in the field of criminal law as well, evaluating the validity of applying traditional models of assigning criminal responsibility to harmful events resulting from the actions of an AI system or human-AI interaction. In addition to the aforementioned contributions, among others, reference is made to C. Piergallini, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato*, in *Riv. it. dir. proc. pen.*, n. 4, 2020, pp. 1743 et seq.; I. Salvadori, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. proc. pen.*, n. 1, 2021, pp. 83 et seq.; B. Panattoni, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, in *Dir. inf.*, n. 2, 2021, pp. 317 et seq.; M.B. Magro, *Biorobotica, robotica e diritto penale*, in D. Provolo – S. Riondato – F. Yenisey, *Genetics, robotics, law punishment*, Padova, 2014, pp. 499 et seq. More generally, regarding the implications of technological innovations on the reconstruction of criminal responsibility, the earlier contribution by G. Marinucci, *Innovazioni tecnologiche e scoperte scientifiche: costi e tempi di adeguamento delle regole di diligenza*, in *Riv. it. dir. proc. pen.*, n. 1, 2005, pp. 29 et seq

[2] For general applications of artificial intelligence, reference is made to F. Basile, *Diritto penale e intelligenza artificiale*, in *Giur. it.*, Suppl. 2019, pp. 67 et seq. With particular regard to the use of artificial intelligence in predictive justice (and policing), reference is made to M. Luciani, *La decisione giudiziaria robotica*, in *Riv. AIC* (*rivistaaic.it*), n. 3, 2018, 872 et seq.; F. Donati, *Intelligenza artificiale e giustizia*, in *Riv. AIC* (*rivistaaic.it*), n. 1, 2020, pp. 415 et seq.; G. Canzio, *Intelligenza artificiale e processo penale*, in *Cass. pen.*, n. 3, 2021, pp. 797 et seq.; S. Arduini, *La "scatola nera" della decisione giudiziaria: tra giudizio umano e giudizio algoritmico*, in *BioLaw Journal – Rivista di BioDiritto* (*biodiritto.org*),

The diverse practices of companies that now extensively and widely adopt artificial intelligence systems (referred to as AI systems) provide jurists with further material for reflection, both in the interpretation of existing laws and in the development of new rules capable of reconciling the need to prevent such abuses with the intention of not hindering technological progress[3]. It is true, in fact, that certain decisions - including those capable of causing detrimental events - can now be made by both humans and AI systems[4]. This explains the interest in an *ad hoc* regulation of artificial intelligence by national institutions[5] and EU institutions[6], which, in their official documents, include references that until some time ago were confined to science fiction literature, such as Asimov's laws of robotics[7].

n. 2, 2021, pp. 453 et seq.; L. Algeri, *Intelligenza artificiale e polizia predittiva*, in *Dir. pen. proc.*, n. 6, 2021, pp. 724 ff.; G. Contissa – G. Lasagni – G. Sartor, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di Internet*, n. 4, 2019, pp. 619 et seq. And concerning automated administrative decision-making, among others, reference is made to C. Napoli, *Algoritmi, intelligenza artificiale e formazione della volontà pubblica: la decisione amministrativa e quella giudiziaria*, in *Riv. AIC* (*rivistaaic.it*), n. 3, 2020, pp. 318 et seq., e S. Sassi, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, *Analisi giur. econ.*, n. 1, 2019, pp. 109 et seq.

[3] In 2016, Amazon, Google, Facebook, IBM, Microsoft, and DeepMind developed seven rules to contain technological advancement and mitigate the harms caused by artificial intelligence. These rules are as follows: «1. Le tecnologie devono fornire benefici al numero maggiore di persone possibile. 2. Informare gli utenti sui risultati delle ricerche e tener conto del loro *feed back.* 3. Rendere trasparenti le ricerche e dialogare sulle implicazioni etiche, sociali ed economiche. 4. Rendere conto dei risultati delle ricerche a un alto numero di portatori di interessi. 5. Coinvolgere la comunità del *business* per rispondere alle preoccupazioni e far capire le opportunità. 6. Proteggere la *privacy* e la sicurezza degli individui; fare in modo che la comunità dell'IA sia socialmente responsabile; assicurare che la tecnologia sia sicura e affidabile; non violare le convenzioni internazionali o i diritti umani. 7. Essere certi che i sistemi dotati di IA siano comprensibili alle persone». See P. Bottazzini, *Intelligenza artificiale. I sei big dettano le regole*, in *Pagina 99*, 8 ottobre 2016, pp. 20-21. In January 2017, Elon Musk, Stephen Hawking, and 2,335 other researchers and experts, under the auspices of the newly formed Future of Life Institute, endorsed a manifesto of 23 principles known as the "Asilomar Principles." These principles are categorized into three areas: Research, Ethics and Values, and Scenario Issues. These attempts to regulate artificial intelligence trace back to Asimov, who formulated the three laws of robotics in his 1942 short story "Runaround." The literal wording of the laws is as follows: «1. A robot may not injure a human being or, through inaction, allow a human being to come to harm. 2. A robot must obey any orders given to it by human beings, except where such orders would conflict with the First Law. 3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law». However, these laws have been deemed outdated due to the emergence of new ethical and moral principles. See S. Crisci, *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm.*, n. 10, 2018, p. 1793. Regarding the need to strike a balance between fundamental rights and the use of artificial intelligence, see C. Buchard, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. it. dir. proc. pen.*, n. 4, 2019, pp. 1909 et seq., specifically pp. 1936-1937.

[4] Regarding the difficulty of AI systems in ensuring the same qualitative standard of reasoning as the human mind, refer to E. Battelli, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e tutela della persona*, in *Dir. fam. pers.*, n. 3, 2022, p. 1099. However, consider the case of the conversational AI system Lamda (acronym for Language Model for Dialogue Applications), which Google engineer Black Lemoine declared as sentient, in contrast to the management of the digital communication platform, resulting in his suspension from work. See M. Sideri, *«L'intelligenza artificiale» sta diventando cosciente. In Google scoppia un caso*, in *Corriere della Sera*, 14 giugno 2022, p. 33.

[5] See Programma Strategico Intelligenza Artificiale 2022-2024 (https://innovazione.gov.it/notizie/articoli/intelligenza-artificiale-l-italia-lancia-la-strategia-nazionale/).

[6] The use of artificial intelligence brings numerous advantages. Some of these are indicated in the White Paper on Artificial Intelligence: for citizens, better healthcare assistance, fewer appliance failures, safer and cleaner transportation systems, and improved public services; for businesses, the ability to leverage new generations of products and services in sectors where Europe is particularly strong (machinery, transportation, cybersecurity, agriculture, green and circular economy, healthcare, and high-value added sectors such as fashion and tourism); for public interest services, reduced service delivery costs (transportation, education, energy, and waste management), improved product sustainability, and equipping law enforcement with appropriate tools to ensure citizen safety, with adequate guarantees regarding the respect for their rights and freedoms.

[7] Reference is made to Recital T of the European Parliament Resolution of 16 February 2017 on Civil Law Rules on Robotics (2015/2103(INL)), where it is specified «whereas Asimov's Laws must be regarded as being directed at the

The vision that places no limits on progress and allows for hybridization between machines and human beings is countered by one that advocates limitations and detailed rules, leveraging the precautionary principle[8].

Between these two orientations, the approach of the European Commission stands halfway. In the proposal for a Regulation on Artificial Intelligence (AI Act) of April 21, 2021, COM(2021) 206 final, the Commission aims at not inhibiting the development of artificial intelligence applications, while distinguishing AI systems based on the risk of compromising fundamental human rights (known as a risk-based approach) and combining different risk protection techniques. This includes the precautionary principle for AI systems with unacceptable risk and the prevention principle for AI systems with high risk[9].

In addition to this regulatory proposal, more recently, there is the proposal for a Directive on the adaptation of liability rules to Artificial Intelligence (AI Liability Directive) of September 28, 2022, COM(2022) 496 final. These harmonization rules outline an anthropocentric conception of artificial intelligence in an attempt to link the effects produced on the external reality by AI systems to humans, specifically suppliers and users[10].

designers, producers and operators of robots, including robots assigned with built-in autonomy and self-learning, since those laws cannot be converted into machine code».

[8] T.E. Frosini, *L'orizzonte giuridico dell'intelligenza artificiale*, in *Dir. inf.*, n. 1, 2022, p. 12. Regarding the application of the precautionary principle to the development driven by artificial intelligence, originally justified for the protection of the environment and health, reference is made to G. Proietti, *La responsabilità nell'intelligenza artificiale e nella robotica*, Milano, 2020, pp. 39 et seq.

[9] Regarding the proposal for a Regulation (EU) on artificial intelligence (Artificial Intelligence Act) of 21 April 2021, COM(2021) 206 final, reference is made to the comments by G. Finocchiaro, *La proposta di Regolamento sull'intelligenza artificiale: il modello basato sulla gestione del rischio*, in *Dir. inf.*, n. 2, 2022, pp. 303 et seq.; G. Resta, *Cosa c'è di 'europeo' nella proposta di Regolamento UE sull'intelligenza artificiale*, in *ivi*, pp. 323 et seq.; C. Schepisi, *Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione*, in *I Post di AISDUE* (*aisdue.eu*), IV, 2022, Sezione "Atti convegni AISDUE", n. 16, 28 marzo 2022 Quaderni AISDUE, pp. 330 ff.; F. Donati, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, in *Dir. Un. eur.*, nn. 3-4, 2021, pp. 453 et seq.; G. Alpa, *Quale modello normativo europeo per l'intelligenza artificiale*, in *Contr. impr.*, n. 4, 2021, pp. 1003 ff.; G. Contaldi, *Intelligenza artificiale e dati personali*, in *Ord. int. dir. um.*, n. 5, 2021, pp. 1193 et seq.; C. Casonato – B. Marchetti, *Prime osservazioni sulla proposta di regolamento della Commissione UE in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto* (*biodiritto.org*), n. 3, 2021, pp. 415 et seq.; G. Proietti, *Intelligenza artificiale: una prima analisi della proposta di regolamento europeo*, in *dirittobancario.it*, may 2021. The general approach of the Council of the European Union on the proposal of 6 December 2022 has followed the initial text, which still constitutes the basis for preparations for negotiations with the European Parliament.

[10] Reference is made to the Proposal for a Directive on the adaptation of rules on non-contractual liability to artificial intelligence (AI Liability Directive) of 28 September 2022, COM (2022) 496 final. In this proposal, a general principle is formulated according to which liability for damages caused by AI systems should fall on humans, not only in cases where users have not been provided with sufficient information about the functioning of the AI system or in the presence of a defect in the AI system but also when the algorithm is so complex that the programmer cannot understand the reasons for its decisions. In this regard, see A. Longo, *Il robot che rompe paga. Stretta europea sui produttori*, in *la Repubblica*, 2 ottobre 2022, p. 28, and G. Ghidini, *Ma chi paga i danni. Se il robot combina guai?*, in *Corriere della Sera*, 13 febbraio 2023, p. 6. In particular, the proposal establishes a rebuttable presumption of causation between the defendant's fault and the output produced by the AI system or the failure to produce output by such system, even if the plaintiff has only demonstrated that the damage originated from the AI system. In legal doctrine, see the commentary by G. Proietti, *Sistemi di Intelligenza Artificiale e Responsabilità: la proposta di AI Liability Directive*, in *dirittobancario.it*, 6 ottobre 2022. Previously, there have been a series of proposals: the Resolution of the European Parliament of 16 February 2017 on civil law rules on robotics recommended granting full legal personality at least to the most sophisticated robots in order to allow for the application of equivalent compensation mechanisms for damage caused by their operation; the "White Paper on Artificial Intelligence - A European approach to excellence and trust" by the European Commission, COM (2020) 65 final, 16 February 2020, supported the need to adapt safety and liability

Even the European Parliament Resolution of February 16, 2017, on recommendations to the Commission concerning civil law rules on robotics (2015/2103(INL)), and the European Parliament Resolution of October 6, 2021, on artificial intelligence in criminal law and its use by police and judicial authorities in criminal matters (2020/2016(INI)), acknowledge the need for a regulatory framework focused on always asserting human responsibility[11].

With regard to the financial market, the application of AI systems has transformed the provision of certain services[12], such as high-frequency algorithmic trading, automated financial advice (robo-advice), and credit scoring[13].

As noted by some scholars, the adoption of artificial intelligence in the financial sector can provide benefits for investors. For example, it can lead to objectively more reliable investment recommendations or credit assessments. Against such benefits, it is necessary to consider the risks entailed. High-frequency algorithmic trading

regulations to the challenges posed by AI systems; the "Report on the implications of artificial intelligence, the Internet of Things and robotics on security and liability" by the European Commission, COM (2020) 64 final, 16 February 2020, expressly stated the requirement that the level of protection for victims of AI systems should not be lower than that provided to victims of traditional products, without compromising the development of technological innovation; finally, the Resolution of the European Parliament of 20 October 2020 on a civil liability regime for artificial intelligence (2020/2014(INL)) distinguished effects based on AI systems, providing for strict liability for high-risk AI systems with mandatory insurance, and presumed fault liability for low-risk AI systems. On the debate within the EU, with particular reference to the Commission's position, see U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, in *Riv. dir. civ.*, n. 6, 2020, pp. 1246 ss., spec. pp. 1249 ff.; A. Fusaro, *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo*, in *Nuova giur. civ. comm.*, n. 6, 2020, pp. 1344 et seq. For the Resolution of the European Parliament of 20 October 2020, see P. Serrao d'Aquino, *La responsabilità civile per l'uso di sistemi di intelligenza nella Risoluzione del Parlamento europeo del 20 ottobre 2020: "Raccomandazione alla Commissione sul regime di responsabilità civile e intelligenza artificiale"*, in *DPER online*, n. 1, 2021, pp. 248 et seq.

[11] Please refer to Recital Z of the Resolution of the European Parliament of 16 February 2017 on civil law rules on robotics (2015/2103(INL)), as well as to Recital J and point 13 of the Resolution of the European Parliament of 6 October 2021 on artificial intelligence in criminal law and its use by law enforcement and judicial authorities in criminal matters (2020/2016(INI)). Regarding the latter resolution, please consult G. Barone, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della Risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cass. pen.*, n. 3, 2022, pp. 1180 et seq., e A. Giannini, *Intelligenza artificiale, human oversight e responsabilità penale: prove d'impatto a livello europeo*, in *disCrimen* (*discrimen.it*), 21 novembre 2022, pp. 1, especially p. 12.

[12] When it comes to the implications of the digital revolution in the financial sector, reference is made to G. Alpa, *Fintech: un laboratorio per i giuristi*, in *Contr. impr.*, n. 2, 2019, pp. 377 et seq., and as for foreign sholarship R.P. Buckley – D.W. Arner – D.A. Zetzsche – E. Selga, *The Dark Side of Digital Financial Transformation: The new Risks of FinTech and the Rise of RegTech*, in *EBI* (*European Banking Institute*), *Working Paper Series*, n. 54, 2019, pp. 1 ff., T.C.W. Lin, *Artificial intelligence, finance, and the law*, in *Fordham Law Rev.*, Vol. 88, Issue 2, pp. 531 et seq. On the provision of digitized financial services G. Ruta, *I.A. nei reati economici e finanziari*, in Aa.Vv., *Intelligenza artificiale e giurisdizione penale*, Atti del Workshop della Fondazione Vittorio Occorsio, Università Mercatorum, Roma, 19 novembre 2021, pp. 58 et seq.

[13] It expressly indicates the specified services as fields of application of AI in the financial sector. M. Rabitti, *Intelligenza artificiale e finanza. La responsabilità civile tra rischio e colpa*, in *Riv. trim. dir. econ.* (fondazionecapriglione.luiss.it), Suppl. n. 2 al n. 3/2021, p. 300. In a broader sense, reference is made to A. Perrone, *Intelligenza artificiale e servizi di investimento*, in C. Costa – A. Mirone – R. Pennisi – P.M. Sanfilippo – R. Vigo (a cura di), *Studi di diritto commerciale per Vincenzo Di Cataldo*, Vol. II, Torino, 2021, pp. 711 et seq., e E. Mostacci, *L'intelligenza artificiale in ambito economico e finanziario*, in *DPCE online* (*dpceonline.it*), n. 1, 2022, pp. 361 et seq. Initially, the proposal for a EU Regulation on artificial intelligence, put forward by the European Commission in April 2021, classified only credit scoring systems as "high-risk" AI systems (Annex III, point 5, letter b) as they involve essential private services and may perpetuate discrimination based on race or ethnic origin, disability, age, or sexual orientation. The subsequent compromise text added, within sector number 5 concerning access to public services and essential private services and their use, to letter b), AI systems intended for insurance purposes, specifically systems for premium determination, underwriting, and claims assessment. However, given the flexible nature of the proposal, it is presumed and desirable that the scope of AI application in financial services can be expanded to include: a) *portfolio construction and rebalancing*, b) *roboadvice* and other forms of AI in advice, c) *trading*, d) *credit rating and risk management*, e) *ESG* (*rating provision, analyses by third-party providers to the benefits of ESG funds*, ...) f) *Shareholders voting process*.

can result in sudden and high volatility in securities prices (known as flash crashes)[14]. Automated financial advice can lead to a standardisation of investor behaviour instead of appropriate evaluation tailored to each individual's profile (known as herding effect)[15]. Credit scoring may lead to the exclusion of certain social groups from accessing credit[16].

It is in this context that the resilience of the regulatory framework on market abuse needs to be evaluated in light of the digitalization of finance and the operation of non-human agents in the markets. This evaluation is particularly urgent in the field of trading, where the use of AI systems is already widespread. However, scholars also highlight a similar need concerning the relationship between market abuse regulations and insider trading[17].

Both the European Union and national legal systems have established a dual sanctioning regime, with a tendency towards overlapping criminal and administrative offenses, aimed at ensuring fair and orderly transactions[18]. The prohibition of insider trading safeguards equal access to sensitive information and counters the illegitimate exploitation of privileged information[19]. The prohibition of market manipulation pro-

[14] A. Lupoi, *La negoziazione algoritmica ad alta frequenza e la struttura dei mercati: due casi negli Stati Uniti*, in *Riv. dir. comm. e dir. gen. obbl.*, n. 1, 2019, pp. 1 et seq.

[15] On the topic R. Ghetti, *Robo-advice: automazione e determinismo nei servizi di investimento ad alto valore aggiunto*, in *Banca borsa tit. cred.*, n. 4, 2020, pp. 540 et seq.; M.T. Paracampo, *Robo-advisor, consulenza finanziaria e profili regolamentari: quale soluzione per un fenomeno in fieri?*, in *Riv. trim. dir. econ.* (*fondazionecapriglione.luiss.it*), n. 4, Suppl. 1, 2016, pp. 256 et seq.; F. Sartori, *La consulenza finanziaria automatizzata: problematiche e prospettive*, in *Riv. trim. dir. econ.* (*fondazionecapriglione.luiss.it*), n. 3, 2018, pp. 253 et seq.

[16] Regarding the risks related to the application of algorithmic credit scoring systems, please refer to F. Mattassoglio, *La valutazione "innovativa" del merito creditizio del consumatore e le sfide per il regolatore*, in *Dir. banca*, n. 2, 2020, pp. 187 ss., e *G.L. Greco*, Credit scoring *5.0 tra* Artificial Intelligence Act *e Testo Unico Bancario*, in *Riv. trim. dir. econ.* (*fondazionecapriglione.luiss.it*), Suppl. n. 3, 2021, pp. 74 et seq., in part. pp. 93-95. For a study on the experience gained by Italian intermediaries in the adoption of credit scoring models, please refer to Aa.Vv., *Intelligenza artificiale nel credit scoring. Analisi di alcune esperienze nel sistema finanziario italiano*, in *Questioni di Economia e Finanza* (*Occasional Papers*), Banca d'Italia (bancaditalia.it), n. 721, ottobre 2022.

[17] See F. Annunziata, *Artificial intelligence and market abuse legislation. A European perspective*, Edward Elgar, 2023 (manuscript, currently being published, consulted with the kind permission of the author).

[18] Italian legislator, through Law No. 62 of April 18, 2005, implementing Directive EC/6/2003 (Market Abuse Directive, also known as MAD), introduced a dual cumulative system of criminal offenses (Articles 184 and 185 TUF) and administrative offenses (Articles 187-*bis* and 187-*ter* TUF).

[19] The legislation revolves around two main obligations: one of disclosure, as it requires listed companies to immediately communicate to the market all privileged information, they become aware of and that concerns them; and a prohibition on trading and selectively disclosing such privileged information to certain parties or providing investment advice. According to Article 7 of Regulation (EU) MAR, information is considered privileged when four elements are met: a) the information relates to one or more issuers (referred to as corporate information) or one or more financial instruments (referred to as market information), b) the information is not public, meaning it is not available to the general investors in the market, c) the information is "precise," and d) the information is price sensitive, meaning it is information that, if made public, «would be likely to have a significant effect on the prices of those financial instruments». In particular, information is considered precise if «if it indicates a set of circumstances which exists or which may reasonably be expected to come into existence, or an event which has occurred or which may reasonably be expected to occur» and ii) «where it is specific enough to enable a conclusion to be drawn as to the possible effect of that set of circumstances or event on the prices of the financial instruments». Furthermore, in the case of «a protracted process that is intended to bring about, or that results in, particular circumstances or a particular event, those future circumstances or that future event, and also the intermediate steps of that process which are connected with bringing about or resulting in those future circumstances or that future event, may be deemed to be precise information». Moreover, it is clarified in the same article that «(a)n intermediate step in a protracted process» can, in turn, constitute privileged

tects the integrity of trading by preventing the dissemination of false information, simulated behaviour, or other artifices put in place by those who can influence the price formation process of financial instruments. Criminal offenses (Articles 184 and 185 D.Lgs. no. 58 of 24 February 1998, TUF) aim to prevent and punish the most serious abusive conduct, only in cases of intent, while administrative offenses (Articles 187-*bis* and 187-*ter* TUF) cover less serious abusive conduct, including negligent actions, which are subject to monetary and restrictive measures[20].

The criminal regulation of insider trading, which is punishable by imprisonment and fines, primarily applies to "primary insiders." These include anyone who, by virtue of their position as a member of administrative, managerial, or supervisory bodies of the issuer, their capital participation in the issuer, or their employment, profession, public function, or office, or their involvement in criminal activities, possesses said privileged information:

«a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;

b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato effettuato ai sensi dell'articolo 11 del regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014;

c) raccomanda o induce altri, sulla base di tali informazioni, al compimento di taluna delle operazioni indicate nella lettera a)» (art. 184 TUF)»[21].

The offense also extends to the so-called "secondary insiders" meaning those who come into possession of privileged information through other circumstances, knowing or at least having the obligation to know that it is privileged information.

The criminal regulation on market manipulation provides for imprisonment and fines for anyone disseminating false information, engaging in simulated transactions,

information. Regarding price sensitivity, «information which, if it were made public, would be likely to have a significant effect on the prices of financial instruments (...) mean information a reasonable investor would be likely to use as part of the basis of his or her investment decisions». Determining the occurrence of insider trading is challenging and requires the use of presumptions that allow for the inference of the unknown fact (*factum probandum*) by deducing it from well-known facts, which are serious, precise, and consistent (indicators or sources of the presumption), following the canons of reasonable probability and rules of experience. On the evolution of the concept of privileged information, both in regulatory and jurisprudential contexts, refer to S. Seminara, *L'informazione privilegiata*, in M. Cera – G. Presti (a cura di), *Il testo unico finanziario*, cit., pp. 2124 et seq.

[20] The offense of market manipulation can be carried out through different types of conduct: the so-called "information-based manipulation" by spreading false news, and the so-called "tade-based manipulation" through the placement of orders or execution of transactions using a variety of strategies, some of which are provided as examples. These behaviours can undermine the transparency and fairness of financial transactions. If two or more of these conducts are committed, they will always result in a single legally relevant sanction, rather than multiple offenses.

[21] The English version of the provision is shown below: «a) buys, sells or carries out other transactions involving, directly or indirectly, for his own account or for the account of a third party, financial instruments using such information; b) discloses such information to others outside the normal exercise of his employment, profession, duties or position or a market sounding conducted pursuant to Article 11 of Regulation (EU) no. 596/2014 of the European Parliament and of the Council of 16 April 2014; c) recommends or induces others, on the basis of such information, to carry out any of the transactions referred to in letter a)».

or employing other actions capable of causing a significant alteration in the price of financial instruments (Article 185 TUF).

Directive 89/592/EEC of November 13, 1989 (Coordinating Regulations on insider trading) initially only prohibited insider trading. It was only with Directive EC/6/2003 (Market Abuse Directive, known as MAD I) that the offense of market manipulation was included within the scope of market abuse offenses, imposing on Member States the obligation to adopt administrative sanctions and leaving it up to national legislators to introduce criminal penalties for both offenses. Subsequently, the European legislator adopted two new regulatory instruments: Regulation (EU) 596/2014, Market Abuse Regulation (MAR), and Directive 2014/57/EU, Criminal Sanctions Market Abuse Directive (CSMAD), also known as Market Abuse Directive 2 or MAD II. With Regulation (EU) MAR, which applies as of July 2, 2016, the objective of maximum and immediate harmonization of the offenses under analysis was pursued. The scope of application was expanded, and the statutory and non-statutory limits of administrative sanctions were detailed. Directive MAD II introduced the obligation (rather than the option) for EU Member States to introduce criminal penalties.

The administrative offenses were subsequently requalified by the case law of the European Court of Human Rights (ECtHR) in the well-known *Grande Stevens* judgment. The judges in Strasbourg held that the administrative offenses of insider trading (Article 187-*bis* TUF) and market manipulation (Article 187-ter TUF) should be considered as essentially criminal offenses due to the severity of the penalties imposed (monetary, restrictive, and confiscatory)[22]. This decision was in line with the criteria established by the same case law in the *Engel* judgment[23].

[22] European Court of Human Rights, March 4, 2014, application no. 18640/2010, *Grande Stevens and Others v. Italy*. On this decision, see among others the comments by G.M. Flick – V. Napoleoni, *Cumulo tra sanzioni penali e amministrative: doppio binario o binario morto? "Materia penale", giusto processo e ne bis in idem nella sentenza della Corte Edu, 4 marzo 2014, sul market abuse*, in *Riv. AIC* (*rivistaaic.it*), n. 3, 2014, 11 luglio 2014, nonché in *Riv. soc.*, n. 5, 2014, pp. 953 ss.; F. Viganò, *Doppio binario sanzionatorio e* ne bis in idem*: verso una diretta applicazione dell'art. 50 della Carta?*, in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*), n. 3, 2014, pp. 219 et seq.; P. Montalenti, *Abusi di mercato e procedimento Consob: il caso Grande Stevens e la Sentenza CEDU*, in *Giur. comm.*, n. 3, 2015, pp. 478 et seq.; A. Genovese, *Il controllo del giudice sulla regolazione finanziaria*, in *Banca borsa tit. cred.*, n. 1, 2017, pp. 49 et seq.; M. Ventoruzzo, *Abusi di mercato sanzioni Consob e diritti umani: il caso Grande Stevens e altri c. Italia*, in *Riv. soc.*, n. 4, 2014, pp. 693 et seq.

[23] European Court of Human Rights, June 8, 1976, application no. 5100/71, *Engel and Others v. Netherlands*, established three criteria for the substantive criminalization of administrative sanctions: the legal classification of the offense under national law; the nature of the offense and the repressive purpose of the sanction; the punitive nature and severity of the sanction; the connection with a criminal violation. Following this judgment, the European Court of Human Rights, November 28, 1999, *Escobet v. Belgium*, held that «in any case, the notion of penalty contained in Article 7 of the Convention, like the notion of a criminal charge in Article 6, have an autonomous scope [...] the Court is not bound by the classifications of domestic law, which have relative value». The criteria developed in the Engel case were substantially endorsed by the EU Court of Justice, in its judgments of June 5, 2012, *Bonda*, C489/10, EU:C:2012:319, paragraph 37, and February 26, 2013, *Åkerberg Fransson*, C-617/10, EU:C:2013:105, paragraph 35.

This interpretation was eventually shared by the Court of Justice of the European Union (CJEU)[24] and the Constitutional Court. The latter recently ruled on the retroactivity of milder administrative sanctions[25] and the right to remain silent (the so-called *nemo tenetur se detegere* principle)[26] in formally administrative proceedings concerning market abuse[27].

Due to this requalification, a series of questions have been raised regarding the alleged violation of Article 6 of the European Convention on Human Rights (ECHR), concerning the right to a fair trial, Article 4 of Protocol 7 to the ECHR, regarding the violation of the principle of *ne bis in idem* (double jeopardy), Article 7 of the ECHR, which enshrines the principle of *favor rei* and the retroactivity of the milder law, as

[24] Respectively, with regard to the offense of market manipulation, provided for in Article 187-ter TUF, and the offense of insider trading, provided for in Article 187-bis TUF, the Court of Justice of the European Union, in its judgment of March 20, 2018, *Garlsson Real Estate SA v. Consob*, C-537/16, EU:C:2018:193, point 33, and its judgment of March 20, 2018, *Di Puma v. Consob*, C-596/16 and C-597/16, EU:C:2018:192, point 35, classifies the sanctions as being substantively criminal based on the nature of the offense and the severity of the sanction.

[25] Constitutional Court, judgment of March 21, 2019, No. 63, to which reference is made to the commentary by E. Bindi – A. Pisaneschi, *La retroattività* in mitius *delle sanzioni amministrative Consob*, in *Giur. comm.*, n. 5, 2019, pp. 1015 et seq.

[26] Constitutional Court, order of May 10, 2019, No. 117, to which reference is made to the comments by A. Logli, *Poteri istruttori della Consob e* nemo tenetur se detegere, in *Giur. comm.*, n. 2, 2020, pp. 230 et seq.; G. Caneschi, Nemo tenetur se detegere *anche nei procedimenti amministrativi sanzionatori? La parola alla Corte di giustizia*, in *Cass. pen.*, n. 2, 2020, pp. 579 et seq. In general, on the subject, reference is made to M. Allena – S. Vaccari, *Diritto al silenzio e autorità di vigilanza dei mercati finanziari*, in *Riv. dir. banc.* (*rivista.dirittobancario.it*), n. 3, 2022, pp. 689 et seq.

[27] Before these decisions, the substantially criminal nature of the proceedings and sanctions relating to market abuse was affirmed by the Constitutional Court, judgments of December 12, No. 223 and April 12, 2017, No. 68. Outside of this scope, the jurisprudence of the Court of Cassation (Cass., Sez. II, September 26, 2019, No. 24081 and No. 24082; Cass., Sez. II, August 6, 2019, No. 21017; Cass., Sez. II, April 5, 2017, No. 8855; Cass., Sez. I, March 2, 2016, No. 4114; Cass., Sez. I, June 30, 2016, No. 13433) and the Courts of Appeal do not recognize the substantially criminal nature of the administrative sanctions imposed by Consob, based on the circumstance that the Grande Stevens judgment solely concerned market abuse, even though the Constitutional Court itself (judgment of March 21, 2019, No. 63) expressly noted that "the idea that the interpreter cannot apply the ECHR except with reference to cases that have already been the subject of specific pronouncements by the Strasbourg Court must be rejected." Similarly, the jurisprudence of the Court of Cassation (Cass. civ., Sez. II, January 3, 2019, No. 4 and Cass. civ., Sez. II, September 28, 2016, No. 19219; Cass. civ., Sez. II, April 18, 2018, No. 9517; Cass. civ., Sez. II, January 11, 2017, No. 463; Cass. civ., Sez. II, August 4, 2016, No. 16313; Cass. civ., Sez. II, March 10, 2016, No. 4725; Cass. civ., Sez. II, December 14, 2015, No. 25141; Cass. civ., Sez. II, December 3, 2013, No. 27038; Cass. civ., Sez. Un., September 30, 2009, No. 20935 and No. 20939; Cass. civ., Sez. II, February 24, 2016, No. 3656) has ruled on all the offenses and proceedings falling under the competence of the Bank of Italy. On the other hand, the Council of State, which remains competent for the administrative sanctions imposed by IVASS, has qualified such sanctions as substantially criminal due to their punitive nature, based on the Engel criteria (Cons. Stato, Sez. VI, March 28, 2019, Nos. 2042 and 2043). This different interpretation is the consequence of the recognition of the jurisdiction vested in different judicial bodies for the sanctioning measures adopted by independent authorities following the interventions of the Constitutional Court, judgments of June 20, 2012, No. 162, and April 4, 2012, No. 94, which reassigned to the ordinary judge, namely the Court of Appeal, jurisdiction over the sanctions imposed by the Bank of Italy and Consob due to a lack of delegation in the Administrative Procedure Code, which had transferred all the sanctions of market regulatory authorities to the exclusive jurisdiction of the administrative judge. For an overview of the jurisprudence on the qualification of the sanctions of the Bank of Italy and Consob, reference is made to E. Bindi – P. Luccarelli – A. Pisaneschi, *Le sanzioni della Banca d'Italia e della Consob*, in *Giur. comm.*, n. 3, 2021, pp. 553 et seq., particularly pp. 555-559, and A. Pisaneschi, *Le sanzioni amministrative della Consob e della Banca d'Italia: gli indirizzi delle giurisdizioni sovranazionali e le problematiche applicative interne*, in *Riv trim. dir. econ.*, n. 2, 2020, Suppl., pp. 81 et seq., particularly pp. 83-86. In doctrine, there is support for extending the scope of the substantially criminal nature to the sanctions imposed by Consob and the Bank of Italy beyond the perimeter of market abuses (I. Sforza, Il nemo tenetur se detegere *nelle audizioni Consob e Banca d'Italia: uno statuto ancora da costruire*, in *Sistema penale* (*sistemapenale.it*), n. 2, 2022, pp. 83, particularly p. 95.)

well as Articles 47 and 48 of the EU Charter of Fundamental Rights for the violation of the right to remain silent[28].

The aforementioned *Grande Stevens* judgment, while highlighting the violation of the principle of due process in Consob's sanctioning procedure regarding market abuse[29], noted that the guarantees provided by Article 6 of the ECHR are nonetheless safeguarded by the provision of an opposition procedure before the Court of Appeals, on both factual and legal grounds, and by the review of legality before the Court of Cassation, limited to issues of legality, against the same sanctioning measures imposed by the supervisory authority. According to the ECtHR, the State is free to choose where to place the guarantees of a fair trial, whether in the administrative phase or the judicial phase, as it is a decision left to the discretion of national authorities[30].

Regarding the alleged violation of *ne bis in idem* (or double jeopardy), the judges in Strasbourg, in a sudden *revirement*, in the case of *A/B v. Norway*, admitted the conventionality of a dual essentially criminal sanction and multiple proceedings concerning the same offense, provided there is a "substantial and sufficiently close temporal connection" identifiable based on certain specific criteria[31].

[28] On all these issues, see, for example, C. Deodato, *Sanzioni formalmente amministrative e sostanzialmente penali: i problemi procedurali connessi all'applicazione delle sanzioni Consob in materia di materia di* market abuse *(e alcune soluzioni)*, in *federalismi.it*, n. 23, 2019, pp. 1 et seq.

[29] The violation referred to the previous Consob Sanctioning Procedure Regulation of December 19, 2013, No. 18750, to the extent that the procedure did not guarantee the respect of adequate adversarial proceedings, did not provide for a public hearing, and did not ensure the impartiality of the judging body. In particular, the procedure, as structured, conflicted with the principle of equality of arms between the prosecution and the defense, as it did not allow the interested party an opportunity to engage in dialogue regarding the Conclusive Report prior to the final determination by the Commission.

[30] After the Grande Stevens judgment of the European Court of Human Rights, the Council of State (judgments of March 26, 2016, No. 1595 and No. 1596) identified the incompatibility of the Consob sanctioning procedure with the principle of adversarial proceedings established by Article 195 TUF, as the Conclusive Report of the Administrative Sanctions Office "is not subject to communication (or other forms of knowledge) and there is no possibility of counter-deduction regarding it." However, these rulings did not find any conflict with the European Convention on Human Rights (ECHR) but only with the "reinforced" adversarial principles established by Article 187-*septies* TUF. In addition to these rulings by the administrative courts, decisions of the ordinary courts have also upheld the legitimacy of Consob's sanctioning procedure (Court of Appeal of Rome, decree of May 30, 2014; Court of Appeal of Rome, judgment of July 1, 2014; Court of Appeal of Bologna, judgment of March 3, 2015, No. 199). Consob has nevertheless amended the Sanctioning Procedure Regulation with Resolution No. 19521 of February 24, 2016, introducing the right of recipients of the charge letter, who have submitted written submissions or participated in the hearing, to receive the final report and submit their counter-deductions regarding the conclusions reached by the office within thirty days from its receipt.

[31] European Court of Human Rights, judgment of November 15, 2016, applications nos. 24130/11 and 29758/11, *A. and B. v. Norway*, established certain criteria for determining such a substantial and temporal connection. Regarding the former, the connection exists «*– whether the different proceedings pursue complementary purposes and thus address, not only in abstracto but also in concreto, different aspects of the social misconduct involved; – whether the duality of proceedings concerned is a foreseeable consequence, both in law and in practice, of the same impugned conduct ("in idem"); – whether the relevant sets of proceedings are conducted in such a manner as to avoid as far as possible any duplication in the collection and in the assessment of the evidence, notably through adequate interaction between the various competent authorities to ensure that the establishment of the facts in one set of proceedings is replicated in the other; – and, above all, whether the sanction imposed in the proceedings which become final first is taken into account in those which become final last, so as to prevent the situation where the individual concerned is in the end made to bear an excessive burden, this latter risk being least likely to be present where there is in place an offsetting mechanism designed to ensure that the overall quantum of any penalties imposed is proportionate*». With regard to the temporal connection, «*the two sets of proceedings have to be conducted simultaneously from beginning to end. [...] the connection in time must be sufficiently close to protect the individual from being subjected to uncertainty and delay and from proceedings becoming protracted over time*». For further commentary on the judgment, please refer to F. Viganò, *La Grande Camera della Corte di Strasburgo su* ne bis in idem *e doppio binario sanzionatorio*, in *Dir. pen. cont.*

The legitimacy of the dual sanctioning system, both criminal and administrative, has also been reaffirmed by EU case law, as EU Member States have been granted «freedom to choose the applicable penalties, which may take the form of administrative penalties, criminal penalties or a combination of the two»[32] as long as the overall cumulative sanctions respect the principle of proportionality[33]. In this regard, Article 187-*terdecies* TUF stipulates that the judicial or administrative authority pronouncing a second sanction for the same offense must take into account the measures already imposed when determining its own sanctions. This proportionality assessment may lead, as stated by the case law, to the total or partial non-application of the sanction that should be imposed last if the first one is commensurate with the gravity of the offense or to modulate the second sanction considering the first one[34].

This process of expanding conventional guarantees has concerned the principle of *favor rei* and the retroactivity of the milder law[35]. In the case of administrative

(*dirittopenalecontemporaneo.it*), 18 novembre 2016, e a A.F. Tripodi, *Corte europea dei diritti dell'uomo e sistemi sanzionatori in materia di abusi di mercato e di violazioni tributarie: la quiete dopo la tempesta*, in *Soc.*, n. 1, 2018, pp. 80 et seq.

[32] Court of Justice of the European Union, judgment of 20 March 2018, C-524/15, *Menci*, para. 47; Court of Justice of the European Union, judgment of 20 March 2018, C-537/16, *Garlsson Real Estate SA and others*, point 49; Court of Justice of the European Union, judgment of 20 March 2018, C-596/16 and C597/16, *Di Puma v. Consob*, point 26. For these three decisions, please refer to F. Consulich, *Il prisma del* ne bis in idem *nelle mani del Giudice eurounitario*, in *Dir. pen. proc.*, n. 7, 2018, pp. 949 et seq.

[33] Court of Justice of the European Union, judgment of 20 March 2018, C-537/16, *Garlsson Real Estate SA and others*, point 60, expressed doubts about the effectiveness of the principle of proportionality, considering the previous wording of Article 187-terdecies TUF, which seemed to refer only to the accumulation of pecuniary penalties and not to the accumulation of an administrative pecuniary penalty of a criminal nature and a custodial sentence.

[34] Court of Cassation, Criminal Division, Judgment of 15 April 2019, No. 3999. See C. Pagella, *L'inafferrabile concetto di "connessione sostanziale e temporale sufficientemente stretta": la Cassazione ancora sul* ne bis in idem *e* insider trading, in *Sistema penale* (*sistemapenale.it*), 9 gennaio 2020. The application of Article 187- *terdecies* TUF was made by the Court of Appeal of Milan, Section II, Judgment of 15 January 2019 (dep. 15 April 2019), No. 284, to which reference is made in the commentary by C. Pagella, *Riflessi applicative del principio di proporzione del trattamento sanzionatorio complessivamente irrogato per i fatti di market abuse e punibilità dell'insider di sé stesso: la Corte di Appello di Milano sul caso Cremonini*, in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*), 20 June 2019. However, such scrutiny of the overall sanctioning response may not be sufficient after the judgment of the Court of Justice of the European Union (CJEU), 6 June 2019, Application No. 47342/14, *Nodet v. France*, which - while explicitly extending the criteria of *A/B v. Norway* to market abuses - adheres to a restrictive interpretation of the criteria, which would concern not only the sanctioning level but also the right not to be subjected to two proceedings for the same offense, with a consequent evaluation of all parameters of the so-called «*close connection*» to exclude the violation of ne bis in idem. See the note by M. Scodetta, *Il* ne bis in idem *"preso sul serio": la Corte EDU sulla illegittimità del doppio binario francese in materia di abusi di mercato (e i possibili riflessi nell'ordinamento italiano)*, in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*), 17 giugno 2019. The issue of dual-track sanctions has recently been addressed by the Constitutional Court, Judgment of 16 June 2022, No. 149, concerning violations of copyright. The Court deemed well-founded the constitutional illegitimacy of Article 649 of the Code of Criminal Procedure insofar as it does not provide for the judge to pronounce acquittal or dismissal in relation to a defendant for an offense relating to copyright that has already been subjected to a sanctioning procedure, now concluded, for the same act. In this circumstance, the judges also issued a warning to the legislator to overcome the disharmony and reconsider comprehensively the dual-track sanctioning systems still in force. See the commentary by M. Scoletta, *Uno più uno anche a Roma può fare due: la illegittimità costituzionale del doppio binario sanzionatorio del doppio binario punitivo in materia di diritto d'autore*, in *Sistema penale* (*sistemapenale.it*), 23 giugno 2022.

[35] The foundation of the principle of retroactivity in favour of the milder law has received constitutional support in Article 3 of the Constitution: the principle of equality «impone, in linea di massima, di equiparare il trattamento sanzionatorio dei medesimi fatti, a prescindere dalla circostanza che siano stati commessi prima o dopo l'entrata in vigore della norma che ha disposto l'abolitio criminis o la modifica mitigatrice» (Constitutional Court, ruling on July 27, 2011, no. 236). Indeed, this principle became part of the national legal system with the decision of the ECHR (ruling on September 17, 2009, application no. 10249/03, *Scoppola v. Italy*), which, through the incorporation clause of Article

sanctions related to market abuse, these principles were enshrined by the Constitutional Court in ruling no. 63 of 2019, which declared Article 6, paragraph 2, of Legislative Decree no. 72 of 2015 unconstitutional to the extent that it excluded the retroactive application of a subsequent more favourable law. In this circumstance, the constitutional judges affirmed the application of principles developed in criminal matters when the act is no longer considered unlawful or when the assessment of its seriousness has changed within the legal system, except in cases where there are constitutional interests that require protection and justify the same level of scrutiny[36].

The latest development concerns the application of the right not to cooperate in one's one incrimination (the so-called *nemo tenetur se detegere principle*) and the defendant's right to silence in administrative proceedings related to market abuse before Consob. This issue has been the subject of a jurisprudential dialogue between the Constitutional Court[37] and the Court of Justice of the European Union[38], following a constitutional question raised by the Court of Cassation[39]. In particular, the Luxembourg judges, based on the consideration that the right to silence is guaranteed by Articles 47 and 48 of the EU Charter of Fundamental Rights, exclude the possibility of sanctioning a person in such circumstances. Sharing this initial premise and considering the punitive nature of administrative sanctions in cases of market abuse, the Constitutional Court declared the illegitimacy of Article 187-*quinquesdecies* TUF insofar as it penalizes those who refuse to answer questions posed by the Bank of Italy and Consob when exercising their right to silence. However, this principle is not considered absolute as the decision specifies that «il diritto al silenzio non giustifica comportamenti ostruzionistici che cagionino indebiti ritardi allo svolgimento dell'attività di vigilanza della CONSOB, come il rifiuto di presentarsi ad un'audizione prevista da tali autorità, ovvero manovre dilatorie miranti a rinviare lo svolgimento dell'audizione stessa. Né il diritto al silenzio potrebbe legittimare l'omessa consegna di dati, documenti, registrazioni preesistenti alla richiesta della CONSOB»[40].

117 of the Constitution, received a new foundation with the inclusion of Article 7 of the ECHR, while acknowledging that its nature is not absolute if the legislature identifies exceptions or limitations supported by a valid justification.

[36] Constitutional Court, judgment of March 21, 2019, no. 63. On this point, reference is made to the comments by P. Provenzano, *Illecito amministrativo e retroattività "*in bonam partem*": da eccezione alla regola a regola generale*, in *Banca borsa tit. cred.*, n. 1, 2020, pp. 52 et seq., e V. Tiganò, *L'estensione del principio costituzionale della retroattività favorevole in materia penale alle sanzioni amministrative punitive contro gli abusi di mercato*, in *ivi*, pp. 62 et seq.

[37] Constitutional Court, order on May 10, 2019, no. 117. Reference is made to the commentary by G. Fares, *Diritto al silenzio, soluzioni interpretative e controlimiti: la Corte costituzionale chiama in causa la Corte di giustizia*, in *dirittifondamentali.it*, n. 1, 2020, pp. 57 et seq.

[38] Court of Justice of the European Union, judgment of February 2, 2021, *DB v. Consob*, C-481/19, EU:C:2021:84. See the commentary by D. Coduti, *Il diritto al silenzio nell'intreccio tra diritto nazionale, sovranazionale e internazionale: il caso D.B. c. Consob*, in *federalismi.it*, n. 22, 2021, pp. 121 et seq.

[39] Court of Cassation, Civil Division, Section II, order of February 16, 2018, no. 3831, with commentary by G.L. Gatta, "Nemo tenetur se detegere" *e procedimento amministrativo davanti alla Consob per l'accertamento dell'abuso di informazioni privilegiate: la Cassazione solleva questione di legittimità costituzionale dell'art. 187-*quinquiesdecies *T.U.F.*, in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*), 27 aprile 2018.

[40] Constitutional Court, judgment of April 30, 2021, no. 84. M. Michetti, *Diritto al silenzio e* insider trading*: il confronto tra Roma e Lussemburgo prosegue sulla via del dialogo (Corte costituzionale, sentenza n. 84/2021)*, in *Consulta online* (*giurcost.org*), n. 3, 2021, pp. 758 et seq., e S. Catalano, *La vicenda decisa dalla sentenza n. 84 del 2021 della Corte costituzionale: un esempio di "buon dialogo" fra Corti*, in *Forum di Quad. cost.* (*forumcostituzionale.it*), n. 4, 2021, pp. 295 et seq.

The legislative framework in this matter, following the adoption of Regulation (EU) MAR and Directive (EU) MAD II, is therefore based on the possibility of establishing a dual track of criminal offenses and administrative offenses, allowing Member States to punish market abuse violations not only with criminal sanctions for the most serious conduct but also with administrative sanctions. This not only creates non-harmonized national regulations but, as noted, potential difficulties in coordination between the supervisory authority proceedings and judicial authority processes, raising the risk of violating the EU (Article 50 of the EU Charter of Fundamental Rights) and conventional (Article 7 of the ECHR) principles of *ne bis in idem*. With reference to the latter issue, European legislation mandates Member States to ensure that the imposition of criminal penalties for offenses under Directive (EU) MAD II and administrative sanctions under Regulation (EU) MAR does not violate the prohibition of double jeopardy for the same act (Recital 23 of Directive MAD II). This issue has been further amplified by the essentially criminal nature of administrative sanctions and the extension of fair trial principles to the procedure[41].

2 The distinction between "weak" AI and "strong" AI

Within the regulatory framework outlined above, artificial intelligence systems have long emerged as key players, raising multiple questions for regulators and interpreters of financial market law.

To approach the topic correctly, it is necessary to identify the phenomenon.

AI systems can be distinguished based on their different levels of interaction with humans[42]. In comparison to primitive AI systems (referred to as "weak" AI systems) whose outputs depend on pre-established instructions from manufacturers, programmers, or users, more advanced AI systems (referred to as "strong" AI systems) possess self-learning capabilities and generate autonomous and unpredictable outputs compared to the initial inputs provided by the manufacturer, programmer, or user[43]. Since

[41] Regarding some proposed solutions, under current legislation and *de iure condendo*, see C. Deodato, *op. cit.*, pp. 28 et seq.

[42] N. Abriani – G. Schneider, *Diritto delle imprese e intelligenza artificiale*, Bologna, 2021, pp. 21 et seq., distinguish artificial intelligence systems based on two different approaches. According to the first approach, different artificial intelligence systems are categorized based on different statistical mathematical models for information processing and machine learning (such as supervised learning, reinforcement learning, unsupervised learning, and deep learning). According to another approach, artificial intelligence systems are identified based on their ability to interact with human intelligence, leading to the distinction between assisted intelligence systems, augmented intelligence systems, amplified intelligence systems, and autonomous intelligence systems. The proposed EU regulation defines "artificial intelligence system" (AI system) as follows: «software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with». In Annex I, the following approaches are indicated: a) machine learning approaches, including supervised learning, unsupervised learning, and reinforcement learning, utilizing a wide range of methods, including deep learning; b) logic-based approaches and knowledge-based approaches, including knowledge representation, inductive programming (logic), knowledge bases, inference and deductive engines, reasoning (symbolic), and expert systems; c) statistical approaches, Bayesian estimation, search methods, and optimization. On the distinction between "augmented intelligence" and "artificial intelligence", see, most recently, F. Annunziata, *Artificial intelligence and market abuse legislation. A European perspective*, cit., pp. 133-141.

[43] The distinction between strong AI systems and weak AI systems is now widespread both in civil law doctrine and in criminal law doctrine, but for an initial exemplification, see P. Spera, voce *Intelligenza artificiale*, in G. Zaccari – P. Perri

the logical decision-making process followed by these strong AI systems is not inherently transparent and immediately decipherable, it is commonly referred to as a "black box"[44].

For strong AI systems, the issue of human control over their functioning and the results of data processing within the system becomes crucial.

The proposed Regulation (EU) on artificial intelligence defines the so-called "duty of human oversight" (Article 14)[45] but does not cover the entire chain of output production. Article 14, in fact, only pertains to the data collection stage and is not extended to their subsequent processing, precisely due to the difficulty of fully understanding the functioning and mechanisms that govern self-learning algorithms[46].

Furthermore, the same proposal for regulation does not provide protective mechanisms that allow victims of "erroneous" outputs to restore their violated legal positions[47]. It is true that the proposed regulation establishes a series of transparency

(a cura di), *Dizionario Legal Tech*, Milano, 2020, pp. 535 et seq., and F. Maggino – G. Cicerchia, *Algoritmi, etica e diritto*, in *Dir. inf.*, n. 6, 2019, p. 1165, but also more broadly see also G. Pasceri, *Intelligenza artificiale, algoritmo* e machine learning, Milano, 2021, pp. 18- 24.

[44] This expression was coined by F. Pasquale, *The black-box society: The secret algorithms that control money and information*, Cambridge-London, 2015. In a critical sense, reference is made to E. Pellecchia, *Profilazione e decisioni automatizzate al tempo della* black box society*: qualità dei dati e leggibilità dell'algoritmo nella cornice della* responsible research and innovation, in *Nuove leg. civ. comm.*, n. 5, 2018, pp. 1210 et seq.

[45] Article 14 of the proposed Regulation (EU) on Artificial Intelligence regulates human oversight, stating that «1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use. 2. Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular when such risks persist notwithstanding the application of other requirements set out in this Chapter. 3. Human oversight shall be ensured through either one or all of the following measures: (a) identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service; (b) identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user. 4. The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (a) fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible; (b) remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons; (c) be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available; (d) be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system; (e) be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure. 5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 shall be such as to ensure that, in addition, no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons».

[46] O. Pollicino – G. De Gregorio – F. Paolucci, *La proposta di Regolamento sull'intelligenza artificiale: verso una nuova governance europea*, in *Privacy & Data Protection Technology Cybersecurity*, n. 3, 2021.

[47] See *European Data Protection Board* (*EDPD*) – *European Data Protection Supervisory* (*EDPS*), *Parere congiunto 5/2021 sulla proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale)*, 18 giugno 2021, p. 22.

obligations that could mitigate the opacity of algorithmic output production processes[48]. However, the difficulty, even from a regulatory perspective, remains in applying well-established general principles of accountability, such as causality and culpability, to strong AI systems.

In practical terms, the autonomy of strong AI systems[49] significantly complicates establishing a causal link between the conduct, whether commissive or omissive, of a human agent and the occurrence of an illicit output. This is due to the opacity of the algorithms that drive AI systems and the barriers to their effective and widespread disclosure. Even if the process leading to a specific output is known and any operational design by a human agent is excluded, the illicit outcome as a sole consequence of AI system functioning could be classified as an intervening supervening causal factor (Article 41, paragraph 2, criminal code)[50]. The unpredictability of strong AI systems in theoretical terms makes it difficult to attribute liability for damages to manufacturers, programmers, or users, even on a negligent basis[51].

This perspective opens unresolved scenarios of irresponsibility, with the resulting prejudice to public interests, especially in the field of criminal law. Civil law, in fact, recognizes more flexible models of imputing responsibility, allowing for the connection of the concrete harmful event through the adaptation of objective forms of

[48] Transparency is one of the fundamental values promoted by the EU for the development, dissemination, and use of AI systems. Since the beginning of the political process for AI regulation, all official documents of the European Union institutions have promoted transparency as a guiding principle in the regulation of the use of AI systems. The proposal subjects high-risk and limited-risk AI systems to rules on generalized and selective transparency, respectively. Regarding high-risk systems, it provides that providers must ensure an "adequate" level of transparency, but it is not specified what should be understood as "adequate" (Article 13). Providers must also establish a framework for the governance and management of data for AI systems that use information databases, including the practices to be followed for training, validation, and testing of datasets (Article 10, paragraph 2), and criteria for relevance, representativeness, completeness, and accuracy of data (Article 10, paragraph 3). It is also established that AI systems must contain technical information before they are placed on the market, with the information being presented in a way that ensures the system's compliance with the regulation (Article 11) and allows for the automatic recording of all events once it is operational (Article 12). At the same time, these systems must be approved and registered by the supervisory authority before being placed on the market, and they must be designed and developed to ensure human supervision and monitoring during their use (Article 14). Providers must register AI systems in a database before placing them on the market (Article 60). The information processed in the database includes details about the AI system (provider, system purpose, type and expiration date of the conformity certificate, indication of the states where it has been placed on the market, put into service, or made available). The establishment of all these mechanisms could facilitate the probative determination of the causal link between the behaviour of the artificial agent and humans, which is often hindered by the difficulty of deciphering the black box and cryptographic codes. See in this sense U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, cit., p. 1247.

[49] B. Panattoni, *op. cit.*, p. 323, considers it preferable to refer to the concept of emergent behaviour rather than autonomy, to avoid attributing decision-making autonomy to AI systems that would be comparable to intentionality. Similarly, A. Amidei, *Intelligenza artificiale e product liability: sviluppi del diritto dell'Unione Europea*, in *Giur. it.*, n. 7, 2019, p. 1717.

[50] C. Piergallini, *Intelligenza artificiale: da 'mezzo' a 'autore' del reato?*, cit., p. 1758.

[51] Unpredictability, not only subjectively but also objectively, according to B. Panattoni, *op. cit.*, p. 344, e M.B. Magro, *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, in *Leg. pen.* (*legislazionepenale.eu*), 10 maggio 2020, pp. 5-6. Sulla difficoltà di muovere un rimprovero all'uomo in questi casi si veda altresì M. Bassini – L- Liguori – O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, pp. 333 et seq. In foreign literature on this phenomenon of "irreducible" artificial agents, i.e., agents that cannot be attributed to humans, reference is made to R. Abbott – A. Sarch, *Punishing Artificial Intelligence: Legal Fiction or Science Fiction*, in *UC Davis Law Rev.*, Vol. 53, 2019, pp. 323 et seq., especially pp. 330 et seq., which identify the characteristics (unpredictability, unexplainability, autonomy) and reasons (enforcement problems, practical irreducibility, legal irreducibility) for which a crime committed by an AI system cannot be attributed to a human.

imputation[52]. Conversely, criminal law does not provide similar criteria for objective imputation, thereby increasing the risk of creating an area of unpunishable offenses[53] (the so-called "responsibility gap"[54]).

3 *Machina delinquere non potest?*

AI systems, whether weak or strong, can be involved in the commission of a crime, either as tools used in the commission or as the actual perpetrators of the offense. This can be seen in various examples such as self-driving cars, robotic surgery, and chatbots spreading fake news[55].

[52] Regarding civil liability arising from damages caused by AI systems, reference is made to C. Leanza, *Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel Terzo Millennio*, in *Resp. civ. prev.*, n. 3, 2021, pp. 1011, especially pp. 1021-1024, who believes that the European derivative product liability regime (Directive 85/374/EEC) is applicable in the case of weak AI systems that have a defect, with liability attributed to the system's manufacturer regardless of the presence of subjective elements such as intent or negligence. This regime does not seem to apply to strong AI systems, which are autonomous and capable of making independent decisions beyond their original programming. For strong AI systems, the concept of "development risk" has been formulated, allowing for the application of the objective liability regime provided in Article 2050 of the Italian Civil Code regarding damage caused by dangerous activities. This encourages manufacturers and programmers to allocate adequate resources to minimize the system's dangerousness. U. Ruffolo, *Intelligenza artificiale, machine Learning, responsabilità da algoritmo*, cit., p. 1700, also suggests the possibility of applying another form of objective liability (Article 2051 of the Italian Civil Code, liability for damage caused by things under custody) to those who provide additional data and "train" the AI system, in addition to a similar liability regime under Article 2052 of the Italian Civil Code that governs damage caused by animals, even if they are lost or escaped. The application of consumer law provisions on liability for defective products, which implement Directive 85/374/EEC, is more challenging in the case of strong AI systems if the damage was caused by behaviour that was neither foreseeable nor avoidable. In this regard, Article 120, paragraph 2, of the Consumer Code is crucial as it excludes the liability of the producer when the defect did not exist at the time the product was placed on the market. This issue is highlighted by M. Ratti, *Riflessioni in materia di responsabilità civile e danno cagionato da dispositivo intelligente alla luce dell'attuale scenario normativo*, in *Contr. impr.*, n. 3, 2020, pp. 1190-1191, e A. Amidei, *Intelligenza artificiale e product liability: sviluppi del diritto dell'Unione Europea*, cit., pp. 1715 et seq., especially pp. 1719 et seq. The latter proposes the configuration of objective liability for the producer of the AI system, considering that the foreseeability of the defect may only be an element for evaluating the presence of the subjective element of fault. It also suggests extending liability to the programmer as the creator of the algorithm that guides and composes the AI system, thereby reducing the responsibility of the manufacturer. Finally, it recognizes that a crucial role in the system's functioning is played by the trainee who provides data to enable the AI system to form its learning and evolution processes. However, this activity is difficult to fit into the notion of a "product" and is more accurately characterized as a service performance, which precludes the application of EU legislation and the injured party's ability to seek compensation from the data provider. G. Finocchiaro, *Intelligenza artificiale e responsabilità*, in *Contr. impr.*, n. 2, 2020, p. 731, proposes the construction of «un modello di responsabilità che sia un sistema puro di allocazione del rischio, prescindendo dalla ricerca dell'errore e ripartendo i costi sui soggetti che sono parte dell'operazione economica, in modo collettivo, eventualmente prospettando la costituzione di un fondo ovvero la formulazione di meccanismi di assicurazione in capo ai soggetti che potrebbero essere chiamati a risarcire il danno». Similarly, Id., *Intelligenza artificiale e protezione dei dati personali*, in *Giur. it.*, n. 7, 2019, p. 1676.

[53] On this point, B. Panattoni, *op. cit.*, p. 325, emphasizes two critical issues arising from the potential attribution of legal personality to artificial agents. Firstly, this perspective would lead to a "growing anthropomorphism" towards artificial agents. Secondly, it fuels the risk of operators being absolved of responsibility. Similarly, C. Piergallini, *Intelligenza artificiale: da 'mezzo' a 'autore' del reato?*, cit., p. 1753, agrees with this view.

[54] In this sense A. Matthias, *The responsibility gap: Ascribing responsibility for the actions of learning automata*, in *Ethics Inf. Tech.*, n. 6, 2004, pp. 175 et seq.

[55] Regarding the ability of artificial intelligence to conceive and develop the typical elements of "new crimes," please refer to the considerations of M. Papa, Future crimes*: intelligenza artificiale e rinnovamento del diritto penale*, in *disCrimen* (*discrimen.it*). 4 marzo 2020, pp. 9 et seq.

In fact, the experimental use of semi-autonomous driving cars[56] has already led to traffic accidents[57] due malfunctioning of the algorithms that control these vehicles[58]. Similar situations have occurred in the healthcare field, where AI systems are widely used in both diagnosis and surgery to speed up decision-making and precision operations[59].

Other recent cases have demonstrated the dangers associated with AI-based voice assistants[60]. These mechanisms, also known as social bots, sometimes acquire information online and select responses to users based on computational criteria, occasionally perpetuating errors and prejudices prevalent in the social sphere[61].

[56] For some reflections in the civil field, reference is made to A. Davola – R. Pardolesi, *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?*, in *Danno resp.*, n. 5, 2017, pp. 616 et seq.; U. Ruffolo – E. Al Mureden, Autonomous vehicles *e responsabilità nel nostro sistema ed in quello statunitense*, in *Giur. it.*, n. 7, 2019, pp. 1704 et seq.; R. Lobianco, *Veicoli a guida autonoma e responsabilità civile: regime attuale e prospettive di riforma*, in *Resp. civ. prev.*, n. 3, 2020, pp. 724 ss. (Parte I), e n. 4, 2020, pp. 1080 et seq. (Parte II); and in penal field a A. Cappellini, *Profili penalistici delle* self-driving cars, in *Dir. pen. cont.* (*archiviodpc.dirittopenaleuomo.org*), n. 2, 2019, pp. 325 et seq.

[57] This is the case of the episode reported by R. Barlaam, Fatal Accident, Uber Suspends Autonomous Driving Tests, in *Il Sole 24 Ore*, March 20, 2018, p. 34. It chronologically refers to the third collision, which occurred in Tempe, Arizona (USA) on March 18, 2018, resulting in the death of a pedestrian rather than the driver. The first incident dates to January 20, 2016, in Handan, China, resulting in the driver's death. The second incident occurred in Williston, Arizona (USA) on May 7, 2016, when a Tesla Model S car collided with a white truck, failing to distinguish it against the bright sky, resulting in the destruction of the vehicle and the driver's death. A final incident took place in Mountain View, California (USA), causing the driver's death.

[58] According to a portion of the doctrine, the circulation of self-driving cars evokes utopian (and perhaps dystopian) scenarios, as envisioned by G. Comandé, *Intelligenza artificiale e responsabilità tra* liability *e* accountability. *Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi giur. econ.*, n. 1, 2019, p. 177. It also raises purely ethical questions, forcefully described as the "trolley problem" by Y. Hu, *Robot Criminals*, in *Univ. Mich. Journal of Law Reform*, Vol. 52, n. 2, 2019, p. 496, about self-driving cars, pondering the following question: «*where an autonomous vehicle must crash into either person(s) A or person(s) B. Into whom should it crash? A child or an old lady? A cyclist with helmet or one without helmet?*». However, these situations likely apply to both self-driving cars and humans since the urgency of driving does not always allow for the expression of the "right" decision (or one that is less morally condemnable), whether by an experienced driver or by the most highly trained autonomous car. In this regard, S. Nyholm – J. Smids, *The Ethics of Accident-Algorithms for Self-Driving Cars: an Applied Trolley Problem?*, in *Ethical Theory and Moral Practice*, n. 19, 2016, pp. 1287-1288.

[59] Refer to U. Ruffolo, *L'intelligenza artificiale in sanità: dispositivi medici, responsabilità e "potenziamento"*, in *Giur. it.*, n. 2, 2021, pp. 502 et seq., particularly pp. 502, 507, according to which one of the first sectors in which human activity will soon be supplanted by AI systems is radiology, as it is now more precise than humans in examining a large amount of information and processing a diagnosis, albeit not necessarily correct because the algorithm (besides being opaque, lacking transparency, and therefore not immediately verifiable) develops outputs based on mere statistical correlations rather than logical inference. However, the author hypothesizes responsibility on the part of the system programmer for not having foreseen internal mechanisms aimed at inhibiting any evolution involving harmful events. For applications and identification of certain limits of artificial intelligence in the healthcare field, see G. Pasceri, *Intelligenza artificiale, algoritmo e* machine learning, cit., pp. 45-50, and Z. Obermeyer – B. Powers – C. Vogeli – S. Mullainathan, *Dissecting racial bias in an algorithm used to menage the health of populations*, in *Science Magazine*, 25 october 2019, Vol. 366, Issue 6464, pp. 447 et seq., which reports the case of the utilization of an algorithm (United Health Group's Optum system) to identify patients with complex healthcare needs, resulting in discriminatory effects based on skin color and consequent overestimation of costs for the disadvantaged population.

[60] One can recall the case of Amazon's application, Alexa, which, in response to a challenge, prompted a ten-year-old girl to insert a halfway inserted phone charger into an electrical outlet and touch the opposite poles with a coin. After the incident, Amazon updated the software to prevent the repetition of similar dangerous challenges. See *Amazon nei guai, la sfida di Alexa alla bimba. «Inserisci una moneta nella presa elettrica»*, in *il Giornale*, December 29, 2021, p. 15. Another case involves the chatbot TAY (Thinking About You), which, just one day after its activation, was blocked for spreading racist, sexist, and xenophobic messages on digital communication platforms, amplifying the effects of the information the application had acquired on the network. On this episode, see L. Benfatto, *Microsoft blocca il* software Tay*: era diventato razzista e xenofobo*, in *Il Sole 24 ore Tecnologia*, 25 marzo 2016.

[61] In this sense the article *L'intelligence artificielle reproduit nos préjugés*, in *Le Monde*, April 18, 2017, pp. 1, 28, but also in legal literature A. Carcaterra, *Macchine autonome e decisione robotica*, in A. Carleo (a cura di), *Decisione robotica*,

As mentioned, the varying levels of autonomy in AI systems have implications for the issue of assigning responsibility. While existing legal rules can be applied to hold humans accountable for the actions of weak AI systems, it becomes more challenging to impute and allocate responsibility to the manufacturer, programmer, or user when it comes to strong AI systems.

3.1 AI systems trained for illicit purposes

It is established that the offense can be directly attributed to the human when artificial intelligence is used as a tool for its commission through a series of instructions[62] given by the person who, by imparting them, has caused the AI to commit the illegal act[63]. This can be observed in financial scams such as phishing emails or phone messages, carried out using software agents that mass-produce attempts to extract customers' access passwords, including those for internet banking.

It can be added that in the case of human involvement in the commission of a crime, the occurrence of a different event (yet still illegal) resulting from an unforeseen deviation of the artificial agent does not sever the causal link and attribution to the human. At most, it can be considered a mere *aberratio causae* that does not negate the imputability of the event to the human agent[64]. Similarly, if the unforeseen deviation of the algorithm does not lead to the commission of a crime, it does not exclude the possibility of attributing the attempted act to the human[65].

Algorithms trained to engage in illegal activities could also be used in the financial sector by traders who exploit the competitive advantage of computational speed compared to trading strategies based solely on human knowledge. No matter how sophisticated human knowledge may be it can never bridge the technological and informational gap of those utilizing AI systems[66].

Bologna, 2019, pp. 38 et seq., recall that this effect has been referred to by data scientists as 'GIGO', which stands for "*garbage in garbage out*".

[62] Reference is made to F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo* (*dirittopenaleuomo.org*), n. 10, 2019, particularly pp. 24 et seq., which mentions as illustrative cases of the use of artificial intelligence systems for the commission of crimes, the so-called online ticket scalping and abusive market manipulation behaviours.

[63] See A. Cappellini, *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale*, in *disCrimen* (*discrimen.it*), 27 marzo 2019, pp. 7-8.

[64] A. Cappellini, *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale*, cit., p. 8. Tuttavia, F. Consulich, *Il nastro di Mobius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca borsa tit. cred.*, n. 2, 2018, pp. 218-219, regarding algorithmic trading in the financial sector, it has been observed that in similar situations, there is a deficiency in the element of intent since there is not a complete and perfect overlap of the specific ways in which the actions performed by the algorithm are manifested.

[65] A. Cappellini, Machina delinquere non potest*? Brevi appunti su intelligenza artificiale e responsabilità penale*, cit., p. 8.

[66] See G. Ruta, *I.A. nei reati economici e finanziari*, cit. pp. 67-70, which provides a case study of three cases in English and American jurisdiction. In addition to the *Coscia* case discussed below, it mentions the case of *Da Vinci Invest Limited and Paul Axel Walter*, which, according to the author, represent an exemplary illustration of market abuse through the interaction of humans and machines, involving the adoption of a massive order mechanism typical of high-frequency trading.

3.2 AI systems as authors of the offense

The commission of the offense may not originate from a human intent but be the consequence of autonomous and unpredictable behaviours of the artificial agent (referring specifically to strong AI systems) when inhibitory mechanisms that identify non-passable behaviour thresholds have not been implemented[67].

A portion of the doctrine has proposed attributing (or recognizing) a legal status to these AI systems in order to establish liability for the offenses they commit[68],

[67] These are not covered by this scope, the offenses caused by a manufacturing, programming, training, or surveillance error or, more specifically, by an informational deficit or inadequate training. C. Piergallini, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato*, cit., p. 1752, distinguishes between «difetti di costruzione», «difetti di progettazione», «difetti di informazione» and «difetti da rischio di sviluppo». Each of these defects corresponds to a specific risk, but except for the development risk discussed below, as B. Panattoni, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, cit., p. 334, points out, it is not a risk inherent in the autonomous operation of AI systems but «di un rischio creato, attualizzato e gestito da quei soggetti che programmano, commercializzano o impiegano il sistema intelligente». C. Da Rold, *Quando gli algoritmi sbagliano spesso sono solo disinformati*, in *Il Sole 24 ore*, 18 settembre 2022, p. 14. discusses the need for informed datasets. In these situations, it should not lead to a reconsideration of existing legal categories but rather to promote some adaptation of the existing ones for new "products" with greater freedom of action than in the past. In particular, in the described cases, the event caused by the AI system could be attributed to negligence on the part of the manufacturer, programmer, trainer, or user. Obviously, the justification for reproach should be differently interpreted: presumably, in the case of poorly informed or poorly trained algorithms, such as when there has been a production or programming defect, an obligation of expertise may have been violated; in the case of uncontrolled AI systems, an obligation of surveillance and therefore diligence may have been violated. These are hypotheses in which it would be possible to reconstruct the reproach in terms of the negligent failure to prevent the event by the operator (i.e., the manufacturer, programmer, trainer, or user), subject to the definition of a criterion of expertise or required diligence commensurate with the risk according to sector-specific regulations. Thus, P. Troncone, *Il sistema dell'intelligenza artificiale nella trama grammaticale del diritto penale. Dalla responsabilità umana alla responsabilità delle macchine pensanti: un inatteso* return trip effect, in *Cass. pen.*, n. 9, 2022, pp. 3287 ss., spec. pp. 3301-3304, suggests that the attribution of illicit acts could be justified by the provision of Article 40, paragraph 2, of the Italian Penal Code. Consequently, omissive charges will assume greater relevance as the human agent will be indirectly involved in the decision-making process. All this will result in greater involvement and accountability of human agents in all phases of the AI system's life, as already outlined in the proposal for a Regulation on Artificial Intelligence (EU). With regard to high-risk AI systems, Chapter II of Title III of the proposed Regulation on Artificial Intelligence (EU) stipulates that, before being placed on the market, they must meet the following conditions: establish and implement a risk management system; establish a governance and data management system for AI systems that involve the use of data; prepare technical documentation before placing on the market or putting into service; design and develop systems by automatically recording events during their operation; design and develop systems to ensure adequate transparency, allowing users to interpret outputs and receive instructions for use; ensure supervision and monitoring during use to prevent and reduce risks to health, safety, and fundamental rights; ensure accuracy, robustness, and cybersecurity of systems to avoid errors, failures, or inconsistencies. These are obligations incumbent on the AI system provider, in addition to the following: establish a quality management system that guarantees compliance with the Regulation; subject the system to the conformity assessment procedure provided for in Article 43 before placing it on the market or putting it into service; prepare a declaration of conformity if the system is compliant and affix the CE marking; retain automatically generated logs; register the system in the EU database before placing it on the market. Similarly, users have obligations such as using and monitoring the system in accordance with the instructions for use provided by the supplier, organizing resources and activities to implement human oversight measures indicated by the supplier, informing the supplier or distributor in the event of a serious incident or malfunction, and ceasing to use the system, ensuring compliance with relevant regulatory obligations (e.g., CRD4 directive for credit institutions, GDPR Regulation in the case of information provided under Article 13).

[68] In this regard, G. Teubner, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi* (translated by P. Femia), Napoli, 2019, pp. 55-60, 70-78, e G.P. Cirillo, *I soggetti giuridici digitali*, in *Contr. impr.*, n. 2, 2020, pp. 580-581, posit the recognition of partial legal capacity, namely the capacity to act as a representative, as they make autonomous decisions and can therefore have consequences in terms of liability. In favour of recognizing electronic legal personality, U. Ruffolo, *La "personalità elettronica"*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, pp. 213 ss., and in common law literature, L.B. Solum, *Legal Personood for Artificial Intelligences*, in *North Carolina L. Rev.*, Vol. 70, n. 4, 1994, pp. 1231 et seq.

along with identifying the elements (*actus reus* and *mens rea*)[69] and reasons[70] for such imputability.

Even the earliest interventions by EU institutions (so far limited to soft law sources), such as the European Parliament Resolution of 16 February 2017 containing recommendations to the Commission on civil law rules on robotics (2015/2103(INL)), implicitly suggested establishing full legal subjectivity for strong AI systems with the specific purpose of creating a centre for imputing responsibility for damages caused by them[71]. However, it left two questions unresolved: (i) the difficulty of making a reproach judgment against "machines"[72], (ii) defining the methods of repair and punishment for the harm caused by the behaviours of artificial agents[73]. In fact, the perspective of considering AI as an autonomous centre of legal imputation has been widely criticized, not only by leading doctrine[74] but also by EU institutions. The European Economic and Social Committee, in its opinion on "Artificial Intelligence - The impact of

[69] With reference to this model of liability, see G. Hallevy, *The Basic Models of Criminal Liability of AI Systems and Outer Circles*, (June 11, 2019), available at SSRN: https://ssrn.com/abstract=3402527 or http://dx.doi.org/10.2139/ssrn.3402527, which draws an analogy between the capacity of AI systems and the capacity of legally incapacitated individuals (i.e., minors) who cannot be held criminally liable. In these cases, although the *actus reus* of a crime may be committed by an AI system, the necessary *mens rea* is still lacking for attributing responsibility to artificial intelligence, which is characterized as a «*mere instrument, even though it is a sophisticated instrument, and the originating actor (the perpetrator-by-another) is the real perpetrator as a principal of the first degree. That perpetrator-by-another is liable for the conduct of the innocent agent, and the perpetrator liability is determined on the basis of that conduct and the perpetrator-by-another own mental state*». A similar view is expressed by the same author in *The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control*, in *Akron Intellectual Property Journal*, Vol. 4, Issue 2, 2010, pp. 170 et seq. In two other scenarios, the author envisions the possibility of attributing liability to the AI system: in the first case, joint liability of both the human and AI system if the programmer or user can be held negligently liable; in the second case, exclusive liability of the AI system if the connection with the programmer or user is severed. For some objections to this approach, see R. Borsari, *Intelligenza artificiale e responsabilità penale: prime considerazioni*, in *Rivista di diritto dei media* (*medialaws.eu*), n. 3, 2019, pp. 267-268.

[70] Y. Hu, *Robot Criminals*, cit., *passim*, identifies a triple set of reasons to consider AI systems criminally responsible: first, the algorithm underlying the AI system possesses algorithms capable of making morally relevant decisions; second, the algorithm can communicate its decisions to humans; and finally, the algorithm is authorized to act without human supervision.

[71] Refer to section 59, letter f), of the European Parliament Resolution of 16 February 2017 containing recommendations to the Commission on civil law rules on robotics (citation), where among the possible legal solutions to be adopted in the future, it evaluates «creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently».

[72] On this point, reference is made to the critical remarks of M.B. Magro, *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, cit., pp. 9-10, where the difficulty of identifying the requirement of culpability is emphasized, as AI is unable to perceive and understand the unlawfulness of conduct. In the same sense, I. Salvadori, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, cit., pp. 98-99; C. Piergallini, *Intelligenza artificiale: da 'mezzo' a 'autore' del reato?*, cit., pp. 1745 et seq.; A. Cappellini, Machina delinquere non potest*? Brevi appunti su intelligenza artificiale e responsabilità penale*, cit., pp 14-15, e P. Severino, *Intelligenza artificiale e diritto penale*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., p. 535., all stress the difficulty in attributing criminal responsibility due to the AI's lack of moral capacity. In Anglo-Saxon literature, P.M. Asaro, *A Body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics*, in P. Lin – K. Abney – G. Bekey (eds.), *Robot Ethics: The Ethical and Social Implications of Robotics*, Cambridge, 2012, pp. 169 et seq., particularly p. 181, excludes the application of criminal responsibility as artificial agents are not endowed with moral capabilities.

[73] As U. Ruffolo, *Intelligenza artificiale,* machine learning, *responsabilità da algoritmo*, cit., pp. 1702-1703, argues it is not necessary to attribute legal personality to AI for it to be responsible and have financial resources to compensate for damages.

[74] In legal doctrine, it is believed that technological advancement has not reached a stage where legal status can be granted to AI systems. In this sense, E. Palmerini, *Soggettività e agenti artificiali: una soluzione in cerca di un problema*,

artificial intelligence on the single (digital) market, production, consumption, employment, and society" (2017/C 288/01) of 22 September 2016, stated that attributing legal personality to robots "would involve an unacceptable risk of moral hazard" as it would eliminate the preventive function inherent in the liability regime[75]. The Expert Group on Artificial Intelligence established by the European Commission in June 2018, in the Report on Liability for Artificial Intelligence and other emerging digital technologies, reiterated that "there is currently no need to give legal personality to emerging digital technologies. Harm caused by even fully autonomous technologies is generally reducible to risks attributable to natural persons or existing categories of legal persons, and where this is not the case, new laws directed at individuals are a better response than creating a new category of legal person"[76]. Similarly, the European Parliament in a subsequent Resolution of 20 October 2020 deemed it unnecessary to confer legal personality on AI systems since there is always a human contribution in all activities[77]. Furthermore, a criminal sanction against AI systems would not be able to fulfil any of the functions recognized for punishment, namely retribution, rehabilitation, and prevention. Firstly, the sanction would not serve any retributive function since no reproach can be made against AI systems: artificial intelligence lacks free will[78]. Secondly, the rehabilitative purpose could not be achieved: the hypothetical provision of destroying or deactivating the AI system would ultimately fall on the owner or user[79], not to men-

in *Oss. dir. civ. comm.*, n. 2, 2020, pp. 445 et seq. Similarly, G. Bevivino, *Situazioni giuridiche "soggettive" e forme di tutela delle intelligenze artificiali*, in *Nuova giur. civ. comm.*, n. 4, 2022, pp. 899 et seq., specifically p. 907, agrees substantively but does not exclude the possibility of regulating forms of direct responsibility in the future if AI systems achieve functioning mechanisms entirely comparable to those of humans. On the contrary, S. Riondato, *Robotica e diritto penale (robot, ibridi, chimere, "animali tecnologici")*, in D. Provolo – S. Riondato – F. Yenisey, *Genetics, robotics, law punishment*, Padova, 2014, pp. 605-606, opposes the creation of AI systems and believes that there may be a prohibition within the legal system against creating AI systems with human-like capabilities. The regulatory provision is identified in Article 13 of Law No. 40 of 2004, which prohibits the production of hybrids and chimeras, considered by the author to also encompass "humanized robots." Furthermore, if the analysis is extended to the realm of civil liability, U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, cit., pp. 1250-1251, critically argues that the perspective of legal personality, linked to the creation of assets or an insurance fund, would only serve as a means to attribute responsibility to a plurality of entrepreneurs and users. Also, refer to E. Bocchini, *Contro la "soggettivizzazione" dell'intelligenza artificiale*, in *Il Nuovo Dir. Soc.*, n. 2, 2023, pp. 195 et seq., for a critical perspective on the "subjectification" of artificial intelligence.

[75] Opinion of the European Economic and Social Committee on «Artificial intelligence — The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society», (2017/C 288/01), 22 settembre 2016. In this sense L. Coppini, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Pol. dir.*, n. 4, 2018, p. 730.

[76] Expert Group on Liability and New Technologies, *Report on Liability for Artificial Intelligence and other emerging digital technologies*, European Commission, 2019, p. 38.

[77] See § 7 of the Resolution of the European Parliament of 20 October 2020, containing recommendations to the Commission on a civil liability framework for artificial intelligence.

[78] In this sense A. Cappellini, Machina delinquere non potest*? Brevi appunti su intelligenza artificiale* e *responsabilità penale*, cit., pp. 15-16, e C. Piergallini, *Intelligenza artificiale: da 'mezzo' a 'autore' del reato?*, cit., pp. 1767-1768. Regarding the ability of algorithms to influence human decisions, please refer to M. Abriani, *Gli algoritmi minacciano il libero arbitrio?*, in *MichePost*, 16 maggio 2020, whilst on the need for an ethical predisposition of algorithms see A. Celotto, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi giur. econ.*, n. 1, 2019, p. 59, and R. Trezza, *Intelligenza artificiale e persona umana: la multiforme natura degli algoritmi e la necessità di un "vaglio di meritevolezza" per i sistemi intelligenti*, in *Ratio Iuris* (*ratioiuris.it*), 19 maggio 2022.

[79] In this sense M.B. Magro, *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, cit., p. 8, and B. Panattoni, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, cit., p. 348.

tion that both "penalties" could be circumvented through reprogramming of the “machine”[80]. Finally, the sanction would not be capable of communicating the social disvalue of the unlawful behaviour to other AI systems as they are insensitive to criminal precepts because they are artificial and, as such, correctable through mere reprogramming[81].

Another doctrinal orientation, on the other hand, suggests attributing the offense still to humans, marginalizing the subjective dimension of guilt and extending the boundaries of predictability and avoidability of the event in order to configure an almost "objective" model of responsibility, reconstructed on the basis of abstract predictability coinciding with assuming a risk, even in the absence of a violation of conduct rules by any of the operators involved in the production and programming process, which is to say only for deliberately putting into operation an AI system with unpredictable behaviour[82]. There is no doubt that this latter reconstruction contradicts the established principle of personal imputation of criminal responsibility. However, it has the merit of incentivising a cautious attitude on the part of producers, programmers, and users, perhaps at the expense of the unlimited technological evolution of AI.

Finally, there is a third scenario, as problematic as the previous two: accepting a "normal" risk in the use of AI systems, comparable to environmental risk or *force majeure* (Articles 45-46 of the Criminal Code), as an imponderable but distributed and shared risk throughout the community[83]. On closer inspection, this is the conscious acceptance of the responsibility gap, from the perspective of a comparative evaluation of benefits and costs that prioritises technological development and downplays the individual's protection needs, with certain limited prohibitions for cases involving completely unacceptable risks[84].

[80] See V.C. Talamo, *Sistemi di intelligenza artificiale: quali scenari in sede di accertamento della responsabilità penale?*, in *ilPenalista*, 3 luglio 2020, pp. 5-6, which excludes the possibility of establishing criminal liability for artificial agents, not only due to the lack of the culpability requirement but also because of the impossibility of any rehabilitative and social reintegration function of the punishment. F. Basile, *Diritto penale e intelligenza artificiale*, cit., pp. 73-74, takes a more optimistic view on the achievement of the functions of punishment, specifically retributive and special preventive aspects, while expressing doubts about a general preventive effect on artificial "entities."

[81] A. Cappellini, Machina delinquere non potest*? Brevi appunti su intelligenza artificiale e responsabilità penale*, cit., pp. 15-16, e C. Piergallini, *Intelligenza artificiale: da ‘mezzo’ a ‘autore’ del reato?*, cit., pp. 1767-1768.

[82] M.B. Magro, *Decisione umana e decisione robotica. Un’ipotesi di responsabilità da procreazione robotica*, cit., pp. 19-20.

[83] M.B. Magro, *Robot, cyborg e intelligenze artificiali*, in A. Cadoppi – S. Canestrari – A. Manna – M. Papa, *Cybercrime*, Torino, 2019, pp. 1180 et seq., specifically p. 1211, outlines this scenario in the criminal context. However, it also opens the door to hypotheses of strict liability in civil responsibility cases where there is no fault on the part of the operator, programmer, or seller.

[84] In this regard, the proposal for a Regulation (EU) on Artificial Intelligence already identifies certain unacceptable practices of artificial intelligence. Specifically, Article 5(1) of the proposal for a Regulation (EU) on Artificial Intelligence prohibits the following practices of artificial intelligence: AI systems that use subliminal techniques (letter a); AI systems that exploit the vulnerabilities of certain individuals (letter b); AI systems used to evaluate the trustworthiness of individuals (letter c); AI systems for real-time biometric identification in publicly accessible spaces (letter d). Article 71 of the proposal for a Regulation (EU) establishes administrative fines of up to €30,000,000 or, if the offender is a company, up to 6% of the total worldwide annual turnover of the previous financial year for non-compliance with the prohibition of illicit practices. The same sanctions are also provided for the violation of rules on data and data governance of high-risk AI systems.

4 Trading, market abuse and AI: an overview

The use of AI systems allows for the acquisition and processing of a large amount of information and the development of new market strategies in a matter of milliseconds. This is due to two main characteristics of certain trading algorithms: statistical arbitrage and latency arbitrage. Economic analysis has highlighted how arbitrage plays a central role in market functioning: on the one hand, it enables operators who know how to implement it to gain (almost) risk-free profits, and on the other hand, it benefits the community of investors by ensuring prices remain consistent with the publicly available information.

All the forms of trading based on algorithms, including algorithmic trading and high-frequency trading, open up new vulnerabilities and unprecedented scenarios for market abuse[85]. The widespread risk becomes evident when considering the assets that the regulatory framework intends to safeguard through a comprehensive sanctioning system that should be updated with measures proportional to these forms of trading.

The various theories justifying the introduction of market abuse prohibitions are driven by the goal of ensuring the proper and orderly functioning of trading venues. By prohibiting insider trading, for instance, the legal system aims to prevent the risk that counterparties enter contracts based on non-public information[86], thereby discouraging market makers from reducing the bid-ask spread, i.e., transaction costs for

[85] In this sense M. De Felice, *Decisione robotica negoziale. Nuovi «punti di presa» sul futuro*, in A. Carleo, *Decisione robotica*, Bologna, 2019, p. 192, e C. Mottura, *Decisione robotica negoziale e mercati finanziari*, in *ivi*, pp. 265 et seq., especially pp. 265 and 271.

[86] In traditional economic analysis, market makers play a crucial role in the functioning of markets as they are the intermediaries who provide liquidity to other market participants through continuous proposals both on the buy side (bid) and the sell side (ask) for a given financial instrument. Typically, the expected profits of market makers increase with the frequency of trades, which allows each of them to reduce the difference between the best bid and the best ask. Competition among market makers for the same financial instrument leads, other things being equal, to a reduction in the overall best bid offered by all market makers (bid-ask spread). This benefits other market participants who view the bid-ask spread as the transaction cost they must incur to make their investments. Therefore, economic analysis pays close attention to policy choices and market operating rules that favour the reduction of the bid-ask spread by market makers. In particular, the role played by market makers in the price formation process or price discovery is examined, which allows prices to incorporate and reflect the information implicitly provided by market participants through their buy and sell orders. When it comes to the question of whether it is good to introduce a ban on insider trading, economists have provided conflicting answers based on different theories. The most important theory that opposes the introduction of the ban relies on the informational efficiency of markets, namely the extent to which prices are able to represent the underlying value of an asset, i.e., its intrinsic or fundamental value. In particular, the classic categorisation proposed by Nobel laureate Eugene Fama distinguishes between weak, semi-strong, and strong informational efficiency, depending on whether prices can incorporate and express information that could alternatively be derived from knowledge of past prices, all publicly available information, or all unpublished (i.e., private) information, respectively. It is evident that if insider trading is prohibited in a market because insiders, by definition, possess private information, then prices in such a market could never achieve strong efficiency, at most semi-strong efficiency. It is further argued that the informational efficiency of markets is also linked to the allocative efficiency of resources. The more prices can express the fundamental values of financial instruments, the easier it will be for the "invisible hand" theorized by Adam Smith to physiologically direct the resources of an economy towards the investments that are most deserving. On the other hand, various theories on market microstructure have shown that market makers are significantly harmed by the presence of insiders in the market. If a market maker provides liquidity to an insider who is aware of privileged information about to be published, the market maker that fails to close the position opened to provide liquidity to the insider before the information is published will suffer a loss at the moment of publication equal to the difference between the new market price and the price at which liquidity was offered to the insider. Being aware of this risk, market makers widen the bid-ask spread, imposing a higher transaction cost on other market participants to compensate for the losses resulting from this potential adverse event. Moreover, since market

the majority of investors, and dissuading institutional investors from taking positions contrary to prevailing trends that are not consistent with the publicly available information set[87].

This approach contradicts the viewpoint of a portion of the doctrine that argues that the indiscriminate use of insider information allows prices in the markets to converge more rapidly toward fundamentals. In various legal systems, the slowdown in the price discovery process resulting from the prohibition of abuse goes side by side with the introduction of disclosure obligations for issuers. It is worth noting how within the EU, obligations for issuers start from the moment information becomes privileged, i.e., when it is ready to be exploited profitably by insiders (Article 17(1) of Regulation (EU) MAR).

Similarly, through the prohibition of market manipulation, the legal system aims to prevent false or misleading information from not only slowing down the convergence process towards fundamentals but even preventing it[88]. Therefore, the dissemination of false information by those who have the ability, through their statements

makers cannot identify the financial instruments and periods in which insiders may appear as counterparties, they systematically widen the bid-ask spread. Consequently, it should also be noted that wider bid-ask spreads drive away those participants who, at the margin, cannot bear such transaction costs, thereby reducing the frequency of trades and, consequently, both the expected profits of market makers and the informational efficiency of prices, which can no longer incorporate the information provided by these participants through their market orders. On the informational efficiency of markets, see E. Fama, *Efficient Capital Markets: A Review of Theory and Empirical Work*, in *Journal of Finance*, 1970; S. Grossman – J. Stiglitz, *Information and competitive price system*, in *American Economic Review*, 1976; AS. Kyle, *Continuous auctions and insider trading*, in *Econometrica*, 1985; AS. Kyle, *Informed speculation with imperfect competition*, in *Review of Economic Studies*, 1989. For major models examining the influence of insider activity on price formation, see F. De Jong – B. Rindi, *The microstructure of financial markets*, Cambridge University Press, 2009; T. Foucalt – M. Pagano – A. Röell, *Market liquidity: theory, evidence, and policy*, Oxford University Press, USA, 2013. On other theories for or against the introduction of a ban on insider trading, see U. Bhattacharya, *Insider trading controversies: A literature review*, in *Annu. Rev. Financ. Econ.* Vol. 6, n. 1, 2014, pp. 385-403; S.M. Bainbridge, *An overview of insider trading law and policy: An introduction to the insider trading research handbook*, in *Research Handbook on Insider Trading, Stephen Bainbridge*, Edward Elgar Publishing Ltd, 2013, pp. 12-15; HG. Manne, *Insider trading and the stock market*. New York Free Press, 1966; HG. Manne, *Insider trading, virtual markets, and the dog that did not bark*, in *J. Corp. Law*, 2005; M. King – A. Roell – J. Kay – C. Wyplosz, *Insider trading*, in *Econ. Pol.*, 1988. On empirical evidence, see : U. Bhattacharya – D. Hazem, *The world price of insider trading*, in *The journal of Finance*, Vol. 57, n. 1, 2002, pp. 75-108; H.B. Christensen – H. Luzi – L. Christian, *Capital-market effects of securities regulation: Prior conditions, implementation, and enforcement*, in *The Review of Financial Studies*, 29.11.2016, pp. 2885-2924; R. Levine - L. Chen – W. Lai, *Insider trading and innovation*, in *The Journal of Law and Economics*, Vol. 60, n. 4, 2017, pp. 749-800.

[87] If, indeed, insiders move prices in advance from their value consistent with the set of publicly available information, as detectable from studies produced by rating agencies and financial analysts, then institutional investors (pension funds, hedge funds, etc.) might be induced to take significant positions that aim at aligning current prices with those consistent with the set of publicly available information. However, when privileged information is made public, such investors are surprised and suffer losses they would not have otherwise incurred. Anticipating this adverse scenario, institutional investors would not be incentivized to demand sophisticated research from financial analysts on the value of prices consistent with the set of publicly available information. As a cascading effect, the reduction in demand leads to less research production and therefore greater price volatility, resulting in less efficiency: M.J. Fishman – K.M. Hagerty, *Insider Trading and the Efficiency of Stock Prices*, in *The Rand Journal of Economics*, Vol. 23, No. 1, Spring1992, pp. 106-122.

[88] The imminent danger of high-frequency trading has been recognized by the EU legislator. Recital 38 of MAR states that "to reflect the fact that the trading of financial instruments is increasingly automated, it is desirable that the definition of market manipulation provides examples of specific abusive strategies that can be carried out with any available trading tool, including algorithmic and high-frequency trading. The examples provided are not exhaustive and do not imply that the same strategies implemented by other means are not abusive." For a description of the most common abusive practices following the spread of high frequency trading, reference is made to V. Caivano – S. Ciccarelli – G. Di Stefano – M. Fratini – G. Gasparri – M. Giliberti – N. Linciano – I. Tarola, *Il Trading ad alta frequenza*, in

or omissions, to influence market prices is sanctioned. As market prices are not only the result of the interaction between supply and demand but also represent information that is read, examined, and evaluated by various types of market participants, the placing of orders or the execution of transactions that alter the price formation process and deviate it from fundamentals, thus creating artificial prices or a distorted information framework, is equally penalized.

In fact, the use of AI systems in financial trading has made supervision more complex, not only in terms of identifying software[89] that drives market dynamics but also in evaluating its behaviour in terms of identifying underlying motivations and determining their legality or illegality and assigning corresponding responsibilities[90]. This is because AI solutions facilitate the conception of new behaviours that affect the interaction between supply and demand and the value of financial instruments.

Artificial intelligence, when applied to financial transactions, has a "disruptive" impact[91], *à la* Schumpeter's, and this study aims to understand to what extent current instances of insider trading and market manipulation can contain the new and different abusive manifestations of the phenomenon[92]. The risk of lagging behind, as often happens, is linked to the difficulty of the "legal" order of the market[93] progressively aligning with its "economic" evolution[94], with the establishment of more innovative "prohibitive", "attributive" and "conformative" rules in compliance with constitutional principles in economic matters. Without these rules, the risks to the stability and integrity of financial markets increase[95].

Discussion papers CONSOB (consob.it), n. 5, 2012; A. Puorro, *High Frequency Trading: una panoramica*, in *Questioni di economia e Finanza* (*Occasional Paper*), Banca d'Italia (bancaditalia.it), n. 198, settembre 2013.

[89] On the opportunity to use artificial intelligence mechanisms to detect the dissemination of insider information to the market by listed issuers, see F. Annunziata, *Intelligenza artificiale e comunicazione al mercato di informazioni privilegiate*, in L. Boggio (a cura di), *Intelligenza artificiale e diritto dell'impresa*, *Giur. it.*, n. 8-9, 2022, pp. 2031 et seq., especially p. 2033, which identifies its basis in the new provision of common law in Article 2086 of the Italian Civil Code, where is used a broad and flexible formulation of «assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa».

[90] In this sense F. Di Ciommo, Smart contract *e (non-) diritto. Il caso dei mercati finanziari*, in *Nuovo diritto civile*, n. 1, 2019, pp. 283-284.

[91] In general, regarding the effects of artificial intelligence on legal regulation, see G. Mobilio, *L'intelligenza artificiale e i rischi di una "*disruption*" della regolamentazione giuridica*, in *BioLaw Journal – Rivista di BioDiritto* (*biodiritto.org*), n. 2, 2020, pp. 401 et seq.

[92] For a description of the new forms of market manipulation through algorithms (particularly algorithmic trading and high-frequency trading), see below. In scholarly literature, the main manipulative schemes of spoofing, pinging, and mass-information are outlined. T.C.W. Lin, *The new market manipulation*, in *Emory Law Journal*, Vol. 66, Issue 6, pp. 1252 et seq.

[93] This expression refers to N. Irti, *L'ordine giuridico del mercato*, Roma-Bari, 2003, *passim*, especially pp. 51-54, which analyzes the shaping function of the law through "prohibitive" norms, i.e., norms that establish prohibitions, "attributive" norms, i.e., norms that confer positions on subjects and goods, and "conformative" norms, i.e., norms that regulate transactions and give their own shape to the market.

[94] On a similar line of reasoning, P. Lucantoni, *Mercato dei capitali, pandemia e informazione al mercato: il dibattito sull'evoluzione della disciplina degli abusi di mercato*, in *Banca borsa tit. cred.*, n. 4, 2022, pp. 549 et seq., about the implications on the legal rationality of the market arising from the pandemic and investment choices related to the phenomenon of so-called "gamification".

[95] In this sense A. Azzutti – W.G. Ring – H. S. Stiehl, *The Regulation of AI trading from an AI Life Cycle Perspective*, in *EBI Working Paper Series* (*ebi-europa.eu*), n. 130, 2022, *passim.*

Indeed, the spread of AI systems is more evident in trading than in the formation and circulation of insider information.

First, in legal doctrine, as well as in economic and financial literature, the effect of algorithmic traders on market quality measures is debated[96]. There is no doubt that each algorithmic transaction constitutes information, just like any other market transaction. However, it is debated in legal doctrine whether they promote a better understanding of transactions overall[97]. From the debate, it seems, in short, that the effect is positive on liquidity and informational efficiency, while there remains doubt regarding volatility and resilience during stress or crash phases[98].

In the EU, the initial attempts at regulation, on the preventive side, concern algorithms that exploit latency speed to limit the commission of abusive conduct. Article 17 of Directive 2014/65/EU (Markets in Financial Instruments Directive, known as MiFID II) establishes that investment firms exercise «effective and adequate system and risk controls» and «prevent the sending of erroneous orders or the functioning of systems that create disorder or contribute to it». Article 48 of MiFID II provides for the introduction of so-called circuit breakers in trading venues to temporarily halt or restrict trading if sudden and unexpected price movements occur[99]. Furthermore, on the enforcement side, the practices of market manipulation have been further defined to ensure more effective protection for the formation of financial instrument prices (see Chapter II, paragraph 2).

The application of AI systems to trading tends to break the connection between financial transactions and individuals[100], exacerbated by the speed of order execution, which makes it impractical to correct the algorithms used[101]. However, even once the causal link between human input and algorithmic output is identified, market abuse offenses require, in terms of criminal liability, an indispensable subjective element that can only be discerned when the algorithm is used as a tool for committing

[96] On this dispute, M. Bertani, Trading *algoritmico ad alta frequenza e tutela dello* slow trader, cit., pp. 274-275, adds that the utilization of these latency advantage-exploiting mechanisms also depletes the market's ability to inform traders about the liquidity level of a financial instrument due to the presumed reduction of the effect in infinitesimal timeframes.

[97] A. Puorro, *High Frequency Trading:* una panoramica, cit., pp. 22-23. Cfr. A. Azzutti – W.G. Ring – H. S. Stiehl, *Machine learning, market manipulation and collusion on capital markets: why the "black box" matters*, in *EBI Working Paper Series* (*ebi-europa.eu*), n. 84, 2021, p. 28, who argue that the opacity of AI system functioning makes it incomprehensible how and why a specific algorithmic operation is performed.

[98] Si vedano B. Biais – T. Foucault, *HFT and market quality*, in *Bankers, Markets & Investors*, Vol. 128, n. 1, 2014, pp. 5-19; A. Kirilenko – A.S. Kyle – M. Samadi – T. Tuzun, *The flash crash: High-frequency trading in an electronic market*, in *The Journal of Finance*, Vol. 72, n. 3, 2017, pp. 967-998; V. Caivano, *The impact of high-frequency trading on volatility. Evidence from the Italian market*, in *Quaderni di finanza CONSOB* (consob.it), n. 80, marzo 2015.

[99] See G. Strampelli, *L'informazione societaria a quindici anni dal T.U.F.: profili evolutivi e problemi*, in *Riv. soc.*, n. 5, 2014, p. 1005.

[100] See F. Consulich, *Il nastro di Mobius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, cit., pp. 195 et seq., especially pp. 207, 218, and M. Palmisano, *L'abuso di mercato nell'era delle nuove tecnologie*, in *Dir. pen. cont.*, n. 2, 2019, pp. 129 et seq., especially p. 133.

[101] According to G. Strampelli, *L'informazione societaria a quindici anni dal T.U.F.: profili evolutivi e problemi*, cit., pp. 1002-1004, the information gap between algorithmic traders and other traders cannot be bridged by regulations on mandatory disclosure. This is because the operational conduct of algorithmic traders is not a result of insider trading abuse but rather the technological advantage provided by the infrastructure they use.

the offense[102]. This was the case in the United States, where Michael Coscia was convicted of programming an algorithm to carry out a "pump and dump" scheme, consisting of simultaneously sending large and small buy and sell orders to create the illusion of demand and manipulate the representation of trades for other market participants[103].

If it is not possible to identify a malicious subjective component attributable to the programmer or user of the trading algorithm, this could result in a delimited area of impunity for criminal offenses[104]. In such cases, the legal order of the market would be safeguarded solely through administrative liability, provided it is still possible to attribute negligent reproach to the individual for manufacturing and design defects or for negligence in supervision[105].

[102] F. Consulich, *Il nastro di Mobius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, cit., p. 209.

[103] A. Lupoi, *La negoziazione algoritmica ad alta frequenza e la struttura dei mercati: due casi negli Stati Uniti*, cit., pp. 4-8.

[104] There is a «*failure of existing liability rules*» A. Azzutti – W.G. Ring – H. S. Stiehl, *Machine learning, market manipulation and collusion on capital markets: why the "black box" matters*, cit., pp. 29-31

[105] In this regard, D.W. Slemmer, *Artificial Intelligence & Artificial Prices: Safeguarding Securities Markets from Manipulation by Non-Human Actors*, in *Brook. J. Corp. Fin. & Com. L.*, Vol. 14, Issue 1, 2019, pp. 149 et seq., proposes that regulatory authorities require users of AI systems to provide meaningful feedback to detect potential manipulations and to create evidentiary records in case there are instances of manipulation by the artificial agent.

II The adequacy of the regulatory provision concerning market abuse

1 Insider trading and AI

For what has been said before, it now stands auto clearly why the various legal systems have responded to the risks of market abuse by implementing multiple safeguards affecting both trading venues and trading platforms, as well as directly accessing parties such as intermediaries, financial instrument issuers, professional or non-professional investors, and even entities whose behaviour influences price formation. This includes media organizations in the economic and financial field, institutions disseminating statistics, research analysts, academics making press interventions, and those who present themselves as "experts" in investment matters on social media. Additionally, various provisions concern regulators themselves.

If the objective is to protect trust in the proper functioning and credibility of the financial market[106], it is not solely the repressive action against abuses that can significantly reduce the risks[107].

Each punitive case is based on defining the scope of application, on the identification of (privileged) information that can be subject to abuse, and examining the actions taken by individuals who naturally differ greatly in terms of their type and quality[108].

[106] S. Seminara, *Il diritto penale del mercato mobiliare*, Torino, 2022, pp. 8 et seq.

[107] Article 16, par. 1, of Regulation (EU) MAR requires market management companies to establish and maintain devices, systems, and procedures aimed at preventing and detecting market abuse. There are several implicit references, such as circuit breakers that automatically halt trading in the event of excessive price fluctuations, random closure of auction trading phases, etc. Additionally, these companies, along with intermediaries and any professionals operating in the markets, must report any suspicious transactions ("STR") they identify through appropriate systems and procedures to the relevant national authority. Articles 17, 18, and 19 of Regulation (EU) MAR impose obligations on issuers regarding the publication of inside information, procedures for managing confidentiality, and public disclosure of transactions made by managers on financial instruments issued. Article 20, paragraph 1, of Regulation (EU) MAR requires financial analysts to comply with a series of measures ensuring the accuracy of their assessments and to publicly disclose conflicts of interest. Article 20, paragraph 2, of MAR instructs institutions disseminating statistics or forecasts that may have a significant impact on the markets to publish them in a correct and transparent manner, avoiding selectivity. Article 21 of Regulation (EU) MAR also addresses journalists and the media, stating that their conduct is evaluated in relation to potential market informational manipulation, unlawful disclosure of insider information, or dissemination of investment recommendations, while considering professional norms. Various rules also apply to national competent authorities, particularly in the case regulated by Article 13 of Regulation (EU) MAR, where they intend to authorize a market practice at the national level that may serve as a defense against information-based manipulation.

[108] For a detailed description of the regulatory evolution of the different types of market abuse, please refer to F. D'Alessandro, *Market Abuse*, in M. Cera – G. Presti (a cura di), *Il testo unico finanziario*, Vol. II, Bologna, 2020, pp. 2166 et

Regarding the latter, over the decades of development and implementation of regulations, certain differences related to the quality of individuals have become less distinct: whether they are natural or legal person s, whether they possess the information due to their occupation, profession, or function (primary insiders), or for other reasons (secondary insiders), whether they are professional or retail investors, regulated or unregulated entities, or whether they are corporate issuers or individuals. As mentioned earlier, recent analysis, including the analysis contained in this essay, examines whether specific rules should be provided for AI systems.

1.1 Criminal insider and AI

One of the most concerning scenarios in countering market abuse involves the case where terrorist or criminal organizations intervene in financial markets, potentially using sophisticated methods, by exploiting information related to ongoing criminal activities which can impact the prices of financial instruments. In the aftermath of the heinous attacks on the Twin Towers in New York on September 11, 2001, due to the sudden and persistent reductions in the prices of many financial instruments that could be exploited by the same terrorist organizations that carried out the attack, the Council of the European Union and the European Parliament intervened on the initial proposal of the European Commission regarding MAD I (Directive 2003/6/EC of January 28, 2003), explicitly extending the prohibition of abuse not only to the managers of listed companies but also to criminal organizations. MAD I Directive (Article 2, paragraph 2, letter d) expanded the scope of primary insiders to include those who possess privileged information "by virtue of their criminal activities." The EU Market Abuse Regulation (MAR) confirmed this approach by including among primary insiders those who possess privileged information "by virtue of being involved in criminal activities"[109].

The literal interpretation shows that a person falls within the category of primary insiders even if the information they come into possession of is not related to their own criminal activity, as was the case with terrorism mentioned earlier, but rather information produced by other parties, possibly even by the issuer itself. For example, someone who steals a document containing important corporate information that is about to be published assumes the status of an active subject of the offense, even if

seq., and to M. Bencini – V. Todini, *Gli abusi di mercato*, in M. Bencini – L. Fanfani – S. Pelizzari – V. Todini, *Profili penali della tutela del risparmio. Truffa, abusi di mercato e gestione patrimoniale*, Milano, 2021, pp. 153 et seq.

[109] In particular, please refer to Considerations 14 and 17 of MAD I, which expressly recognized that «(t)his Directive meets the concerns expressed by the Member States following the terrorist attacks on 11 September 2001 as regards the fight against financing terrorist activities» and specified that «account should be taken of cases where inside information originates not from a profession or function but from criminal activities». Following the expansion of the prohibition on the use of inside information to anyone who possesses such information «by virtue of his criminal activities» the Italian legislator extended the prohibition to anyone in possession of inside information «a motivo della preparazione o esecuzione di attività delittuose» (Article 184(2) TUF). For further analysis, see M.I. Steinberg, *The Sec and the Securities Industry Respond to September 11*, in *International Lawyer*, Vol. 36, n. 1, 2002, pp. 131 et seq. Subsequently, with MAD II, Article 3(3)(d) expanded the prohibition to anyone who possesses inside information "being involved in criminal activities". In this way, the qualification of a criminal insider and the possession of inside information no longer arise solely from the commission of a criminal activity, but also from the scenario in which the insider participates in the offense committed by others.

he did not participate in the creation of that event and was uninformed about it "through the exercise of an employment, profession, or duties."

The substantial alignment already achieved by MAD I Directive (and, more recently, in Italy, in the criminal sphere, by Law No. 238 of December 23, 2021, which amended Article 184 TUF) between primary insiders and secondary insiders means that this subjective distinction only matters in terms of defining the penalty, which, under equal conditions, should be higher for primary insiders given the role or activity they perform[110]. It is highly likely that a criminal insider who does not fall into the category of primary insider will still receive a significantly high penalty due to the significant negative value of their conduct.

AI systems could potentially be tools trained to commit crimes as part of broader criminal schemes carried out by the AI systems themselves or by other systems acting in various ways under the control of the same subject or multiple colluding entities.

Let us consider for example cyber-attacks that disrupt major operators, intermediaries, or institutional investors, forcing them to engage in significant sales of financial instruments to prevent further problems (such as prudential stability) or even create difficulties for the trading platform, where an impact on prices or a halt in trading can be predicted in advance. Such information could easily assume privileged nature and be exploited by an AI system through market orders calibrated just before the attack is made public by the involved parties or the media.

In such situations, we would fall into the category of AI systems trained to commit crimes (see paragraph 3 above). However, the same can be said, even more so, if the privileged information is part of the planned activity of the same AI system. Classic cases involve acquiring the credentials of a broker's clients, enabling AI systems to manipulate those accounts for the benefit of others or to place buy or sell orders that create bubbles in the prices of specific financial instruments, facilitating easy gains for colluding individuals.

Another strategy of abusing AI systems could involve committing small but repeated violations, making it difficult for victims to realize that they have been lured or defrauded. This strategy becomes more insidious as the algorithm becomes more "intelligent" (or rather, cunning) and manages to distribute illicit activities in a way that makes the overall criminal plan unrecognizable.

[110] Directive 89/592/EEC (MAD I), which introduced a framework for insider trading in EU law, defined in Article 4 the secondary insider as «(a)ny person [...] who with full knowledge of the facts possesses inside information, the direct or indirect source of which could not be other than» a primary insider. With Directive 2003/6/EC, and subsequently with Regulation (EU) No 596/2014 (MAR) and Directive 2014/57/EU (MAD II), the second condition was removed, so the secondary insider is simply defined as « the person who knows, or ought to have known, that it is inside information» thus severing the link between the secondary insider and the primary insider. As highlighted, "This provision clearly demonstrates that the European prohibition of insider trading is based on an equal access to information theory, and not on fiduciary duties" (M. Ventoruzzo, *Comparing insider trading in the United States and in the European Union: History and recent developments*, in *European Company and Financial Law Review*, Vol. 11, n. 4, 2015, pp 554-593).

1.2 Self insider and AI

Widely debated in doctrine and jurisprudence is the hypothesis in which a subject abuses information related to an event designed/conceived by the same subject.

In the context of insider information concerning public takeover bids, the *Cremonini case* has long been examined, relating to transactions carried out by the subject controlling the listed company before launching a takeover bid that would lead to its delisting.

According to Consob's opinion, if the market purchases by the subject controlling the issuer were made when they had already decided to launch a delisting takeover bid but had not yet disclosed it to the public, then those purchases would have violated the related regulations, despite the circumstance that the information was conceived by the same subject who carried out the transactions[111].

However, a part of doctrine holds a different view, according to which the unlawfulness of the conduct requires a «necessaria alterità nei confronti dell'informazione» because, even semantically, «un determinato nucleo di conoscenze potrà essere qualificato "informazione" solo ove sottenda il suddetto passaggio trasmissivo di due sfere di conoscenze»[112]

In jurisprudence, on the other hand, the prevailing opinion is that the self-insider is punishable both in criminal and administrative aspects[113].

[111] Consob Resolution No. 17777 of May 11, 2011. The Consob resolution was subject to opposition, pursuant to Article 187-*septies* TUF, before the Court of Appeal of Bologna, which subsequently rejected it; a decision later upheld by the Court of Cassation, Civil Section, on April 13, 2017, No. 24310, in *Banca borsa tit. cred.*, n. 6, 2018, pp. 962 et seq., with a note by A. Bartalena, *O.p.a. per* delisting *e* insider trading*: brevi riflessioni sull'*insider *di sé stesso*, in *ivi*, pp. 2617 et seq., e di F. Cadorin, *OPA per il* "delisting" *fra* "insider" *di se stesso ed efficienza del mercato*, in *Giur. comm.*, n. 1, 2019, pp. 105 et seq.; S. Lombardo, *L'*insider *di se stesso alla luce della decisione della Corte di Cassazione (civile)*, in *Giur. comm.*, n. 4, 2018, pp. 666 et seq.

[112] S. Seminara, *Il diritto penale del mercato mobiliare*, cit.; M. Ventoruzzo, *Qualche nota su cosiddetto "insider di sé stesso" alla luce del Regolamento UE sugli abusi di mercato*, in *Soc.*, n. 6, 2018, pp. 745 et seq.; A.F. Tripodi, *Informazioni privilegiate e statuto penale del mercato finanziario*, Padova, 2012.

[113] Refer to the decision of the Criminal Court of Cassation, Fifth Section, April 15, 2021, No. 31507, in which the judges of the Supreme Court affirm the criminal relevance of the self-insider. In particular, the Court outlines a new interpretation of the concept of «informazione» as a «insieme di dati descrittivi della realtà» which does not necessarily imply a «dinamica» component of information collection and transmission, but also a «statica» component, meaning «il dato di conoscenza, ancorchè quest'ultimo sia rappresentativo di una realtà prodotta dal medesimo soggetto obbligato». Based on these considerations, the Court deemed the grounds for appeal unfounded and clarified that Article 184, par. 1, TUF does not require necessary distinctiveness between the creator and user of the information, establishing that the provision in question «non punisce chi disponga di una mera posizione privilegiata derivante dalla possibilità di meglio leggere, valorizzare, interpretare informazioni, ivi incluse quelle di pubblico dominio, delle quali disponga, ma colui che, come nel caso di specie, essendo a conoscenza, in ragione delle qualità soggettive indicate dal legislatore, di eventi *price sensitive* [...], sfrutti siffatta conoscenza per operare in condizioni di disparità con gli altri investitori, finendo per danneggiare un valore (la fiducia nella trasparenza dei mercati), che mira ad incentivare e a non scoraggiare l'afflusso e la circolazione dei capitali nell'interesse degli stessi imprenditori interessati al loro utilizzo per iniziative produttive». Regarding this ruling, see D. Federici, Insider *di sé stesso e abuso di informazioni privilegiate: la Corte di Cassazione conferma la punibilità anche del creatore della notizia*, in *Sistema Penale* (*sistemapenale.it*), 13 ottobre 2021, e A. Santangelo, *Una soluzione "di favore" per l'*insider *di se stesso: la* rule of lenity *quale criterio di risoluzione di casi difficili*, in *Dir. pen. proc.*, n. 10, 2022, pp. 1343 ss., and A. Santangelo, *Una soluzione "di favore" per l'*insider *di se stesso: la* rule of lenity *quale criterio di risoluzione di casi difficili*, in *Dir. pen. proc.*, n. 10, 2022, pp. 1343 et seq. Contrary to this decision, refer to the previous decision of the Civil Court of Cassation, Second Section; May 12, 2020, No. 8782, and the related commentary by C. Passi, *Esiste il* Self-insider*, ma va scagionato! Riflessioni intorno*

As highlighted[114], in the context of mandatory takeover bids, regulatory requirements pushing for the legitimacy of pre-emptive purchases by the offeror still face a difficult limit when the definition of insider information (the decision to launch the takeover bid) precedes such purchases.

A self-designed AI system that exploits market transactions based on information it has designed would certainly commit an offense[115].

A tangible example of insider information that an artificial operator is capable of designing or conceiving involves AI systems that initially acquire elementary information on pending orders by 'caring' for them (perhaps obtained from the same intermediary managing the AI system in its relationships, whether computerized or not, with retail or institutional clients) and subsequently define an optimal dynamic minimization strategy for the price impact of those orders[116]. In this context, the AI system could be 'extended' with the decision to execute additional orders for the intermediary's proprietary accounts, taking advantage of the impact that the predefined dynamic minimization strategy would generate in the market. Essentially, this falls within the scope of a sort of front-running scheme.

Similar examples could involve investment recommendations generated by robo-advisors, where the AI system exploits such information by anticipating the probable orders of the clients receiving those recommendations, possibly in separate documents (such as studies or research on specific industrial sectors or securities or as commentary on news disseminated by the media or on price trends).

The issue of self-insider detection related to an AI system is more complex. In cases where weak AI systems are in operation[117], such detection is always possible because the logical decision-making process leading to market orders is transparent by definition. Conversely, for strong AI systems, such detection is made challenging due to the opacity (black box) of their logical decision-making process.

1.3 Tipping, tuyautage and AI

In addition to executing transactions, other main forms of exploiting insider information that are typically prohibited by regulations involve communicating the in-

alla sua qualificazione giuridica, in *Soc.*, n. 4, 2021, pp. 455 et seq. The decision of the Supreme Court concludes a judicial process in which the Milan Court of First Instance, Third Section, ruled on February 5, 2016, No. 12149, and then the Milan Court of Appeal, Second Section, on January 15, 2019, No. 284, considering the conduct of the self-insider relevant in criminal proceedings. See F. Raffaele, *Ritorno Futuro 3: l'"insider di se stesso" all'esame della Cassazione e il nuovo tentativo di ipostatizzare il market egalitarianism*, in *Giur. comm.*, n. 4, 2019, pp. 778 et seq.

[114] M. Maugeri, *Offerta pubblica di acquisto e informazioni privilegiate*, in *Riv. dir. comm.*, n. 2, 2018, pp. 267 et seq.

[115] M. Ventoruzzo, *Qualche nota su cosiddetto "insider di sé stesso" alla luce del Regolamento UE sugli abusi di mercato*, cit.

[116] As known, these AI systems are used by both intermediaries and institutional investors.

[117] As illustrated in Section II, paragraph 1, AI systems can be distinguished based on their different capacity for interaction with humans. While weak AI systems produce outputs that depend on preestablished instructions from producers, programmers, or users, more advanced strong AI systems, equipped with self-learning capabilities, generate autonomous and unpredictable outputs compared to the initial inputs provided by the producer, programmer, or user.

formation to third parties without a "legitimate reason" (known as tipping) and recommending to third parties (known as tuyautage[118]) based on the insider information to engage in advantageous transactions. Similar prohibitions apply to the recipients of such illicit communication and recommendations. These prohibitions are necessary to prevent easy circumvention of insider trading rules and serve to safeguard the integrity of the markets. Without these prohibitions, there could be theoretically paradoxical situations where the number of individuals aware of insider information exceeds the number of individuals unaware of it[119].

For cases of tipping and tuyautage, it is necessary to identify the privileged information that an AI system could potentially abuse. The analyses mentioned before apply in this regard, regarding cases such as a system considering information related to a cyber-attack, pending client orders, or investment recommendations to clients.

With respect to investment recommendations, we can examine a scenario where the recommendations precisely concern the set of information that prompts the AI system to execute trading activities for which it has been programmed, leveraging its significant data storage and processing capabilities for profitability. For example, the multitude of micro-information regarding movements occurring in the depth of order books for financial instruments traded on multiple trading venues or related and correlated financial instruments—entering the realm of big data. Another example includes information gathered by satellites about traffic volume on highways, enabling more accurate revenue predictions for highway companies, within the realm of alternative data and mosaic theory[120]. Yet another example is the immediate detection of information released by news agencies.

It is evident that such information utilized by AI systems to develop their speculative, investment, trading, or arbitrage strategies, which could be qualified as privileged if made public by the system (consider the case where the trading strategy is represented in a specific study distributed by the intermediary to its clients), can not only be used by the AI system as its own insider but also be subject to lawful communication to third parties or recommendations to transact in a certain direction. This is the case with robo-advising[121].

In general, if the fundamental information on which such strategies are based is public, there is no presumption of abuse.

However, the question arises as to whether certain types of information, such as those contained in photographic observations processed by orbital satellites, can be

[118] They are sometimes also referred to as illegal disclosure and tipping, respectively.

[119] For an analysis of tipping and tuyautage behaviours, please refer to V. Calandra Buonaura, *Sub art. 184*, in *Commentario breve al Testo Unico della Finanza*, Padova, 2020, pp. 1228 ss., especially pp. 1236-1241.

[120] D.E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, in *The Yale Law Journal*, 2005: «*The "mosaic theory" describes a basic precept of intelligence gathering: Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information. Combining the items illuminates their interrelationships and breeds analytic synergies, so that the resulting mosaic of information is worth more than the sum of its parts*».

[121] N. Linciano – V. Caivano – D. Costa – P. Soccorso – T.N. Poli – G. Trovatore, *L'intelligenza artificiale nell'asset e nel wealth management*, *Quaderni FinTech*, Consob, n. 9, 2022.

considered public given the significant investment required to acquire them. With specific reference to the financial field, the same could be said for substantial investments necessary for the reprocessing of information related to order books or to the collection of disaggregated information.

Considering that such investments are not accessible to every investor, to the extent that the difficulty of accessing such information has raised concerns about market competitiveness[122], it could be evaluated whether this difficulty undermines the rationale of the regulation that justifies the introduction of the abuse prohibition with the (at least potential) egalitarianism of participating investors in the exchanges.

In this regard, it must be noted that there are indeed many entities investing in these technologies (and, of course, even more that have the possibility to do so), and expertise moves fluidly, involving academia in an indispensable manner, which brings forth a drive for technology and output dissemination[123]. It is also worth noting that an incentive for dissemination is inherent in data providers. Consider the functions offered by Bloomberg or Refinitiv Eikon to their extensive client base, both professional and non-professional, which enable real-time access to variables that academic literature has qualified as "informative" because they express market sentiment, such as the number of times a stock's name appears on Google or Twitter[124].

In conclusion, it seems that the observation made in the past regarding access to information disseminated by newspapers still applies to this new context: although access to such information may require a significant cost for many investors, it does not question the soundness of the regulation's rationale.

Therefore, if the privileged information detected (rather than created) by the AI system can be presented in the form of studies, research, or investment recommendations and disseminated by the intermediary managing the AI system to its respective customers, it is evident that the communication of such information or the trading recommendations based on it would be considered lawful.

However, it is essential to comply with the general framework provided by MAR, ensuring that such studies, research, or investment recommendations are disseminated to the clientele in a fair manner that prevents abuses. For instance, the MAR requires these studies to indicate the date and time of their initial dissemination to

[122] D. Duffee – T. Foucault – L. Veldkamp – X. Vives, *Technology and Finance*, CEPR, 2022.

[123] The issue appears to be very similar to that of restricted access to research or studies disseminated for a fee by financial analysts, which are then widely distributed by media providers to their extensive clientele in summarized form (target price, recommendations, annual corporate earnings forecasts). It is precisely the media providers who determine the so-called analysts' consensus, which is a statistical summary of the estimates produced by the analysts.

[124] J. Bollen – H. Mao – X. Zeng, *Twitter mood predicts the stock market*, in *Journal of computational science*, Vol. 2, n. 1, 2011, pp. 1-8; J.W. Godell – S. Kumar – W.M. Lim – D. Pattnaik, *Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters from bibliometric analysis*, in *Journal of Behavioral and Experimental Finance*, Vol. 32, 2021, pp. 100577; A. Yadav – D.K. Vishwakarma, *Sentiment analysis using deep learning architectures: a review. Artificial Intelligence Review*, Vol. 53, n. 6, 2020, pp. 4335-4385; X. Li – W. Pangjing – W. Wenpeng, *Incorporating stock prices and news sentiments for stock market prediction: A case of Hong Kong*, in *Information Processing & Management*, Vol. 57, n. 5, 2020, pp. 102212; P.C. Tetlock – M. Saar – M. Tsechansky – S. Mackassy, *More Than Words: Quantifying Language to Measure Firms' Fundamentals*, in *The Journal of Finance*, Vol. 63, 2008, pp. 1437-1467.

customers[125]. Therefore, anyone who receives them before that moment should refrain from using them for market transactions, as they still qualify as insider information, or from disclosing them to third parties. Conversely, those who receive them after that moment are aware that the information has likely already been acted upon by other clients.

2 Market manipulation and AI

The challenges in the use of artificial intelligence are among the most debated issues today, not only in the financial market[126]. Particularly concerning the challenges of AI in the realm of financial transactions, the risks to market integrity arising from the behaviour of AI systems are perceived to be greater in trading rather than in the creation and circulation of insider information. They have been the subject of numerous investigations and regulatory interventions, especially regarding high-frequency trading (HFT) carried out primarily by market participants[127].

The trading activity of a weak AI system is ultimately nothing more than a highly sophisticated evolution of elementary conditional orders, such as iceberg orders or stop-loss orders, which, upon reaching certain price levels, introduce a certain quantity for purchase or sale into the market. These types of orders emerged in the wake of the introduction of electronic trading systems in the 1990s, presenting various critical aspects that were nevertheless largely overcome.

The regulatory framework that has emerged to manage HFT activities appears to be quite adequate in addressing the associated risks[128]. Moreover, some cases of abuse have already been sanctioned in several jurisdictions, including within the EU[129].

[125] Please refer to Articles 7 and 8 of Delegated Regulation (EU) 2016/958. Article 7 states that «(w)here a person producing recommendations, actually disseminates a recommendation it produced, it shall include in the recommendation the date and time when the recommendation was first disseminated».

[126] In a letter published on the Future of Life Institute website on March 22, 2023 (https://futureoflife.org/open-letter/pause-giant-ai-experiments/), signed by Elon Musk, Yuval Noah Harari, Steve Wozniak, Andrew Yang, and others, the risks posed by artificial intelligence to society and humanity are highlighted. The authors question whether AI systems should become as competitive as humans, posing a danger of losing control over our civilization. They conclude the letter expressing the hope to be prepared for the autumn of artificial intelligence after a long summer of AI development. This letter has received media attention; see, among others, M. Gaggi, *Perché l'intelligenza artificiale spaventa i re della tecnologia*, in *Corriere della Sera*, March 30, 2023, pp. 1-22. More recently, Geoffrey Hinton, the father of the technology behind ChatGPT, has joined this appeal, warning about the "terrifying" consequences of utilizing artificial intelligence, as this technology would be capable of learning separately and instantly sharing knowledge with all other systems. See P. Pisa, *Il 'Nobel' dell'informativa lascia Google. "L'intelligenza artificiale è pericolosa"*, in *La Repubblica*, 3 maggio 2023, p. 14.

[127] On the evolution of the regulatory framework concerning market manipulation, see E. Amati, *Abusi di mercato e sistema penale*, Torino, 2012, pp. 171 et seq., and more recently, regarding administrative offenses, Id., *L'illecito amministrativo di manipolazione del mercato e le persistenti criticità del doppio binario sanzionatorio*, in *Giur. comm.*, n. 2, 2021, pp. 263 et seq., and, concerning criminal offenses, to F. Consulich, *Manipolazione dei mercati e diritto eurounitario*, in *Soc.*, n. 2, 2016, pp. 203 et seq.

[128] On the prospects for a revision of the EU regulation, see ESMA "MIFID II Review Report," September 28, 2021, ESMA70-156-4572.

[129] The case law includes (in parentheses the year in which the manipulation occurred): in USA *US SEC vs Athena Capital Research LLC* (2009); *US SEC, CFTC e UK FCA vs Michael Coscia* (2011); *CFTC vs Jiongsheng Zhao* (2012 -2017); *CFTC vs Morgan Stanley Capital Group Inc.* (2013 – 2014); *CFTC vs Krishna Mohan* (2013); *CFTC vs Propex Derivatives PTY Ltd*

Naturally, significant doubts remain regarding the behaviour of an individual weak AI system or the combined behaviour of multiple AI systems, especially in conditions of high market uncertainty or during market disruptions, such as flash crashes.

To assess the challenges associated with the simultaneous use of multiple AI systems, consider, initially, that it is not uncommon to observe disjointed trading activities by intermediaries, typically when trading in markets through multiple desks (including human ones) for the same financial instrument, each pursuing different objectives. One desk may act as a market maker, another for delta hedging[130] the proprietary portfolio, and yet another to exploit short-term or very short-term price trends (referred to as directional trading). In such cases, suspicions of manipulation may arise if one leg of a desk's transactions (either the buying or selling leg) intersects with or crosses paths with another desk's leg, resulting in apparent fictitious transactions (matched orders)[131] in the first case, and typical manipulative practices (such as trash & cash) in the second case[132].

(2012 - 2017); *CFTC e US SEC vs Navinder Singh Sarao* (2019 – 2015); *FINRA vs Trillium Brokerage Services, LLC* (n.d.); *US SEC vs Hold Brothers On-Line Investment Services* (2009 – 2011); *AMF vs Virtu Financial Europe* (2009); *AMF vs Getco Europe* (2010 – 2012); *AMF vs 3Red Trading LLC* (2012 – 2013).

[130] Delta hedging involves daily buying and/or selling operations on the underlying of derivative financial instruments to hedge the risk of price variations of the underlying on previously taken positions on such derivative financial instruments. (J. Hull, *Opzioni futures e altri derivati*, Pearson, 2022).

[131] In Annex II of Commission Delegated Regulation (EU) 2016/522 supplementing MAR (Level 2), the practice (manipulative) of «Transactions carried out as a result of the entering of buy and sell orders to trade at or nearly at the same time, with very similar quantity and similar price, by the same party or different but colluding parties — usually known as 'improper matched orders'. This practice may also be illustrated by the following additional indicators of market manipulation: (i) transactions or orders to trade which have the effect of, or are likely to have the effect of setting a market price when the liquidity or the depth of the order book is not sufficient to fix a price within the session; (ii) the indicators set out in Points 1(a)(i), 3(a)(i) and 3(a)(ii) of this Section [i.e.: unusual concentration of transactions and/or orders to trade, whether generally, or by only one person using one or different accounts, or by a limited number of persons;]*, e par. 3, lett. a), punti i) e ii)* [i.e.: «Entering into arrangements for the sale or purchase of a financial instrument, a related spot commodity contract, or an auctioned product based on emission allowances, where there is no change in beneficial interests or market risk or where beneficial interest or market risk is transferred between parties who are acting in concert or collusion — usually known as 'wash trades'. This practice may also be illustrated by the following additional indicators of market manipulation: (i) unusual repetition of a transaction among a small number of parties over a certain period of time; (ii) transactions or orders to trade which modify, or are likely to modify, the valuation of a position while not decreasing/increasing the size of the position»]. Examples of manipulation through "improper matched orders" have been sanctioned by Consob, including cases where an asset manager, responsible for the operations of two funds, favoured the performance of one fund at the expense of the other, from which they received lower fees. Specifically, the asset manager first entered a large order on behalf of the favoured fund at a price that was far from the bid-ask spread (thus not affecting the price formation process), and subsequently entered an even larger order on behalf of the other fund at a price that would cross all orders at more favourable prices from the first fund, effectively "climbing" the trading book until reaching the intended fund. This operation effectively "cleaned" the book with a series of trades, generating a significant instantaneous price variation, which typically rebounded shortly after due to the activity of arbitrageurs recognizing a price inconsistent with publicly available information. For a detailed analysis C. Milia, *Essays in Market Manipulation and Insider Trading*", PhD Thesis, Bocconi University, 2008.

[132] In the Annex II of Delegated Regulation (EU) 2016/522 of the Commission supplementing MAR, the practice (manipulative) identified is the one of «(t)aking of a short position in a financial instrument, related spot commodity contract, or an auctioned product based on emission allowances and then undertaking further selling activity and/or disseminating misleading negative information about the financial instrument, related spot commodity contract, or an auctioned product based on emission allowances with a view to decreasing the price of the financial instrument, related spot commodity contract, or an auctioned product based on emission allowances, by the attraction of other sellers. When the price has fallen, the position held is closed — usually known as 'trash and cash'. Essentially, this practice is the opposite of the 'pump and dump,' that is, the manipulative price bubble.

Now, when desks are managed by individuals or weak AI systems, suspicions of manipulation could ultimately be ruled out by examining the track record of previous transactions on the same accounts, identifying the external conditions that motivated the orders, seeking explanations from traders or the compliance unit of the intermediary, and so on.

Furthermore, as a preventive measure, the market management company could counter the risks associated with such potential suspicious operations (matched orders)[133] by automatically cancelling the intersecting contracts produced by the same intermediary's own account, even if they are from different desks.

To assess the challenges associated with the use of a single weak AI system, it is worth considering that it is already common practice for many major institutional investors to place their substantial orders according to specific timing determined by AI, for example, to minimize the impact of their transactions on prices (price impact)[134]. The orders that these investors enter into the markets to manage their significant portfolios are often much larger than the market liquidity, so their execution requires that a period of time elapses in order to avoid generating adverse price impacts. If an investor intends to take a position in a stock, the more their buying orders cause price increases, the higher the entry price of the position they intend to take will be, and thus the lower the potential profit they may achieve if the expected price rise materializes. It is therefore usually preferable to enter orders into the market gently, spaced out over time, "taking care"[135] as Italian institutional investors verbally advised the intermediaries entrusted with executing such substantial orders.

While minimizing the price impact should also reduce the risks of significantly affecting the price formation process[136], it is also true that the overarching goal of minimizing costs may not be subject to further conditions. In a scenario where an institutional investor intends to reduce his position in a financial instrument, an algorithm that even anticipates a forthcoming price reduction for that instrument would find it advantageous to accelerate the entry of sell orders for the same instrument to reduce the expected losses resulting from the anticipated worsening of price conditions. The timeliness and aggressiveness of execution with frequent and substantial sell orders would, therefore, be fully consistent with the aforementioned goal of reducing the price impact of the orders.

It is worth noting that the weak AI system that triggered the well-known flash crash on May 6, 2010, was used by an institutional investor who aimed to hedge his extremely high positions in individual stocks by rapidly and progressively selling

[133] Borsa Italiana S.p.A. provides, as a preventive measure, the possibility for member intermediaries to automatically cancel orders placed by proprietary accounts, known as Self-Trade Prevention ("Guide to the Euronext Trading System," Version 1.2, March 2023).

[134] *Ex pluribus*, see Bouchaud, Jean-Philippe. "Price impact." arXiv preprint arXiv:0903.2428 (2009).

[135] The "curando" order is an order in which the client relies on the intermediary's expertise to select the best market opportunities. These orders do not specify any price conditions and must be executed by the intermediary in the most suitable manner and timeframe for the client.

[136] For applications of AI in trading activities, please refer to ESMA "*Artificial Inteligence in EU Security Markets*", ESMA-164-6247, 3 February 2023.

futures on the stock index. That algorithm placed unlimited price sell orders every minute as long as they represented 9% of the total quantities traded in the market in the previous minute, thus progressively intensifying the downward trend of prices[137].

The doubts and challenges raised by the aforementioned trading models take on a new dimension when considering the hypothesis that such conduct is carried out using strong AI systems[138], namely those based on artificial neural networks, deep reinforcement learning, where the algorithm is capable of recognizing new profit opportunities on its own, without the same algorithm or its programmers or managers being able to explain the logical path that led to the observed trading choices[139].

Indeed, when legs are driven by a strong AI system, the possibility for the intermediary, the market management company, and even the regulatory authorities to retrospectively identify the origin of the pursued trading strategy is lost. Market making, delta hedging, directional trading[140], and so on. In other words, it may be possible to represent what the strong AI has done, one may explain why it should have done it, but one cannot explain why it did it.

Additionally, consider the realistic scenario where the AI system, despite being strong in terms of deep learning and autonomous development of trading strategies, lacks self-awareness, meaning it is unable to recognize that some of the orders it sees in the order book have been entered by itself, as if it were a headless octopus.

In a recent analysis conducted by the Dutch authority AFM, it emerges that many intermediaries do not use strong AI systems due to concerns about managing the risk of market disruptions, also stemming from the inability to possibly provide explanations to the authorities[141].

Nevertheless, evidence of the use of strong AI systems exists.

It does not mean that their adoption necessarily leads to behaviours that constitute market manipulation on their own. However, if the same institutional investor, perhaps through the same account and the same strong AI system, were to enter orders in the opposite direction to the trend triggered by the aforementioned sell orders, then

[137] A. Kirilenko – A.S. Kyle – M. Samadi – T. Tuzun, *op. cit.*, pp. 967-998. CFTC SEC, *Findings regarding the market events od May 6, 2010 – Report to the Staffs of CFTC and SEC to the joint advisory committee on emerging regulatory issues*, 30 September 2010.

[138] In the mentioned Asilomar principles, strong AI systems are referred to as both "advanced AI systems" (Principle n. 9) and "(h)ighly autonomous AI systems" (Principle n.10). The Asilomar principles can be found on the Future of Life Institute's website (https://futureoflife.org/open-letter/ai-principles/).

[139] E. Martínez-Miranda – P. McBurney – M.J.W. Howard, *Learning unfair trading: A market manipulation analysis from the reinforcement learning perspective*, 2016 IEEE Conference on Evolving and Adaptive Intelligent Systems (EAIS), Natal, Brazil, 2016, pp. 103-109. To address the need for transparency and open the "black box," numerous analyses are being conducted by the scientific community in the field of *Explainable AI* (ovvero, XAI): P. Bracke – A. Datta – C. Jung – S. Sen, *Machine Learning exlainability in finance: an application to default risk analysis*, in *Staff Working Paper*, Bank of England, August 2019; P. Giudici – E. Raffinetti, *Shapley*-Lorenz *eXplainable artificial intelligence. Expert systems with applications*, Vol. 167, 2021, pp. 114104.

[140] Directional trading involves trading activities aimed at taking a buying or selling position in financial instruments based on forecasts of the future market prices.

[141] AFM, *Machine Learning in Trading Algorithms – Application by Dutch Proprietary Trading Firms and Possible Risks*, March, 2023.

we would fully fall into a manipulative trash & cash scheme, and probably no one would be in a position to provide an alternative explanation to this. The strong AI system, when left to self-learning and not "trained" to avoid manipulative patterns such as trash & cash, would find it consistent with the objective of minimizing the cost for the investor resulting from the placement of substantial sell orders to follow them with purchase orders capable of profitably mediating the entry price of the sell orders.

Therefore, it is appropriate to question whether strong AI systems can be allowed in trading and under what conditions.

In the hypothesis that it is deemed possible for AI systems to trade in the markets, it is also necessary to consider whether the provisions established by regulations are adequate to counter manipulative behaviours or any other actions that excessively jeopardise market integrity.

2.1 EU regulatory approach

To address the complexity of abusive schemes and the risks of unintentionally capturing legitimate speculative conduct or, furthermore, the difficulty for authorities to distinguish violations from compliant behaviour, Directive 2003/6/EC introduced a comprehensive and well structured approach that contrasted with the holistic approach in force in Italy since 1991 and which still survives, with some modifications, in Article 185 TUF, albeit "limited" to the criminal regime.

While the latter provision currently sanctions «(c)hiunque diffonde notizie false o pone in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari»[142], the Regulation (EU) MAR, which derives from that directive and underpins the corresponding Directive 2014/17/EU that identifies behaviours subject to criminal sanctions, is based on a comprehensive approach consisting of four pillars: the types of behaviours, divided into four categories (Article 12(1)), the examples of such behaviours (Article 12(2)) and the "indicators" of those behaviours (Article 12(3) and Annex I), as well as additional manipulative "practices" (which could be described as manipulated examples or strategies) that specify those indicators (Article 4 and Annex II of Delegated Regulation (EU) 2016/522). Furthermore, Article 15 states the prohibition of manipulation, Article 5 provides for certain exemptions for the purchase of own shares and stabilisation if conducted under certain stringent conditions, and Article 13 establishes a framework for market practices that may be permitted by national supervisory authorities[143].

[142] The English version of the provision is shown below: «any person who disseminates false information or sets up sham transactions or employs other devices concretely likely to cause a significant alteration in the price of financial instruments».

[143] To date, only one practice has been admitted, concerning liquidity contracts and implemented in different ways by the authorities of France, Spain, Italy, and Portugal. Regarding liquidity contracts, a market practice has been generally established for all SMEs with shares traded on their respective growth markets under Regulation (EU) 2019/2155.

The richness of this approach clearly demonstrates how the inherent difficulties in defining wrongdoing are otherwise considered at risk of subjective interpretations: a plurality of behaviours, accompanied by examples and indicators often (but not necessarily) characterizing the manipulative scheme, should indeed reduce such risk, which, according to some[144], is so significant that it is preferable not to introduce any prohibition of manipulation and offer no protection to the value represented by the "proper functioning of the market", i.e., the price formation process and, therefore, the informational efficiency and allocative efficiency of resources[145].

[144] D.R. Fischel – D.J. Ross, *Should the Law Prohibit Manipulation in Financial Markets*, in *Harvard Law Review*, 1991.

[145] Unlike what was previously illustrated regarding insider trading, economic analysis is substantially in agreement that manipulation damages the market. Conducts that artificially deviate market prices from fundamental values or, in any case, from what the market considers as such at a given moment, alter the price formation process, provide false signals to other market participants, reduce the informational efficiency of prices, and ultimately, the allocative efficiency of resources (see L. Loss, *Fundamentals of Securities Regulation*, Boston MA, 1988). Moreover, typically, the gains of the manipulator correspond to at least equal losses for other market participants. It is not necessarily a zero-sum game, as false signals transmitted by the manipulator can generate additional losses for those deceived by such false signals. Furthermore, scandals associated with market manipulation, both information-based and trade-based, systematically lead to a loss of trust in the functioning of markets and thus to the withdrawal of many investors from the markets, or at least from the segments where the scandals occur. Consider, for instance, the corporate bond market after the Parmalat and Cirio scandals or the subprime mortgage market after the 2007 financial crisis. However, several economists have argued that the introduction of a market manipulation prohibition could be excessively costly due to the risk of authorities making evaluative errors in classifying conduct as manipulative, both in terms of information-based and trade-based manipulation (see C.F. Camerer, *Can Asset Markets Be Manipulated? A field Experiment with Racetrack Betting*, in *Journal of Political Economy*, 1988). This is especially true when considering that technically it is not easy to manipulate markets. In fact, compared to the former, it has been argued that those spreading false or misleading information cannot repeat the conduct multiple times without damaging their reputation, leaving no room for long-term market manipulation. Regarding the latter, it has been highlighted that price elasticity (see J.S. Mill, *Principles of Political Economy*, London: Longmans, Green and Co., 1921), high market liquidity, increasingly sophisticated microstructure measures (such as circuit breakers or random closure of electronic auctions), and significant transparency in trades (including disclosure requirements for short sales) do not allow prices to be significantly altered over a prolonged period (see E. Avgouleas, *The Mechanics and Regulation of Market Abuse*, Oxford University Press, 2005). On the other hand, other studies have shown that with regard to information-based manipulation, if false information is not verifiable *ex post* or if the disseminating party can appear to have acted in good faith (as is the case, for example, with financial analysts who produce numerous research reports each month), significant opportunities for market manipulation would exist even in the long run (see R. Benabou – G. Laroque, *Using Privileged Information to Manipulate Markets : Insiders, Gurus and Credibility*, in *Quarterly Journal of Economics*, 1992). Concerning trade-based manipulation, it is now evident that price elasticity depends on the many quantity and time conditions that characterize the orders generating them, while liquidity, microstructure, and transparency, despite limiting the space for potential market manipulation, cannot completely eliminate it. Thus, from an empirical standpoint, at the end of the last century, market manipulation seemed confined to the inadequate structure of markets in previous centuries, with the spectacular price bubbles like tulips bulbs (see P.M. Garber, *Famous First Bubbles*, The MIT Press, 2000), the 18th-century games of stock jobbers (see F. Annunziata, *Un Robinson Crusoe alla borsa di Londra*, La Vita Felice, 2019) or in the early decades of the last century with cornering derivatives markets for commodities (F. Allen – L. Litov – J. Mei, *Large Investors, Price Manipulation, and Limits to Arbitrage: An Anatomy of Market Corners*, in *Review of Finance*, 2006) and *stock pools* (G. Jiang – P.G. Mahoney – J. Mei, *Market Manipulation: A Comprehensive Study of Stock Pools*, in *Journal of Financial Economics*, 2005, p. 77), and more recently, pump & dump schemes, but only in minor markets such as OTC bulletin pink sheets (see R.K. Aggarwal – G. Wu, *Stock Market Manipulations*, in *Journal of Business*, 2006, Vol. 79, n. 4, pp. 1915 ss.). The closer scandals of the new millennium related to IPOs during the tech bubble, to benchmark and Libor manipulation, to the manipulation of spot currency market fixing (see P. Hillion – M. Suominen, *The Manipulation of Closing Prices*, in *Journal of Financial Markets*, 2004, p. 7), the high-frequency trading during flash crashes, and the issues related to the Gamestop case (see US SEC, *Staff Report on Equity and Options Market Structure Conditions in Early 2021*, 14 October 2021) have gradually overturned that optimistic outlook, leading the EU Commission to propose MAD II, the first directive related to the harmonization of criminal sanctions. Moreover, the fragmentation of trading across multiple trading venues has expanded the number of correlations and interconnections of trades, opening up new or additional spaces for cross-market and cross-product market manipulation strategies.

Beyond the different approach at the European level compared to the national one, as still expressed today in the criminal context by Article 185 TUF, it seems possible to agree with those who conclude that "despite the differences in wording, the scope of Article 185 and Article 187-*ter* (which refers to the European regulation, author's note) tend to coincide"[146]. Moreover, following a severe infringement procedure initiated by the European Commission, the national legislation has ultimately been deemed consistent with the Directive 2014/17/EU that identifies behaviours subject to criminal sanctions, which, in turn, in Article 5 perfectly references, with the necessary adjustments due to the criminal nature of the behaviours, the comprehensive wording provided in Article 12 of Regulation (EU) MAR for behaviours sanctioned administratively.

Subsequently, reference will be made to the definitions of Regulation (EU) MAR, starting with trade-based manipulation, the focus of the analyses on the subject.

2.2 Trade-based manipulation and AI

Trade-based manipulation is defined in Article 12, par. 1, of Regulation (EU) MAR, letters a) and b)[147].

It should be noted that the behaviour referred to in letter a) is further divided into two types, both subject to the same dual condition:

«*a)* *entering into a transaction, placing an order to trade or any other behaviour which:*

(i) *gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of, a financial instrument, a related spot commodity contract or an auctioned product based on emission allowances;*

[146] S. Seminara, *Il diritto penale del mercato mobiliare*, cit., p. 121.

[147] The origin of the definitions adopted by the legislator can be found in a study conducted by FESCO "Market Abuse - *FESCO's response to the call for views from the Securities Regulators under the EU's Action Plan for Financial Services*", 29 June 2000: «*Definition of Market Abuse. The objective of an European legislative framework to combat Market Abuse is to defend the integrity of the market. Market Abuse is behaviour which involves the misuse of Material Information (...), the dissemination of false or misleading information or behaviour which abnormally or artificially affects, or is likely to affect, the formation of prices or volumes of Financial Instruments. Consequently, an European regime against Market Abuse should cover: a) Misuse of Material Information in relation to Financial Instruments traded on a Regulated Market before that information has been disclosed to the public in accordance with existing disclosure requirements. Material Information can be misused: i) through trading, or ii) encouraging others to trade, or iii) through passing on the information to any third party except if such disclosure is made during the normal course of the exercise of a person's employment, profession or duties and the recipient is made aware that the information is material and has not been disclosed to the rest of the market. b) Dissemination of information which gives, or is likely to give, false or misleading signals as to the supply, demand or price of Financial Instruments traded on a Regulated Market. It will include: i) the dissemination of misleading rumours; ii) the dissemination of false or misleading news about companies; c) Trades, or orders to trade in a Regulated Market, which either: i) give, or are likely to give, false or misleading signals as to the supply, demand or price of Financial Instruments traded on a Regulated Market; or ii) Interfere with the interaction of supply and demand and produce, or is likely to produce, an abnormal or artificial effect on prices or volumes of Financial Instruments traded on Regulated Markets. (...) The definition in (...)(c) above is designed to prohibit, non exhaustively, the following conduct: a) The creation of a false or misleading appearance of trading in a Financial Instrument; b) Trading by one or more persons in collaboration with each other which has the effect of securing the market price of a Financial Instrument at an abnormal or artificial level; c) The employment of any fictitious transaction or devices or any other form of deception or contrivance; (...)*».

> *(ii) secures, or is likely to secure, the price of one or several financial instruments, a related spot commodity contract or an auctioned product based on emission allowances at an abnormal or artificial level;*
>
> *unless the person entering into a transaction, placing an order to trade or engaging in any other behaviour establishes that such transaction, order or behaviour have been carried out for legitimate reasons, and conform with an accepted market practice as established in accordance with Article 13»*.

It is observed that in the sub i) conduct, the success of the strategy relies on the reaction of other market participants who may be deceived by the "false or misleading signals" transmitted by the manipulator's conduct, thanks to orders placed or the resulting transactions. On the other hand, in the sub ii) conduct, the success of the conduct directly stems from the manipulator's forceful action, regardless of the reaction of other market participants, "fixes" the price at an "abnormal or artificial level" (finding it somehow convenient).

Both behaviours influence the price formation process.

Now, it is evident that there is an enormous amount of orders that daily influence (or, more precisely, are likely to influence) the price formation process because prices are formed in the market through the interaction of a multitude of participants who align their quotes, at least approximately, with general expectations. While certain frictions may slow down this process, it is inherently dynamic: the price that has just formed undergoes further processing by traders, who in turn react with new orders that contribute to the formation of another value, allowing for iterative convergence towards the fair value that reflects the underlying financial instrument's fundamentals, in line with publicly available information. This ensures the semi-strong informational efficiency of the market and, therefore, the allocative efficiency of resources, channelling them more easily towards investments deserving of funding.

The potential effects resulting from illicit conduct, namely "false or misleading signals" or prices at "abnormal or artificial levels" highlight the importance of a counterfactual assessment focused on the difference between what the conduct has caused and what would have happened in its absence.

Since these definitions are intentionally effect-based rather than intent-based, designed to penalize even non-intentional behaviours, references to falsehood, misleadingness, and artificiality should not presuppose the recognition of malicious conduct but rather the mere potential impact on the price formation process.

If that is the case, as it appears to be, then, as mentioned earlier, there is a great number of orders placed in the market that daily influence or could influence this process by providing false or misleading signals or by driving the price to abnormal values.

Consider the number of orders that cause significant price variations in a direction opposite to that consistent with publicly available information and that can be justified, for example, by the need for liquidity from one of the investors (liquidity trader).

Hence, to avoid the absurdity of classifying hundreds of manipulations every day, the first of the two conditions provided in Article 12, paragraph 1, letter a) comes to the rescue, «*unless the person entering into a transaction, placing an order to trade or engaging in any other behaviour establishes that such transaction, order or behaviour have been carried out for legitimate reasons (...)*»[148].

Therefore, the ability to verify the existence of legitimate reasons becomes crucial, typically including those related to arbitrage, investment, or speculation strategies.

However, the black box nature of strong AI systems inhibits the possibility of clarifying whether the conduct is justified by legitimate reasons. Hence, the relevance of the issue concerning the admissibility of trading on financial markets through strong AI systems and, if deemed acceptable, the adequacy of the trade-based manipulation definition provided by Regulation (EU) MAR.

Indeed, there is another provision capable of encompassing manipulative behaviours carried out using AI systems, whether weak or strong. This provision is found in Article 12, paragraph 1, letter b), which considers manipulative «*entering into a transaction, placing an order to trade or any other activity or behaviour which affects or is likely to affect the price of one or several financial instruments, a related spot commodity contract or an auctioned product based on emission allowances, which employs a fictitious device or any other form of deception or contrivance*».

As highlighted by scholars, however, Article 12, par. 1, letter b) «*suscita così problemi a causa della sua genericità, accresciuta dall'assenza di ogni riferimento ai potenziali effetti sul prezzo degli strumenti finanziari*»[149]; this leads to considering this provision more of a closing rule for the trade-based manipulation and to be resorted to only exceptionally.

It is true that layering and spoofing strategies (perpetuated by AI systems) have been subject to sanctions in other Anglo-Saxon jurisdictions, relying on the concept of artificiality of the conduct. However, it is evident that such an approach would not be consistent with the more comprehensive, transparent, and rigorous approach of Regulation (EU) MAR, which has proved itself well since the beginning.

It is also important to acknowledge that the approach of Regulation (EU) MAR already provides another avenue to address the trading activity of AI systems, which does not rely on defining the specific offense but on directly illustrating the manipulative example. This approach has been taken to tackle the initial manifestations of high-frequency trading by AI systems, known as High-Frequency Traders (HFT)[150].

[148] Added emphasis.

[149] The provision is not accompanied by indicators in Annex I of Regulation (EU) MAR and Annex II of Delegated Regulation (EU) 2016/522.

[150] On the characteristics of algorithmic trading, reference is made to M. Gargantini – M. Siri, *Il "prezzo dei prezzi". Una soluzione di mercato ai rischi dell'*high frequency trading*?*, in *Riv. soc.*, n. 5-6, 2019, pp. 1100 et seq., and, with regard to statistical arbitrage and latency arbitrage, to M. Bertani, Trading algoritmico *ad alta frequenza e tutela dello* slow trader, in *Analisi giur. econ.*, n. 1, 2019, p. 268. Algorithmic trading and high-frequency trading (HFT) must be explicitly considered legitimate based on the recognition received from domestic legislation, particularly Article 1, paragraphs

Article 12, par. 2, letter c) clarifies with three examples that constitute relevant manipulation: «*the placing of orders to a trading venue, including any cancellation or modification thereof, by any available means of trading, including by electronic means, such as algorithmic and high-frequency trading strategies, and which has one of the effects referred to in paragraph 1(a) or (b), by: (i) disrupting or delaying the functioning of the trading system of the trading venue or being likely to do so; (ii) making it more difficult for other persons to identify genuine orders on the trading system of the trading venue or being likely to do so, including by entering orders which result in the overloading or destabilisation of the order book; or (iii) creating or being likely to create a false or misleading signal about the supply of, or demand for, or price of, a financial instrument, in particular by entering orders to initiate or exacerbate a trend*»[151]. In addition, Annex II of Delegated Regulation (EU) 2016/522 provides specific indicators and important examples of the offenses under Article 12(1)(a) referred to as "quote stuffing", "momentum ignition", "layering and spoofing" and "smocking"[152].

However, it is the recitals (5-9) of Delegated Regulation (EU) 2016/522 that, besides clearly explaining the indicative and non-exhaustive nature of the indicators and examples of manipulative practices, and the intention to consider technological developments in the markets, specify, among other things, that: «*Certain examples of practices set out in this Regulation describe cases that are included in the notion of market manipulation or that, in some respects, refer to manipulative conduct. On the other hand, certain examples of practices may be considered legitimate if, for instance, a person who enters into transactions or issues orders to trade which may be deemed to constitute market manipulation may be able to establish that his reasons for entering into*

6-quinquies and 6-septies TUF, the concepts of which were introduced in Article 4, nos. 39 and 40, of Directive 2014/65/EU (Markets in Financial Instruments Directive, MiFID II), implementing the ESMA Guidelines on system and controls in an automated trading environment for trading platforms, investment firms, and competent authorities (ESMA/2012/122), 24 February 2012. In particular, "algorithmic trading" is defined as «la negoziazione di strumenti finanziari in cui un algoritmo informatizzato determina automaticamente i parametri individuali degli ordini, come ad esempio l'avvio dell'ordine, la relativa tempistica, il prezzo, la quantità o le modalità di gestione dell'ordine dopo l'invio, con intervento umano minimo o assente, ad esclusione dei sistemi utilizzati unicamente per trasmettere ordini a una o più sedi di negoziazione, per trattare ordini che non comportano la determinazione di parametri di negoziazione, per confermare ordini o per eseguire il regolamento delle operazioni» (Art. 1, comma 6-*quinquies*, TUF). "High-frequency algorithmic trading" is defined as «qualsiasi tecnica di negoziazione algoritmica caratterizzata da: a) infrastrutture volte a ridurre al minimo le latenze di rete e di altro genere, compresa almeno una delle strutture per l'inserimento algoritmico dell'ordine: co-ubicazione, hosting di prossimità o accesso elettronico diretto a velocità elevata; b) determinazione da parte del sistema dell'inizializzazione, generazione, trasmissione o esecuzione dell'ordine senza intervento umano per il singolo ordine o negoziazione, e c) elevato traffico infra-giornaliero di messaggi consistenti in ordini, quotazioni o cancellazioni» (Art. 1, comma 6-*septies*, TUF).

[151] Added emphasis.

[152] "*Quote suffing*": "place large quantities of buy and sell orders and/or cancel and/or update such orders to create uncertainty among other participants, slow down their process and/or mask one's own strategy". "*Momentum ignition*": "enter buy or sell orders or a series of such orders or enter into transactions or a series of transactions that are likely to initiate or accentuate a trend and to encourage other participants to accelerate or amplify that trend in order to create an opportunity to close or open a position at a favourable price". "*Layering and spoofing*": "transmit multiple or large trading orders, often with parameters different from those on one side of the trading book, to execute a trade on the other side of that book. Once such trading has taken place, orders not intended for execution are removed'. "*Smoking*": "place buy and sell orders to attract other market participants using traditional trading techniques ('slow traders'), and then quickly modify these orders by making the terms less generous, in the hope that their execution will be profitable compared to the incoming flow of slow traders' buy and sell orders". On the new commissioning methods of the offense of market manipulation, please refer to G. Cazzella, *Tecnologia e intelligenza artificiale nei mercati finanziari; le ricadute penali della "*new market manipulation*"*, Tesi di Laurea, Università Cattolica del Sacro Cuore – Milano, 2019/2020, pp. 80 et seq.

such transactions or issuing orders to trade were legitimate and in conformity with an accepted practice on the market concerned»[153].

These examples, aimed at countering potential manipulative activities by HFTs, do capture behaviours of AI systems. However, on one hand, they are not comprehensive, and on the other hand, they refer to weak AI systems. They do not address the central issue of the relationship between the legitimate use of strong AI systems and the risks associated with the difficulty of reconstructing the logical motivational basis of their transactions.

In conclusion, from an analysis of the regulations on trade-based manipulation, it becomes evident that the current regulatory framework, while commendably seeking to balance the protection of the fair price formation process and the freedom of intermediaries and investors to engage in behaviours and strategies justified by legitimate reasons, unintentionally risks inadequately supporting – and indeed, in practice, hindering – the diffusion and development of strong AI systems in financial markets. This limitation also hampers scientific and technological progress and the significant benefits they can bring to market growth and the economy.

2.3 Information-based manipulation and AI

Strong AI systems enable a disruptive expansion of potential information manipulation strategies that can be successfully employed by malicious actors. For example, consider the phenomenon of apps that generate fake news using images or human voices, creating highly realistic false information presented to the public.

These extensions naturally raise concerns that go beyond financial markets and specifically market manipulation, encompassing broader social and political issues concerning privacy, consensus formation, and the protection of vulnerable populations, as well as political leaders and public figures.

In cases of potential blatant abuses, such as the use of strong AI systems employing deepfake techniques to disseminate false information through "fake" images of influential individuals capable of orientating market participants or public opinion, the speed of response becomes crucial. It is important for the affected parties, primarily the victims but also journalists and media, to quickly disclose the error to the public, thereby limiting the duration of the impact on market prices.

In such cases, the objective attribution of the conduct to the elements of informational manipulation is typically evident, especially when accompanied by market transactions aimed at exploiting the effects on prices (note that Regulation (EU) MAR does not require market transactions to be carried out for informational manipulation to occur). The mere ability of false statements to affect markets renders them

[153] Added emphasis.

illicit and subject to sanctions, irrespective of the potentially playful nature of deepfakes or the authors' intention to manipulate the price of one or more financial instruments.

In addition to blatant cases of clear fraudulent nature, subtler instances are also of interest, where the use of AI systems induces a plurality of actors (or even a few actors holding a market power) to coordinate their behaviour, influencing security prices in a manner advantageous to the strong AI system. In such cases, it may be challenging to recognize the manipulative nature of the conduct and respond promptly to prevent a prolonged impact on prices.

The provision established in Article 12(1)(c) of Regulation (EU) MAR appears suitable for countering the hypothetical conduct described, allowing for manipulative behaviour to be addressed not only «*through the media, including the internet, or by any other means, (...) including the dissemination of rumours*».

However, the provision requires the fulfilment of the condition that «the person who made the dissemination knew, or ought to have known, that the information was false or misleading». We then come back to the difficulties already identified for a strong AI system to meet these requirements.

Therefore, a corrective intervention in the provisions of Regulation (EU) MAR seems appropriate in this regard as well.

Other situations of informational manipulation can arise "automatically" if the AI system, for example, acquires quantities in the market that trigger the obligation of disclosure of holdings under Article 120 TUF. Such messages can transmit false or misleading information as they may not correspond to the "intent" that generated the decision to trade in that direction. Once again, the strong AI system would not be able to provide reliable answers, as that intent cannot be reconstructed ex post or even "remembered."

Finally, the case of robo-advisors resurfaces, which could generate "incorrect, biased, or manifestly influenced" investment recommendations, thus falling under the indicators of manipulation as referred to in Article 12(1)(b), especially if accompanied by opportunistic transactions carried out immediately before or after the dissemination of such recommendations.

3 Market abuse offenses committed by multiple colluding AIs

The realm of trading becomes even more relevant when considering the interactions that an AI system can have with both human investors and other algorithmic traders.

First and foremost, some AI systems enjoy a more pronounced competitive element compared to any form of trading: the speed at which they can enter a significantly high volume of orders for execution, modification, or cancellation of orders in close temporal proximity. This highlights a stark disparity in capabilities between these algorithmic trades and any human investor in the financial market. Undoubtedly, the ability to manage, within fractions, milliseconds, or microseconds, the direction of investments through a multitude of orders and transactions with the intent to exploit this competitive advantage and attract the attention of other market participants, particularly slow traders, in profitable terms, evokes a greater possibility of abusive conduct[154]. However, the competitive potential does not necessarily concern "ultrafast" transactions[155], as it can seep into less rapid exchange dynamics, in which the so-called algorithmic black box processes trading decisions based on motives, calculations, and strategies that are more difficult to comprehend compared to human behaviour, even for the producer, programmer, or user of the AI system[156].

In addition to this, the use of artificial intelligence can lead human traders to devise a variety of innovative mechanisms for intervention in trading. In particular, algorithms can be used as a tool to implement, carry out, or facilitate collusive agreements among financial operators[157]. In these scenarios, collusive phenomena are easily attributable to the involved market participants.

The in-depth examination of the flash crash that occurred on May 6, 2010, in the E-Mini S&P 500 Futures already highlighted how various HFTs had responded in a similar and aggressive manner (herding) to a significant sell order placed by an institutional investor who used an algorithm to hedge against the risk associated with the Greek crisis for his positions in the US stock market. This occurred regardless of the presence of a serial manipulator, Navinder Sarao, who habitually, including on that day, set algorithms in motion that employed a layering and spoofing strategy.

Considering that algorithmic orders now make up 80% of the total trades on the most liquid financial instruments, their interaction is part of the ordinary price formation process. Therefore, from a supervisory perspective, flash crashes and manipulation transactions appear as the visible part of a phenomenon, namely algorithm interaction, which generally does not seem to pose problems.

However, as demonstrated by the case of Navinder Sarao's manipulation, supervisory action may not be swift in detecting market abuses that occur at high speeds. It is possible that within an apparent calmness of the markets, a multitude of micro-manipulations may be concealed, to the detriment of other participants, with significant effects on indicators that express market quality.

[154] In this regard, M. Bertani, Trading *algoritmico ad alta frequenza e tutela dello* slow trader, cit., *passim*, especially p. 267, extensively discusses the information asymmetry faced by slow traders in comparison to algorithmic traders. This results in a reduction of risk for the algorithmic operator and an increase in risk for the slow trader or human investor.

[155] A similar viewpoint is presented by A. Azzutti – W.G. Ring – H. S. Stiehl, *The Regulation of AI trading from an AI Life Cycle Perspective*, cit., p. 13.

[156] Regarding this risk in financial markets, V. Carlini, *I robot e le scelte oscure spesso inspiegabili per l'uomo*, in *Il Sole 24 ore*, February 21, 2018, pp. 1 and 25.

[157] This is the risk of the so-called "human-machine" association, as defined by G. Teubner, *op. cit.*, pp. 105-113.

Furthermore, when considering more advanced AI systems based on "reinforcement learning," their mutual interaction can spontaneously generate tacit collusive behaviours without initial programming[158], behaviours that cannot be attributed to humans[159]. As reported in the news, «si sono già avute istanze a Wall Street di sistemi intelligenti che, davanti alle istruzioni dei loro creatori di «massimizzare il ritorno» sugli investimenti che gestiscono, hanno autonomamente sviluppato meccanismi di collusione con altri computer [...], comportamenti che sarebbero certamente illegali se fossero stati stabiliti tra esseri umani». All of this could result in a state of *de facto* impunity, as current provisions solely sanction conscious and voluntary behaviours or, at the very least, behaviours attributable to potential negligence by producers and programmers[160].

Regarding the repression of these illicit manipulative dynamics (or more broadly abusive), just like illicit behaviours agreed upon by two or more traders, doctrine, albeit with exclusive reference to high frequency trading, has highlighted that forms of tacit algorithmic collusion inherently escape the traditional regulatory and supervisory model based on humans. In these cases, the reciprocal implications among algorithmic traders, as well as their interactions with traditional investors, are difficult to control because the interaction between traders «rischia di essere così tanto correlata che se anche uno di questi sfugga ai controlli *ex ante* e di conformità, tutti i controlli effettuati sugli altri partecipanti sino a quel momento risulterebbero essere stati vani»[161]. Particularly, even in the hypothesis where the actions of one trader can be predictable, «diviene automaticamente imprevedibile per l'impossibilità di prevedere il comportamento (non per forza ragionevole) anche degli altri partecipanti «robotici» che sarà possibile ritrovare nel mercato»[162].

[158] A definition of "tacit collusion" resulting from the use of algorithms can be found in the Organisation for Economic Co-operation and Development (OECD), *Algorithms and collusion. Competition Policy in the Digital Age*, 2017, p. 19. It specifies that tacit collusion «*refers to forms of anti-competitive co-ordination which can be achieved without any need for an explicit agreement, but which competitors are able to maintain by recognising their mutual interdependence. In a tacitly collusive context, the non-competitive outcome is achieved by each participant deciding its own profit-maximising strategy independently of its competitors. This typically occurs in transparent markets with few market players, where firms can benefit from their collective market power without entering in any explicit communication*».

[159] This risk was initially identified by scholars of competition law. With reference to antitrust enforcement issues, please refer to the following sources: M. Filippelli, *La collusione algoritmica*, in *Orizz. dir. comm.* (*orizzontideldirittocommerciale.it*), fasc. speciale, 2021, pp. 375 et seq.; P. Manzini, *Algoritmi collusivi e diritto antitrust europeo*, in *Mer. Conc. Reg.*, n. 1, 2019, pp. 163 et seq.; L. Calzolari, *La collusione fra algoritmi nell'era dei* big data*: l'imputabilità alle imprese delle "intese 4.0" ai sensi dell'art. 101 TFUE*, in *Rivista di diritto dei media* (*medialaws.eu*), n. 3, 2018, pp. 21 et seq.; G. Colangelo, *Artificial Intelligence and Anticompetitive Collusion: From the 'Meeting of Minds' towards the 'Meeting of ALgorithms'*, in *Stanford-Vienna TTLF Working Paper*, No. 74 (http://ttlf.standford.edu.). Regarding the effects of algorithmic collusion in financial markets, with particular emphasis on the stability of capital markets, refer to A. Azzutti – W.G. Ring – H. S. Stiehl, *Machine learning, market manipulation and collusion on capital markets: why the "black box" matters*, cit., who identify the market factors that can facilitate the production of algorithmic collusion (market transparency, a higher frequency of interactions, product homogeneity, market concentration, entry barriers, and innovations).

[160] Thus J. Hansen, *Ci sono anche i pc delinquenti*, in *ItaliaOggi*, 11 maggio 2019, pp. 1 e 11.

[161] P. Lucantoni, *L'*high frequency trading *nel prisma della vigilanza algoritmica del mercato*, in *Analisi giur. econ.*, n. 1, 2019, p. 311.

[162] Ibid., pp. 310-311. In the same sense, F. Di Ciommo, *La conclusione e l'esecuzione automatizzata dei contratti (*smart contract*)*, in G. Cassano – F. Di Ciommo – M. Rubino De Ritis (a cura di), *Banche, intermediari e* FinTech, Milano, 2021, p. 106, argues that the phenomenon cannot be limited to high-frequency trading but encompasses the use of various dynamic and aggressive technologies, all leading to the phenomenon of so-called ghost liquidity. In particular, it is

These concerns can certainly be extended to AI systems, whose trading mechanisms, already inscrutable, can develop collusive behaviours that cannot be detected based on autonomous relational dynamics, regardless of the speed of algorithmic trading. Such a phenomenon may not only involve illicit manipulative behaviours not attributable to humans, but also produce effects on the overall functioning of the financial sector.

4 Information-based manipulation in social networks and AI

Algorithmic trading should also be examined in relation to the potential of social media and social networks[163]. The new online platforms for news have radically changed the dissemination of information, characterized by two main features: the speed of circulation and the decentralization of information[164].

Social networks allow individuals not only to consume news but also to produce news, which is disseminated in real-time on the internet to all connected users/individuals[165]. The combination of these new communication methods with algorithmic traders can have systemic effects on the stability of the financial market. Algorithmic traders, through their ability to acquire and process all communication sources, including those derived from mass information channels, can produce a "rebound" effect on the prices of listed financial instruments. An algorithmic trader's investment decision can be based on the «numero delle volte in cui il nome dello strumento finanziario compare nei circuiti di diffusione di informazioni e sulle piattaforme di comunicazione di cui usufruiscono gli operatori»[166], without being able to identify fault signals that would deter a human trader from trading[167].

The dynamic influence of trading by social media and social networks can be exacerbated by a more invasive manifestation, namely that of mass disinformation,

possible that trading volumes surge due to two circumstances explained by the author: «1) gli automi, in un tale contesto, per minimizzare i rischi possono decidere di porre in essere strategie di brevissimo periodo (compro e vendo in pochi minuti); e 2) gli automi tra loro si condizionano inevitabilmente, sicché, se un automa decide di comprare in modo massiccio un certo titolo, gli altri automi, che raccolgono in tempo reale l'informazione sul mercato e la relativa oscillazione del prezzo, possono decidere di comprare anch'essi, quel titolo o altri titoli, e così può succedere che si determini un momento positivo di borsa ed anche che un momento positivo si trasforma in momento di euforia. Ciò genera la sensazione che nel mercato sia entrata nuova liquidità, quando invece tale liquidità non c'è, tanto che di lì a poco, in ragione della strategia di breve periodo di cui si diceva, è probabile che gli automi comincino a vendere per monetizzare il guadagno (e cioè l'aumento di prezzo del titolo) e che anche questa dinamica ribassista, per lo stesso meccanismo di condizionamento appena cennato, si produca rapidamente».

[163] It should be noted that the inherent danger of social networks is not limited to the spreading power of algorithmic traders. Reference can be made to the *Gamestop* case, in which it was not algorithmic power that disrupted the speculative dynamics of investment funds, but rather a mass of small investors whose alliance was made possible by their belonging to the same digital community. In this regard, M. Cupella, *I mercati finanziari a confronto con nuove tecnologie e Social Media: le prospettive penalistiche dell'*Affaire GameStop, in *Bocconi Legal Papers*, n. 16, 2021, pp. 145 et seq.

[164] For further insights into these aspects, extensive reference can be made to G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in *Rivista di diritto dei media* (*medialaws.eu*), n. 1, 2018, p. 22.

[165] Ibidem. See also F. Donati, *L'art. 21 della Costituzione settanta anni dopo*, in *Rivista di diritto dei media* (*medialaws.eu*), n. 1, 2018, pp. 93 et seq.

[166] M. Palmisano, *op. cit.*, p. 135.

[167] P. Lucantoni, *L'*high frequency trading *nel prisma della vigilanza algoritmica del mercato*, cit., p. 300.

which involves the dissemination of incorrect information and fake news and is considered by doctrine as «the most damaging form of market manipulation in terms of market value and investor confidence»[168]. These pieces of information are not always reliable nor attributable to an easily identifiable subject[169]. Such information could also imply "investment recommendations," triggering obligations under Regulation (EU) MAR[170] if the advertisement directly relates to financial products, especially by unregulated entities that are not subject to specific financial rules to guide investors' choices based on their knowledge and risk tolerance. Indeed, mass disinformation can constitute new forms of information manipulation, disrupt the normal interaction between supply and demand, and impact the value of financial instruments[171].

The resulting effects can be even more misleading and disruptive when this information is "captured" by trading algorithms, especially high-speed ones, leading to episodes of high volatility in financial securities (the so-called flash crashes mentioned earlier), as reported in some news stories[172]. This happens because said algorithms have the ability «di sfruttare al meglio i movimenti rapidi e spesso violenti che i mercati manifestano dopo la pubblicazione di dati macro o notizie importanti»[173].

Therefore, it is necessary to assess whether the traditional prohibition on making false statements, which applies to anyone holding a market power (managers, institutional investors, gurus, financial analysts, politicians, journalists, etc.) is adequate to counter cases of mass disinformation and, more generally, the dissemination of false or misleading information through decentralized methods.

[168] T.C.W. Lin, *The new market manipulation*, cit., pp. 1292-1294, especially p. 1293.

[169] L. Califano, *La libertà di manifestazione del pensiero … in rete; nuove frontiere di esercizio di un diritto antico.* Fake news, hate speech *e profili di responsabilità dei* social network, in *federalismi.it*, n. 26, 2021, p. 14, emphasises how news circulating online «possono (e spesso è così) non avere una paternità evidente, trattandosi di *meme*, articoli anonimi, estratti di *blog*, i cui contenuti vengono divulgati medianti strumenti quali la condivisione o il *retweet* che consentono di perpetuare l'anonimato».

[170] Article 3, paragraph 1, 35) of Regulation (EU) MAR on market abuse provides a definition of « investment recommendations» in terms of «information recommending or suggesting an investment strategy, explicitly or implicitly, concerning one or several financial instruments or the issuers, including any opinion as to the present or future value or price of such instruments, intended for distribution channels or for the public».

[171] A. Canepa, Social media e fin-influencers *come nuovi fonti di vulnerabilità digitale nell'assunzione delle decisioni di investimento*, in *Riv. trim. dir. econ.* (*fondazionecapriglione.luiss.it*), Suppl. al n. 1, 2022, pp. 307 et seq., especially pp. 311 e 321.

[172] Please refer to M. Longo, *Allarme* social network. *Così insidiano le Borse*, in *Il Sole 24 ore*, 22 marzo 2018, pp. 1 and 3. The article highlights at least four cases of fake news spread through social networks that have caused episodes of high volatility in the financial market or in certain securities. The first case involves false news in 2010 about a Qantas plane crashing in Indonesia; the second occurred in April 2013 when hackers sabotaged the Twitter account of the Associated Press and spread the false news of an attack on the White House; the third episode began in 2013 with a trader creating fake Twitter accounts for financial research companies, which disseminated false news that Sarepta Therapeutics was under investigation; the fourth case, which took place in 2009, involves false news spread by two individuals about certain stocks on the New York Stock Exchange. For the first two episodes, refer to C. Mottura, *Decisione robotica negoziale e mercati finanziari*, cit., pp. 272-274.

[173] A. Puorro, High Frequency Trading*: una panoramica*, *op. cit.*, p. 16.

Criminal law profiles III

1 The objective delimitation of market abuse offenses and AI

There is no financial crime that cannot be committed by artificial intelligence[174], and AI, when left to itself, is inclined to engage in illegal activities because it is much faster than humans in identifying favourable opportunities.

However, considering the various definitions already presented, it is not clear what artificial intelligence is[175]. This is evident from the fact that more than seventy alternative definitions have been identified[176], in addition to an 'official' one processed by the Commission in a recent proposal for AI regulation[177]. Perhaps the most well-known definition is McCarthy's, who referred to it as the science and engineering of creating intelligent machines, especially intelligent computer programs, while also speaking of intelligence as the computational part of the ability to achieve goals in a variety of ways[178]. Other definitions that have followed are undoubtedly equally effective in outlining a promising semantic core for legal reflection. For example, consider Russell and Norvig's definition, according to which an artificial agent can be characterized by «thinking like a human, acting like a human, thinking rationally, and acting rationally»[179].

What is underlying this latter definition, and what seems more important to the eyes of a criminal lawyer, has been further clarified by a simple notation by Jacob

[174] Regarding the uncertainty in defining artificial intelligence, see, J. KAPLAN, *Artificial Intelligence: What Everyone Needs to Know*, Oxford, 2016, p. 1; M.C. SCHEAU – L. ARSENE – G. POPESCU, *Artificial Intelligence/Machine Learning Challenges and Evolution*, in *Int' J. Info. Sec. Cybercrime*, Vol. 7, Issue 1, 2018, pp. 11 et seq.

[175] The fact that artificial intelligence is not a clear-cut concept is highlighted by C. BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, *op. cit.*, p. 1914.

[176] S. LEGG – M. HUTTER, *A collection of definitions of intelligence*, in *Frontiers in Artificial Intelligence and Applications*, Vol. 157, 2007, pp. 17 et seq. (https://arxiv.org).

[177] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final. The EU regulation proposal, in Article 3(1), defines an AI system as: « software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with». This definition was modified in the position elaborated by the Council of the European Union on December 6, 2022, and has taken the following literal text: «a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts».

[178] J. MCCARTHY, *What Is Artificial Intelligence?*, 12 novembre 200, (www.formalstandford.edu).

[179] S. RUSSELL – P. NORVIG, *Artificial Intelligence: A Modern Approach*, Hoboken, 2021, p. 2.

Turner, according to which the most typical characteristic of AI is its ability, despite being a non-natural entity, to make choices through an evaluation process[180]. Common features of today's known forms of artificial intelligence include the ability to detect and analyse data constituting the environment in which they operate in order to efficiently achieve the characteristic objective, which in the field of financial markets is typically identifiable as profit[181].

This propensity for deliberate choice has significant implications for a discipline that aims to regulate *ex ante* and punish *ex post* choices that do not conform to the protective options expressed by the legislator.

The oxymoron of a decision free from law and its consequences is not tolerable in the legal system, and the frustration deriving from the impotence of contemporary legislators is masked by the choice of varied and not always efficient solutions in attributing the act of the algorithm to some natural person.

The financial markets sector is certainly the one that allows us to confront the challenges of artificial intelligence more than any other because the regulated activity is already mostly carried out by nonphysical traders. Therefore, what we will say mainly applies to this sector, despite the fact that there are indeed many offenses that can be committed by an artificial agent, including even the purchase of drugs on the deep web, as demonstrated by the case of the bot shopper (specifically the *Random Darknet Shopper*, a program dedicated to online product purchasing) built for artistic purposes in 2014. Precisely thanks to the demonstration that they acted for this purpose, the programmers who had designed the exhibition were acquitted of all charges[182].

The presence of a cybernetic form of market abuse represents an initially impossible challenge for regulators because the uncertainty regarding the salient features of an artificial agent is compounded by the inaccuracy of any definition of manipulation, that is, how it can be objectively distinguished from legitimate speculative forms[183], albeit aggressive, and even the transfiguration of the characteristics of the

[180] J. Turner, *Robot Rules: Regulating Artificial Intelligenc*e, Cham, 2019, p. 16.

[181] Refer to the solid points outlined by the Committee on Artificial Intelligence of the Council of Europe, as discussed by C. Barbaro, *Lo studio di fattibilità di un nuovo quadro normativo sulla concezione, lo sviluppo e l'applicazione dei sistemi di Intelligenza Artificiale sulla base delle norme del Consiglio d'Europa. Il lavoro del Comitato ad hoc sull'intelligenza artificiale del CdE*, in *Questione Giustizia*, 28 aprile 2021, pp. 1 ss.

[182] Regarding the incident, see. M. Power, *What happens when a software bot goes on a darknet shopping spree?*, available at the following URL https://www.theguardian.com).

[183] On the ongoing difficulties in reaching a consensus in literature on the concept of manipulation, refer to A. Verstein, *Benchmark Manipulation*, *B.C. L. Rev.*, Vol. 56, 2015, pp. 272 et seq.; On the uncertainty in distinguishing between legitimate trading programs and actual disruption, see, T.E. Levens, *Comment, Too Fast, Too Frequent? High Frequency Trading and Security Class Actions*, *U. Chi. L. Rev.*, Vol. 82, 2015, pp. 1515 et seq. In the Italian context, reference can be made toF. Consulich, *La giustizia e il mercato*, Milano, 2010, 37 et seq.

financial market. In fact, we have long been witnessing a true Balkanization of exchanges[184] because even the venue where supply and demand meet, once institutionalized, is a disputed asset subject to competition among market participants, undergoing relentless evolution in search of the best efficiency for "client" transactions.

In a context where every landmark is in motion, externalities concentrate on the subjects least responsive to changes, a characteristic that tends to coincide with small investors or slow traders. This is a recurring observation, starting from Michael Lewis's work, *Flash Boys*[185].

As market entropy increases, the competitive advantage of those who make speed of decision their defining characteristic, namely high-frequency trading algorithms, also increases. However, it should be clear that these algorithms do not exhaust the forms of artificial intelligence's manifestation in markets and in the application of artificial intelligence in various social contexts.

Therefore, the preventive/repressive action made possible by criminal provisions in financial markets must adapt to the changing criminological scenario, as confirmed by the SEC itself, which has defined high-frequency trading as one of the most significant developments in market structure in recent years[186].

With this clarification, in order to delimit the scope of the investigation as accurately as possible, it is clear that the quintessential crime that can be perpetrated by means of artificial intelligence (and not by artificial intelligence itself) is market manipulation. The use of algorithms has facilitated the execution of common manipulative techniques and has also allowed for the development of new forms that necessarily require the use of high-frequency trading. The expression "by means of" must therefore be somewhat reconsidered: it should not be understood purely mechanistically, but rather with an awareness of creative instrumentality, in which humans lay the groundwork and establish a desired result in terms of the kind or class of events they wish to produce, and the artificial agent bridges the gap between the initial conditions and the final outcome in non-predefined ways. It is evident that an intelligent system can learn and even "invent" new techniques and opportunities to disrupt trading and the prices of listed instruments. The analysis does not encompass cases where market distortion occurs accidentally, due to an algorithm's misinterpretation of reality or its lack of information, which objectively influences its choices and renders them manipulative. This latter hypothesis falls outside the realm of legally relevant matters, not because of the lack of intentionality on the part of artificial intelligence (which lacks psychological connotations) but rather due to the involvement of a natural person

[184] The expression is from T.C.W. Lin, *The new market manipulation*, cit., p. 1296. On the inadequacy of regulations in financially advanced countries regarding cybernetic distortion of trades, see J.W. Markham, *Law Enforcement and the History of Financial Market Manipulation*, New York, 2014, 390-91; G. Scopino, *Do Automated Trading Systems Dream of Manipulating the Price of Futures Contracts? Policing Markets for Improper Trading Practices by Algorithmic Robots*, in *Florida L. Rev.*, Vol. 67, 2015, pp. 221, 222-24; Y. Yadav, *The Failure of Liability in Modern Markets*, in *Virginia L. Rev. Ass.*, Vol. 102, 2016, pp. 1031, 1034-39.

[185] M. Lewis, *Flash Boys: A Wall Street Revolt*, New York-London, 2014, p. 171.

[186] Staff of the Division of Trading and Markets, Equity Market Structure Literature Review: Part 11; High Frequency Trading, 4 (18 marzo 2014), avalaible in http://perma.cc.

who employs it. In this case, we are dealing with negligent manipulation, which is only administratively relevant if there is a failure by the human operator to prevent predictable errors by the computer system.

It is clear that the financial sector is an elective field for study given the existing regulatory implications, practical emergencies, and scholarly reflections. The legislator has exerted its normative force most prominently in the field of finance (although certainly not exclusively[187]). However, whether it has met the necessary requirements is a separate issue, as ongoing examples of harmful manifestations of artificial intelligence demonstrate[188]. Moreover, it should be noted incidentally that the transversal dimension of the risks associated with artificial intelligence (perceived even by non-experts[189]) has now led to reflection on a horizontal discipline that provides protection in non-financial sectors of public and private importance[190].

At this point, we programmatically set aside the opposite case from what has been considered so far, namely the one in which the artificial intelligence system is not deceiving but is deceived. Even the new algorithms of artificial intelligence that trade automatically in the market can detect artificially induced changes solicited by speculators, thereby running the risk of being misled. From a criminological perspective, however, this hypothesis does not have distinct peculiarities compared to cases where human traders are the victims. The only difference is that the deception suffered by a high-frequency trading algorithm can result in a significantly greater number of transactional acts performed due to the error, leading to more severe damage[191].

2 The areas of criminal relevance of artificial intelligence in the financial domain

As illustrated above, from a punitive perspective, the classification of reproved behaviours refers to Articles 184 and 185 TUF in the criminal realm, as well as Articles 187-*bis* and 187-*ter* TUF in the administrative realm.

[187] Certainly, outside the realm of market regulations, Article 22 of EU Regulation 2016/679 (GDPR) should be mentioned, which states in paragraph 1: «The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her».

[188] See the incident that occurred on the major European stock exchanges in early May 2022, as discussed by M. Sabella, Flash crash *in Borsa, l'algoritmo che affonda Piazza Affari per 5 minuti: cos'è successo*, in *Corriere della sera*, 2 maggio 2022.

[189] For example, refer to the considerations of J. Hansen, *op. cit.*, as well as the case described by A. Lana, *Alexa sfida una bimba a inserire una moneta nella presa elettrica: Amazon aggiorna il* software, in *Corriere della sera*, 29 dicembre 2021.

[190] The reference is made to the aforementioned Proposal for a Regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, available at the following url: https://eur-lex.europa.eu

[191] On the other hand, despite its name, artificial intelligence often lacks perspicacity and is devoid of common sense, leading to its being dubbed "artificial stupidity" by P. Domigos, *The Master Algorithm*, New York, 2015, pp. 23 et seq., 57 et seq. Regarding the biases affecting AI, see S. Barocas – A.D. Selbst, *Big Data's disparate impact*, in *Cal. Law Rev.*, Vol. 104, 2016, pp. 671 et seq.

It is not surprising that the reference also extends to insider trading, not only to mere market manipulation. Indeed, it is more likely that the non-human agent commits the latter offense, but it is also conceivable that it creates and then abuses insider information based on the analytical and data processing capabilities that the algorithmic operator possesses to a significantly greater extent than human intermediaries. By definition, the artificial agent knows more than a human and therefore acts with more information. Of course, this refers to information circulating on the network and with a digital dimension, as well as information derived from the combined analysis of these sources. It does not encompass information confined to confidential relationships between individuals, insider tips given directly to an investor, or other strictly private phenomena occurring off the record, which are inaccessible to AI that trades in binary code and feeds on bytes (and their multiples)[192].

There is another aspect to consider in understanding why reference must be made to Articles 184/187-*bis* TUF. The algorithmic trader can gain access to information from the financial institution to which it belongs and then utilize it for its own benefit autonomously. If not adequately supervised, nothing prevents the program from interfacing with the structure that holds confidential data and infiltrating its most hidden folds. Its autonomy should not be understood merely as automation or the ability to perform a task without human intervention, but as independence from external instructions and freedom from the determinations of others. This unpredictability in its interactions with the surrounding environment, which it tends to adapt to or seeks to modify[193], renders it capable of behaving like the canniest raiders, taking advantage of data stolen from the organization it belongs to, eluding any control.

While the relevance of malicious artificial intelligence in market manipulation is already evident based on existing cases, its impact on insider trading is not as prominent. However, a few words are enough to clarify the issue. Consider the current structure of financial information in relation to the role played by artificial intelligence in the trading system.

The financial market is the paradigmatic example of situational uncertainty in which everyone is compelled to act. According to some, the presence of artificial agents prevents human operators from having well-founded expectations of behaviour[194]. In the face of anonymous transactions, it is not possible to determine who represents the counterparty, whether it is human or digital, nor objectively understand the basis on which the algorithmic operator will decide to act and in which direction. With the advent of artificial agents, one could move away from the model, already somewhat idealistic, of a level playing field, which is the goal of the entire anti-insider

[192] For the point, refer to F. Annunziata, *Artificial intelligence and market abuse legislation. A European perspective*, cit., pp. 6 and 114.

[193] The concept of autonomy has recently been used to structure a taxonomy of types of artificial intelligence and interaction between physical and artificial agents by M. Simmler – R. Frischknecht, *A taxonomy of human–machine collaboration: capturing automation and technical autonomy*, in *Ai & Society*, Vol. 36, 2021, pp. 239 et seq.

[194] About this S.R. McNamara, *The Law and Ethics of High-Frequency Trading*, in *Minn. J.L. Sci. & Tech.*, Vol. 17, Issue 1, 2016, pp. 135 et seq.

trading discipline[195]. The uneven distribution of information characterizes financial market transactions, but regulations are in place to prohibit the use of non-public information and to allow all investors who wish to do so to access publicly available information at reasonable costs.

Another consideration arises. One must not be misled by a form of synecdoche that equates the whole (artificial intelligence) with one of its specific manifestations (high-frequency trading algorithms), no matter how commonplace it may be.

Studies conducted by ESMA highlight how, starting mainly from 2018, there has been a 50-70% increase in algorithmic trading in the European stock market (with lower impact in the bond and derivatives sectors)[196]. Regarding the national context, trades attributable to High-Frequency Traders in the Electronic Stock Market (MTA) accounted for around 30% of total concluded trades from 2016 to 2019, with a decrease to 26% in the last reference year[197].

This is not the appropriate forum to typify the manipulative conduct made possible by HFT technology, not only because it has already been carried out in practice and addressed by previous authors[198], but also because high-frequency algorithms are now better-known and studied forms of non-human intelligence. However, there are other artificial authors that can disrupt trades, about which little has been said in the field of criminal law applied to economics and on which it is advisable to reflect.

In the field of so-called *Fintech* (an ever-evolving label), in addition to high-frequency trading, the main areas of application include unregulated exchange platforms, which in combination with the influence of social media can produce significant distorting effects on trades.

We are operating on a level where trading intertwines with communication since social media can be a place of exchange or a place for discussion regarding exchange matters.

Hence the dual role of artificial intelligence tools, as they can be used not only as vectors for manipulative transactions but also to spread false news and thus influence the prices of securities from outside the market. In particular, through so-called "bots" (autonomous programs operating on the network), untrue information

[195] Consider the remarks on this concept by Z.J. GUBLER, *Reconsidering the Institutional Design of Federal Securities Regulation*, in *William Mary L. Rev.*, Vol. 56, Issue 2, 2014, pp. 409, 424-26. The case of *Sec. Exch. Comm'n v. Texas Gulf Sulphur Co.*, 401 F.2d 833, 852 (2d Cir. 1968) is fundamental in jurisprudence, repeatedly emphasizing that the purpose of securities legislation is that "all members of the investing public should be subject to identical market risks." Regarding the difficulty of aligning the reality of markets with the political-criminal ideal, consider the skeptical position of the judiciary in *United States v. O'Hagan*, 521 U.S. 642, 658 (1997): «*Although informational disparity is inevitable in the securities markets, investors likely would hesitate to venture their capital in a market where trading based on misappropriated non public information is unchecked by law*».

[196] ESMA, Consultation Paper. MiFID II/MiFIR review report on Algorithmic Trading, 18 dicembre 2020, reperibile in https://www.esma.europa.eu, 21.

[197] Cfr. CONSOB – Commissione Nazionale per le Società e la Borsa, "Relazione per l'anno 2019", 31 marzo 2020, https://www.consob.it

[198] Recently, a taxonomy has been outlined by G. RUTA, *op. cit.*, pp. 65 et seq., previously we had dealt with it ourselves F. CONSULICH, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, cit., pp. 195 et seq.

about listed companies can be repeated multiple times and influence the sentiment surrounding the company itself or a financial instrument.

Recent events, which reached their peak in late January 2021, have demonstrated how a very high volatility of certain US stocks, linked to a significant accumulation of short positions, was induced by a generally consistent behaviour of retail investors. Influenced and limited in their behavioural options by information shared on social media, they moved as if they were a single centre of interest[199].

Phenomena of investment conditioning are more frequent when exchanges become deinstitutionalized, such as when they are placed on trading platforms[200]. Accessible through simple applications dedicated to mobile devices, they expose retail customers to a pincer manoeuvre: on one hand, they provide investment advice, and on the other hand, after a few clicks, customers can easily start making investments[201].

These phenomena also occur in the case of online advice provided by robo-advisors, before and regardless of the provision of an infrastructure for conducting trades.

The issue of the impact of social media and unregulated platforms on trading operations is closely linked, as seen, to the realization of online advice that can affect investors' decisions potentially beyond any control.

In this regard, it should be noted that in August 2021, the SEC launched a public request for information regarding the use of digital platforms for investments, online brokers, and robo-advisors[202].

It is clear, therefore, that the criminal offenses likely to be impacted by artificial agency in the coming years are those of financial abuse, considering what has just been observed, as well as insider trading and market manipulation.

[199] For a reasoned reflection on this point, in our doctrine, refer to G. Ruta, *op. cit.*, 61 ss.

[200] The "trading platform" is not a "trading venue." It is neither a multilateral trading facility (MTF) nor an organized trading facility (OTF), let alone a regulated market. Instead, it is a computer tool integrated into the structure of authorized broker/dealers, which they use in their interaction with clients and to route order flow to trading venues and/or counterparties through algorithms that identify the best conditions for subsequent execution.

[201] Both ESMA and CONSOB have already focused their attention on this phenomenon due to the potential risk it poses in terms of manipulation by insufficiently informed investors. See ESMA's statement, February 17, 2021, at [https://www.esma.europa.eu], and CONSOB's "Dichiarazione sui casi di anomala volatilità nella negoziazione di azioni e nell'utilizzo di social forum e piattaforme di trading online" resa dalla Consob e rinvenibile in https://www.consob.it.

[202] The text can be found at [https://sec.gov/rules/other/2021/34-92766.pdf]. Specifically, the SECURITIES AND EXCHANGE COMMISSION has requested information and public comments on issues related to broker-dealers and investment advisors, the use of digital engagement practices including behavioural prompts, differential marketing, game-like features (this is referred to as the gamification of investment), and other design elements or functionalities to interact with retail investors on digital platforms (e.g., websites, portals, and applications), as well as the tools and technological analytical methods used in connection with these digital engagement practices. It also seeks input on the use of technology by an investment adviser to develop and provide investment advice.

3 Technological asymmetries and corporate information

It has always been believed that the relevance of high-frequency trading (HFT) was limited to market manipulation phenomena, but upon closer analysis, it must be noted that such a perspective is likely to prove partial.

We must start with the observation that HFT exploits every possible price fluctuation of listed securities. For this reason, it could be said that algorithmic traders only focus on numerical variations in stock prices, making investment choices indifferent to the fundamental value of financial instruments[203].

The first paradox encountered when reflecting on the relationship between high-frequency algorithms and markets is that these entities, despite conducting a significant portion of trades in listed securities, are influenced to a negligible extent or entirely unaffected by available data regarding the financial instruments being traded, their issuers, or the market in general. In fact, the extremely short time horizon of their positions makes it unlikely that they would benefit from such information. On the contrary, if there is a risk of being affected by such information, they prefer to withdraw[204]. In summary, financial and macroeconomic information is a negligible variable for a substantial portion of market participants, specifically high-frequency algorithmic traders.

The sensitivity of HFT to informational flows concerning individual financial instruments or general market trends depends on the type of algorithm used to determine buying and selling decisions.

Given this, it is inevitable to question the impact that the invasive presence of algorithmic operators in high and low-frequency financial trading may have on the notion of financial information, including the transformation of the reasonable investor concept. This could potentially challenge the pillars of criminal protection against market abuse.

The question is similar to the concern that arises when imagining, from a sociological standpoint, that a few major intermediaries can manipulate market trends at their will, compromising the "democracy of the markets" which, “voting” every day, assigns proper value to various activities. It is also similar to the recent concern raised in economic and financial literature when noting that globally, a few large institutional investors hold positions capable of influencing major public companies and, therefore, the real economy of the planet[205].

[203] It must be acknowledged that this characteristic is also present in some non-algorithmic investors such as day traders, market makers, and so on, but while for the latter, it is a possible attitude, for HFT (High-Frequency Trading), it is a constant structural feature.

[204] Numerous empirical studies have shown that the activity of HFT significantly slows down in the minutes e where macroeconomic information is expected to be released (AMF, *Study of the behaviour of high frequency traders in Euronext Paris*, Risks & Trends, January 2017, p. 12).

[205] A. Haldane, *The age of asset management? Speech at the London Business School* 4.4, 2014; M. Backus – C. Conlon – M. Sinkinson, *The common ownership hypothesis: Theory and evidence*, in *Economic Studies at Brookings*, January 2019.

However, the question becomes significantly more disturbing. While evaluations by these intermediaries and institutional investors must be somewhat tied, anthropologically speaking, to an estimation of fundamentals, which although highly subjective, elitist, or convenient, can hardly be purely arbitrary, at least because it must be accompanied by persuasive narratives, the evaluations generated by algorithmic operators can truly be arbitrary or reasonably appear so. This is because these operators willingly reject financial information but remain ready to massively invest in the direction indicated by an incomprehensible neural network or, as seen above, by multiple neural networks that unintentionally coordinate their responses to the same inputs. Consequently, they provide the public with financial information that lacks value-based content or, if such content exists, cannot be adequately represented, told, and ultimately appreciated or criticized.

3.1 The current profile of the reasonable investor and the competence 'trap': in search of financial information in contemporary markets

The law of the financial market is based on the assumption that relevant information is what motivates the reasonable investor to take action, forming the foundation of their determinations.

Currently, the correlation is in a state of deadlock because, as known, the notion of the reasonable investor is quite contentious. It is challenging to find a point of agreement within the universe of authors who have dealt with the subject[206]. Many, especially from the US perspective, indicate that although we are dealing with an anonymous and elusive figure, the most credited description of this subject should be that of a neoclassical *homo economicus*[207], embodying the characteristics of a long-term investor rather than a short trader[208].

Others argue that the paradigm is entirely unrealistic and therefore futile. It would be better to encourage the emergence of a new hermeneutic model of financial markets, that of the irrational investor, who does not fully comprehend financial information, is influenced by irrelevant factors, and is driven by emotions and biases[209].

[206] Among the myths of the securities market, the notions of the average investor and the reasonable investor are fully included. References include: H. Kripke, *The Mith of Informed Layman*, in *Bus. Law.*, Vol. 2, n. 2, 1973, pp. 631 et seq.; more recently,B. Black, *Behavioral Economics and Investor Protection: Reasonable Investors, Efficient Markets*, in *Loyola U. Chi. L. J.*, Vol. 44, 2013, pp. 1494 et seq.

[207] In this sense see J. MacLeod Heminway, *Female Investors and Secuities Fraud: Is the Reasonable Investor a Women?*, in *Wm. & Mary J. Women & L.*, Vol. 15, 2009, p. 297; P.H. Huang, *Moody Investing and the Supreme Court: Rethinking the Materiality of Information and the Reasonableness of Investors*, in *Sup. Ct. Econ. Rev.*, Vol. 13, 2005, p. 111; C. Rodriguez-Sickert, *Homo Economicus*, in *J. Peil - I. Van Staveren* (eds), *Handbook of Economics and Ethics*, The Hague, 2009, p. 223.

[208] Thus T.C.W. Lin, *The New Investor*, in *UCLA L. Rev.*, Vol. 60, 2013, p. 695.

[209] On this point see E.M. Kerjan, *An Idea Whose Time Has Come*, in E.M. Kerjan, *The Irrational Economist: Making Decisions in a Dangerous Word*, New York, 2010, pp. 3 ss.; T.C.W. Lin, *The New Investor*, cit., pp. 696 et seq.

Efforts have been made to reconcile this radical dichotomy through a new explanatory framework, that of the 'investor without qualities'. This investor is structurally better informed than a casual and irrational investor but certainly not capable of mastering the vast amount of data he receives. With increasing technological support, this operator makes investment decisions faster but is not immune to unmediated imitative impulses, especially in certain market scenarios (such as massive index crashes or sudden surges in stock prices). Despite attempting to diversify his investments, still he is aware of his emotional limitations[210].

What is certain is that a monolithic notion of the reasonable investor lacks any informative content regarding the reality of financial markets and risks diverting criminal protection from actual needs, generating unsatisfactory discipline with respect to both the protection claims of professional investors (in some way underestimated in their abilities) and to small investors claims of protection (overestimating their competences)[211].

This already problematic scenario is further stressed by the growing role played by algorithmic operators in recent years. Disregarding their consideration risks constructing an even more mythical and elusive notion of the reasonable investor, if understood as the personification of information expectations held by individual and occasional counterparty initiates. These subjects can be as heterogeneous as human operators in terms of pursued objectives, initial knowledge, and specific competencies, making it challenging to create a synthesis figure that parameterises the qualities of privileged information[212].

Often, the investment decision is the result of the unpredictable 'interaction' between the intrinsic characteristics of the information and the knowledge possessed by the recipient who becomes aware of it. Article 181, paragraph 4, TUF, also in light of EU legislation (particularly Article 7, paragraph 4, of Regulation (EU) MAR), clearly indicates that privileged information is one of the elements, but not the only one, that

[210] For a summary of these attributes of the modern investor, making them resemble a "*modest cyborg*", see T.C.W. Lin, *The New Investor*, cit., pp. 700 et seq.

[211] In light of these remarks, although it goes beyond the scope of this contribution, it is worth noting that, *de lege ferenda*, the legislator should perhaps structure the regulation of financial markets with an awareness of the existence of at least three major classes of investors, in order to establish a realistic criminal protection that is more faithful to the empirical basis of reference and the protection needs that emerge from it.

[212] For an analysis of the notion of the reasonable investor in light of the recent interventions of the European legislator on the subject, see F. Consulich – F. Mucciarelli, *Informazione e tutela penale dei mercati finanziari nello specchio della normativa eurounitaria sugli abusi di mercato*, in *Soc.*, n. 2, 2016, pp. 179 et seq. In the vast literature on the subject, it is worth noting, quite curiously, a series of recent contributions that, in the US literature, question the adequacy of the concept from its roots considering the diversification of skills among investors. See T.C.W. Lin, *Vistas of Finance*, in *UCLA L. Rev. Disc.*, Vol. 61, 2013, pp. 78 et seq.; Id., *The New Investor*, cit.; S.M. Bainbridge, *The New Investor Cliffhanger*, in *UCLA L. Rev. Disc.*, Vol. 61, 2013, pp. 678 et seq.; B. Black, *Behavioral Economics and Investor Protection: Reasonable Investors, Efficient Markets*, in *Loy. U. Chi. L.J.*, Vol. 44, 2013, pp. 1493 et seq.; J. MacLeod Heminway, *op. cit.*, pp. 291, 297. defines the reasonable investor as one of the core concepts of financial market regulation D.A. Hoffman, *The "Duty" to Be a Rational Shareholder*, in *Minn. L. Rev.*, Vol. 90, 2006, pp. 537, 537-39. For recent jurisprudential survey, see T.M. Madden, *Significance and the Materiality Tautology*, in *J. Bus. & Tech. L.*, Vol. 10, 2015, pp. 217 et seq.

the reasonable investor can base their decisions on, even if the news alone would not have had sufficient strength to determine an investment decision[213].

An immediate correlation of direct proportionality can be observed: as the capabilities and knowledge of the operator acquiring the information increase, the number of pieces of information that are irrelevant for an average investor, particularly unqualified ones, but highly significant for the investment choices of hyper-competent investors, also increases. These hyper-competent investors can grasp the importance of seemingly negligible information[214]. On the other hand, it should be noted that the reasonable investor is not the average investor, so price-sensitive information can indeed be relevant only to a minority of investors if it has the power to influence prices[215].

From here, the premises of a true "anaphylaxis" for market law can be glimpsed. If greater competence leads to the genesis of new privileged information, it is easy to see what can happen with a subject endowed with analytical capabilities incomparably superior to those of any human professional operator, such as a second-generation algorithmic operator: the uncontrollable expansion of information's price sensitivity, and thus the notion of privileged information, resulting in a proliferation of opportunities for its abuse[216].

This issue has already arisen globally with the rise of hedge funds, which, with their sophisticated analysis and valuation capabilities of seemingly overlooked information, data, and aspects for many financial analysts and listed companies themselves, manage to achieve substantial profits. The regulatory solution in the United States and the European Union has been to require companies to disclose any information provided in bilateral or restricted meetings[217].

It should be noted that these obligations for issuers entail new burdens: identifying and managing such informational details to prevent them from selectively reaching hedge funds.

Now, with the advent of big data and alternative data, that is, with the availability of an enormous amount of detailed data and information on a global scale, the profit possibilities for algorithmic trading strategies based on hidden correlations among such detailed information significantly increase. This, in turn, imposes new obligations on listed companies that intend to comply (voluntarily?) with the rules of fair

[213] On this point, see S. Seminara, *Disclose or Abstain? La nozione di informazione privilegiata tra obblighi di comunicazione al pubblico e divieti di* insider trading*. Riflessioni sulla determinatezza delle fattispecie sanzionatorie*, in *Banca borsa tit. cred.*, n. 3, 2008, p. 337, and F. Mucciarelli, *Sub art. 184*, in M. Fratini – G. Gasparri (a cura di), *Il testo unico della finanza*, Torino, 2012, p. 2338.

[214] In this sense, for example, see F. Denozza, *La nozione di informazione privilegiata tra "*Shareholder Value*" e "*Socially Responsible Investing*"*, in *Giur. comm.*, n. 5, 2005, pp. 593 et seq., and F. Annunziata, *Abusi di mercato e tutela del risparmio*, Torino, 2006, 15. G. Strampelli, *L'informazione societaria*, cit., p. 1037, points out that even information considered price sensitive only by a minority of investors should be subject to disclosure if those investors are capable of influencing prices through their conduct.

[215] Referring to F. Consulich – F. Mucciarelli, *Informazione e tutela penale dei mercati finanziari nello specchio della normativa eurounitaria sugli abusi di mercato*, cit., pp. 184 et seq.

[216] The point is noted by G. Strampelli, *L'informazione societaria*, cit., p. 1038.

[217] Art. 17, par. 8, MAR.

disclosure towards the investment world. Information such as the number of hours worked in a geographical area, the energy consumption of a facility, the daily number of acquired customers at various points of sale, etc., could be well-utilized to extract trends and predict the quarterly results of a listed company or a sector or sectors belonging to the same supply chain.

The expansion of price-sensitive information can thus quickly lead to an unruly hypertrophy of communication and abstention duties that substantiate the regulation of insider trading, burdening market participants with so many obligations that it becomes impossible to carry out any economic transaction without rational justification, considering that the information considered by algorithms is often devoid of economic relevance and pertains, for example, to occasional and rapid price disparities between supply and demand for a security, which otherwise have minimal value.

Consider again what would happen if the obligation to communicate or engage in fair disclosure or the prohibition on trading were imposed regarding entirely negligible information, yet relevant only to algorithms, such as the recurrence of a specific word or group of terms within market information systems.

One of the most well-known phenomena of high-frequency trading is the so-called "trading on news," which can be executed by exploiting the continuous flow of information from major financial news services. HFT can associate a trading strategy with specific groups of words that are statistically correlated with a precise trend in trading, both positive and negative, adapting strategies according to the resonance of the news, for example, by quantifying how many times the news is reported in information systems[218].

Therefore, the increase in operators' analytical competence can trap the anti-insider trading discipline: it leads to the emergence of relevant information (which is crucial for high-frequency algorithmic intermediaries) but not reasonable since it is entirely independent of economic assessment of the negotiated object.

The effect of algorithmic operators entering financial information, with particular reference to the notion of privileged information, is easily understood: the emergence of price-sensitive information, capable of influencing prices because it is important for HFT, but not reasonable since it (even if only seemingly so) lacks economic quality and may not be (as far as known) correlated to the value of the security, the issuer's structure, or the market conditions.

3.2 The emergence of price-sensitive but not reasonable information

HFTs, as well as low-frequency deep learning systems[219], interact with the concept of information in two ways:

[218] On *trading on news* see for example A. Puorro, *op. cit.*, p. 16.

[219] Deep learning is a subcategory of machine learning that refers to the branch of artificial intelligence that uses algorithms inspired by the structure and function of the brain. We are dealing here with true artificial neural networks,

1) They discover new information: they are information producers and, for this reason, they create opportunities for front running based on informational asymmetries resulting from their greater analytical and operational capabilities[220]. Second-generation algorithms are able to process a vast amount of data, accessing computerized news dissemination circuits, and thus create new market scenarios of which they become aware before anyone else. The concept of an insider is often associated with individuals who are occasionally involved in the production of privileged information due to their temporary position of advantage. Algorithmic traders, on the other hand, fall into the category of structural insiders, as they exist with the characteristics of data acquisition and processing that distinguish them[221];

2) They often employ information that may be economically irrelevant for "physical" investors, assuming it is financially significant: they are information consumers.

As mentioned in paragraphs 3 and 3.1, second-generation algorithmic traders, due to the nature of their numerous non-informative transactions (often resembling market spasms rather than deliberate actions), do not convey significant information[222] regarding the intrinsic value of the traded securities. Consequently, the postulate of contemporary financial market law, which assumes that investor behaviour carries information and provides useful context for reasonable observers, risks falling apart. The withdrawal of "ordinary" investors from markets perceived as dominated by structurally "different" operators is a concrete risk[223].

As previously stated, HFTs rely on quantitative mathematical analyses related to the fluctuations of financial instruments within a given period or the frequency of the issuer's name in industry news outlets. These may be completely inconsequential pieces of information in terms of variables relevant to professional traders. Generally, HFTs have no long-term perspective but aim to profit from very short-term movements

which are used, for example, in programs for automatic speech recognition, natural language processing, audio recognition, and bioinformatics.

[220] For an in-depth study on a predatory model of HFT (*High-Frequency Trading*) based on front running, which refers to the ability of HFT to act before other traders by taking advantage of early knowledge of a large buy or sell order in the market due to their faster information acquisition and processing capabilities compared to other traders, see J. Adrian, *Informational Inequality? How High Frequency Traders use premier access to information to prey on institutional investors*, in *Duke L. & Techn. Rev.*, Vol. 14, n. 1, 2016, pp. 261 et seq., and more recently N.E. Sokol, *High Frequency Litigation: SEC Responses to High Frequency Trading as a Case Study in Misplaced Regulatory Priorities*, in *Science and Techn. L. Rev.*, Vol. 17, n. 2, 2016, p. 421. Già nel 2010 M.J. McGowan, *The Rise of Computerized High Frequency Trading: Use and Controversy*, in *Duke L. & Techn. Rev.*, Vol. 9, 2010, pp. 1-25, pointed out the link between price volatility and predatory strategies of HFT, which result in irrational lower or higher buying or selling prices.

[221] On the presence of "Structural insiders" in markets affected by algorithmic trading, see Y. Yadav, *Insider Trading and Market Structure*, in *UCLA L. Rev.*, Vol. 63, 2016, pp. 978 et seq., 1013 et seq., which highlights (1032) how the concurrent regulation of insider trading is now deeply challenged by algorithmic operators who, while providing certain benefits to trading, also cause damages similar to conventional insider trading conducted by individuals. Other types of structural insiders may include intermediaries executing large-scale orders, advisors in M&A transactions, and top managers of publicly traded companies.

[222] This point is well addressed, for example, in G. Strampelli, *L'informazione societaria*, cit., p. 998, and H.T.C. Hu, *Too Complex to Depict? Innovation, 'Pure Information,' and the SEC Disclosure Paradigm*, in *Texas L. Rev.*, Vol. 90, n. 7, 2012, pp. 1705 et seq. Regarding the theory that markets represent the most efficient tool for aggregating dispersed information among participants, see F.A. Hayek, *The Use of Knowledge in Society*, in *The Amer. Econ. Rev.*, Vol. 35, n. 4, 1945, pp. 519-211.

[223] On this point, see T.C.W. Lin, *Reasonable Investor(s)*, in *Boston Univ. L. Rev.*, Vol. 95, 2015, pp. 461 et seq.

in a security, exploiting anticipation without considering the issuer's growth prospects or market fundamentals. However, one must refrain from making overly categorical statements, as a well-regulated artificial intelligence could undoubtedly contribute to greater allocative efficiency in markets. Nevertheless, the risk remains that if professional traders imitate algorithms, it may lead to an overall degradation in the quality of transactions, deviating the exchange price from the intrinsic value of securities[224].

The problem is well known to financial market participants, to the extent that, in order to avoid being captured and imitated by high-frequency algorithms, they increasingly tend to distance themselves from institutional markets and operate in low-transparency trading platforms, such as dark pools. In these platforms, participants are not obliged to disclose a series of pre-trading data or any information that could provide insight into their trading strategy[225].

It is evident that the massive presence of algorithmic traders may require the implementation of specific regulations different from those currently adopted by national legislators, as they are based on different principles.

Therefore, it is appropriate to reflect, *de lege ferenda*, on the introduction of legislation specifically aimed at regulating the responsibility arising from the use of such tools and governing their trading activities. This reflection should take into account:

i) The difficulty of adopting an all-encompassing notion of a reasonable investor to define the information obligations for issuers, due to the granularity of information relevant to algorithmic trading.

ii) The unknown "reasoning" that leads strong AI systems to value certain information in their trading activity and the difficulty of retrospectively understanding this reasoning.

iii) The potential dissociation between market action and financial information, considering: i) the ability of HFT, in particular, to "separate" the transaction from the information, hindering the process of incorporating available information into prices (according to the theoretical notion of efficient capital markets hypothesis), and ii) the progressive dominance of AI systems in financial markets[226].

[224] Also see H.T.C. Hu, *Too Complex to Depict?*, cit., p. 1707.

[225] On the phenomenon, see G. Strampelli, *L'informazione societaria*, cit., p. 1000; more recently, J. Adrian, *op. cit.*, p. 264; previously, the fundamental contribution of M.J. McGowan, *op. cit.*, p. 38, who estimated, already in 2010, the existence of 40 operational dark pools; Brown, Chasing the Same Signals, cit., p. 116. Also, T.C.W. Lin, *The New Investor*, cit., p. 690 et seq., and more recently, on the challenge for regulators posed by the presence of so-called *private electronic venues*, Id., *The New Market Manipulation*, cit.

[226] Reference is made to the essential contribution of E.F. Fama, *Efficient Capital Markets. A Review of Theory and Empirical Work*, in *Journal of Finance*, Vol. 25, 1970, pp. 373 et seq.; on the ability of HFT to disrupt the assimilation process of financial information into prices, see Z. Goshen – G. Parchomovsky, *The Essential Role of Securities Regulation*, in *Duke L.J.*, Vol. 55, 2006, pp. 733 et seq.

4 The role of criminal law in regulating artificial intelligence

Given the significant risks faced by investors interacting with artificial intelligence (often not even perceived by potential victims), there have been calls from various international and domestic sources for the legal system to impose stricter control, including the use of criminal law[227].

However, the perspective of criminal law is far from easy to adopt. Its emphasis on personal responsibility for the harm caused by criminal acts and the principles of protection that characterize it (at least in democratic systems) prove incompatible with the phenomenon of offenses against investments. This poses a challenging task for contemporary legislators, requiring a thorough examination to determine whether these obstacles can be overcome, albeit with great difficulty, or whether they are unpassable.

It is important to address these hindrances (declined in the plural) not only because they are numerous but also because they have different nature and structure depending on the legal position taken regarding a fundamental choice. Before considering a criminal intervention, it is necessary to resolve a fundamental question: whether the artificial agent is capable of legal responsibility, not only in the strictly criminal sense.

4.1 The 'evolutionary' perspective: the direct criminal liability of artificial agents

From a previously mentioned perspective, one could argue that the recipients of criminal regulations are not a closed group but are naturally bound to grow as society changes: individuals first, then entities, and finally artificial agents. However, if we were to consider holding artificial intelligence accountable, the path would be uphill. First and foremost, how can we even conceive, from a regulatory standpoint, the idea of culpability for such an entity[228]?

If we were to resort to a sanction without culpability, employing a purely objective attribution, an option that is entirely possible since no constitutional rights could prevent such a model regarding AI, the immediate problem would be the certain spillover effect[229]. Such a recipient would not possess economic resources to draw

[227] The problem lies in identifying the responsible party in the presence of AI systems that self-learn, as noted by E. Hilgendorf, *Autonome Systeme, künstliche Intelligenz und Roboter*, in *Festschrift für Thomas Fischer*, München, 2018, pp. 111 et seq. One of the most problematic aspects of AI is the autonomy of programs that adapt to the context by changing their action characteristics, as highlighted by G. Comandè, *op. cit.*, p. 172. The autonomy of robots is precisely what is emphasized in Recital AA of the Resolution on recommendations to the Commission regarding civil law rules on robotics (2015/2013 INL). The ethical limits of research in the field of artificial intelligence are also addressed in the guidelines of the European Commission, *Ethics Guidelines for Trustworthy AI*, 2018, p. 12, and in the context of the so-called Greater Europe, *Responsibility and AI*, Council of Europe Study 2019.

[228] Scepticals also include R. Abbott – A. Sarch, *op. cit.*, p. 327.

[229] W.R. Thomas, *The Ability and Responsibility of Corporate Law to Improve Criminal Punishment*, in *Ohio St. L.J.*, Vol. 78, 2017, pp. 601, 619.

from, and even if we were to limit or entirely prohibit its activity, its users would suffer the consequences.

Moreover, there would be a far more fundamental criticality.

It is logically impossible to speak of punishment for artificial agents and therefore of a legal system that governs it. Punishment involves inflicting some form of suffering through legal procedures following a legally recognized offense[230]. However, it is impossible for AI, in any form, to perceive even a vague diminishment of rights or a limitation of its social status as a result of the sanction[231]. Without this component, even before culpability, it is impossible to define and then uphold a proportionality constraint that signifies the 'deserved' punishment for AI. In essence, there is no balance between harm suffered - *malum passionis*, and wrongful action - *malum actionis*.

A penal system directed at artificial intelligence would require it to renounce itself, at least in the constitutional version of penalization gained in Western democracies (although it is true that Anglo-Saxon experiences still retain forms of strict liability, these are diminishing and limited to minor offenses[232]).

Thus, it would not only be objective but also devoid of any possibility of afflicting its recipients. We would be facing a purely restorative and automatic mechanism aimed at reacting to harm caused by AI, essentially a civil law right, even if formally qualified as criminal (one could invoke a sort of *matière civile*, paraphrasing conventional terminology).

Only a legislator intending to employ symbolic law for the sake of consensus would prioritize the criminal label, given the misplaced use of AI as a true "electronic scapegoat".

For the sake of completeness, and as a mere consequence of the lack of culpability and perception of sanction, brief considerations can also be made from the perspective of the goals of 'punishment.'

For example, from the standpoint of general deterrence, deterrence as a mechanism could only be activated through the threat of punishment if AI had been designed to comprehend it and make cost-benefit assessments in relation to its planned actions.

[230] On the necessity of suffering or consequences normally considered unpleasant for there to be punishment, see H.L.A. Hart, *Punishment and Responsibility: Essays in the Philosophy of Law*, Oxford, 2008, p. 4.

[231] They point out how in the presence of AI there may be a lack of capacity to commit culpable conduct, and thus a general prerequisite of criminal law R. Abbott – A. Sarch, *op. cit.*, p. 350.

[232] It must be noted that *strict liability*, although still known and practiced in *common law*, is subject to criticism and progressive downsizing, R.A. Duff, *The Realm of Criminal Law*, Oxford, 2018, p. 19. There is now agreement on the indispensability of voluntariness of the conduct considered by a criminal norm. W.R. La Fave, *Substantive Criminal Law*, Eagan, 2018, p. 572: «*criminal liability requires that the activity in question be voluntary*». The same *Model Penal Code* states that a person who has voluntarily engaged in conduct or omitted conduct of which they were physically capable cannot be convicted, see *Model Penal Code*, § 2.01(1) (Am. Law Inst. 1962). On the requirement of voluntariness as a physical act guided by conscious mental representation, see G. YAFFE, The Voluntary Act Requirement, in G. Yaffe, *The Voluntary Act Requirement*, in A. Marmor (ed.), *The Routledge Companion to the Philosophy of Law*, New York, 2012, pp. 174 et seq.

Shifting to special prevention, the reorientation of the artificial agent towards respect for violated values does not seem possible except through forced reprogramming (far from the paradigm of rehabilitation) or learning within the AI system regarding others' interests or collective interests. However, this depends on the initial instructions that determine the fundamental characteristics of the system and establish its willingness to learn from sanctions.

Thus, it becomes evident that autonomous responsibility of the artificial agent is an optical illusion and depends on the choices made by the programmer. By punishing AI, we are merely attributing the 'fault' of the creator to their creation.

4.2 The traditional perspective. Variation on the theme of individual (natural and/or legal) responsibility: the 'vicarious' model

If attributing the act to artificial intelligence is logically impossible, we must remain within the realm of individual or collective responsibility.

The conceptual basis would be provided by the long-standing paradigm of *respondeat superior*, reinterpreted so that the actions of the artificial agent are imputed to the legal or natural person whenever the former acts in pursuit of the interests of the subject, whether individual or collective, who is then held accountable[233].

Two variants are thus abstractly available:

i) The responsibility of the natural person for the actions of the artificial agent.

ii) The exclusive responsibility of the legal person for the actions of the artificial agent.

Upon closer examination, however, option (a) is impossible in the case of AI because AI does not relate to the individual as the natural person does to the *societas*, which is an aggregation of natural persons acting in its interest. AI and the natural person have a relationship of mere instrumentality. This is because the legal person is composed of natural persons, and both the collective entity and its shareholders have their own identifiable interests *ex ante*. AI is structurally *aliud* from the human horizon. Devoid of independent objectives to align with those of a different individual, the artificial agent is merely a means that, by definition, identifies its own ends with those of its user. Therefore, it makes no sense to ask whether it acted in the interest of someone else.

[233] On the use of *respondeat superior* regarding the punishment of the *company*, see A.S. Kircher, *Corporate Criminal Liability Versus Corporate Securities Fraud Liability: Analyzing the Divergence in Standards of Culpability*, in *Am. Crim. L. Rev.*, Vol. 46, 2009, pp. 157 et seq.; E. Lederman, *Models for Imposing Corporate Criminal Liability: From Adaptation and Imitation Toward Aggregation and the Search for Self-Identity*, in *Buff. Crim. L. Rev.*, Vol. 4, 2000, pp. 641, 654-55. Anche D. Lina, *Could AI Agents Be Held Criminally Liable*, in *South Carolina L. Rev.*, Vol. 69, Issue 3, 2018, p. 692, believes that it is the only adequate mechanism to hold individuals accountable for the actions of artificial intelligence at the moment.

The alternative of holding entities accountable for the use of malicious or excessively risky artificial agents, which are not controlled, is much more plausible. This would involve identifying the responsibility of the entity that has employed an employee/collaborator who, in turn, has used an artificial agent. American doctrine has already noted how the replacement of human operators with artificial agents can result in the imputation of events produced by machine malfunction to the entity[234].

In most cases, the actions of AI cannot be attributed to the natural person, at least due to the lack, on the part of the latter, of the subjective element required by the respective offense, given the artificial operator's autonomy of choice, which effectively decides freely how and when to commit an offense. In this case, it would be an autonomous and exclusive imputation to the legal person, bypassing the human agent and directly linking the artificial agent to the legal entity. Our legal system may already be prepared to such an evolution since, as known, Article 8 of Legislative Decree no. 231/2001 contains *in nuce* the prodromes of independent forms of responsibility, even though it currently still requires an act committed by an individual, whereas not imputable, punishable, or identified[235].

Alongside this solution, one can consider forms of direct criminal liability of the natural person for the dangerous use of artificial intelligence in the financial field. However, in order to better understand such a perspective, a preliminary clarification is necessary regarding the central role that the concept of risk is assuming in European legislation, both concerning the protection of markets from disruptions caused by artificial intelligence and in the broader discipline of AI-related damages.

5 Following: the role of risk in public market oversight today

Although criminal law has not yet been employed to counter market abuses achieved through HFT or other forms of artificial intelligence, a network of rules has already been established that allows for the implementation of sanctioning provisions based on risk, from civil to regulatory perspective. This model could be replicated in other sectors where AI is used.

We do not refer to the delayed adaptation to EU regulations by Law No. 238 of 2021[236], but to the regulatory and supervisory framework resulting from the synthesis of European legislation and CONSOB through stringent and common rules at the continental level and specific obligations for investment firms employing these techniques and the trading venues in which they are used.

[234] M.E. Diamantis, *The Extended Corporate Mind: When Corporations Use AI to Break the Law*, in *North Carolina Law Review*, Vol. 98, n. 4, 2020, pp. 898 et seq.

[235] Referring here to F. Consulich, *Il principio di autonomia della responsabilità dell'ente. Prospettive di riforma dell'art. 8*, in *Rivista 231*, n. 4, 2018, pp. 197 et seq.

[236] For a commentary on the Martiello Law, *Il "ravvedimento comunitario" del legislatore nazionale in materia di repressione degli «abusi di mercato»: prime note di commento all'art. 26 della legge n. 238/2021 («legge europea 2019-2020»)*, in *Leg. pen.*, 30 maggio 2022.

Without delving into the analysis of such regulations, it is worth noting that these obligations find their rationale in the inherently risky nature of trading, reflecting a regulatory approach based on risk management[237]. Rules of conduct have been established for traders, imposing organizational safeguards, while trading venues have been subject to similar structural requirements to test, monitor, and ensure system resilience under severe market stress scenarios.

This regulatory model is further explicated in the recent Proposal for a Regulation on Artificial Intelligence[238], which classifies products using AI software, either fully or partially, based on the risk of negative impact on fundamental rights of citizens and the infrastructure that supports contemporary democratic states, such as human dignity, freedom, equality, democracy, non-discrimination, data protection, as well as health and security.

As the riskiness of the AI system increases, the measures taken to eliminate or mitigate negative impacts become more stringent, to the point of prohibiting trades that pose an unreasonable risk.

At the most extreme level of illicit risk, there is an almost absolute ban on usage. According to the proposal (p. 14, as well as Article 5 and Annex III), this refers to «AI systems that use subliminal techniques to substantially distort a person's behaviour, thereby causing or likely to cause physical or psychological harm to that person or others; AI systems that exploit vulnerabilities related to age or disability of a specific group of people to substantially distort the behaviour of a person belonging to that group».

There is also a category of tendentially illicit risk, where the use of artificial agents is not entirely prohibited but requires a prior rigorous compliance assessment

[237] In addition to *MiFID II* directive, Delegated Directive (EU) 2017/593, Regulation (EU) No. 600/2014 (*MiFIR*), the provisions of Delegated Regulation (EU) No. 2017/584 must also be considered. The regulation on algorithmic trading is then contained in the following European legislative measures adopted by the Commission on draft regulatory technical standards (RTS) submitted to the Commission by the European Securities and Markets Authority (ESMA).

- Commission Delegated Regulation (EU) 2017/587 of July 14, 2016, on transparency requirements for trading venues and investment firms in respect of shares, depositary receipts, exchange-traded funds, certificates and other similar financial instruments and on transaction execution obligations in respect of certain shares on a trading venue or by a systematic internaliser;
- Commission Delegated Regulation (EU) 2017/589 of July 19, 2016, on organizational requirements and operating conditions for investment firms engaged in algorithmic trading;
- Commission Delegated Regulation (EU) 2017/578 of June 13, 2016, supplementing Directive 2014/65/EU of the European Parliament and of the Council on markets in financial instruments with regard to regulatory technical standards specifying the requirements on market making agreements and schemes;
- Commission Delegated Regulation (EU) 2017/566 of May 18, 2016, supplementing Directive 2014/65/EU of the European Parliament and of the Council on markets in financial instruments with regard to regulatory technical standards for the ratio of unexecuted orders to transactions to prevent disorderly trading conditions;
- Commission Delegated Regulation (EU) 2017/588 of July 14, 2016, supplementing Directive 2014/65/EU of the European Parliament and of the Council about regulatory technical standards on the tick size regime for shares, depositary receipts, and exchange-traded funds.

[238] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, April 21, 2021, available at www.eur-lex.europa.eu.

with stringent mandatory requirements and the adoption of an adequate management system that includes continuous verification and monitoring.

Below this category is the tendentially lawful risk, which includes systems subject to minimum and specific transparency obligations, such as chatbots and voice assistants. Finally, there are entirely lawful artificial agents that are deemed not risky *ex ante*, allowing for their continuous use.

This regulatory model is also emerging in other acts, as seen in the White Paper on Artificial Intelligence, where the European Commission has established the principle that AI is a strategic technology as long as it follows an anthropocentric, sustainable, and respectful approach to fundamental rights[239].

In summary, the efforts made so far, both at the national and EU levels, have focused on imposing organizational and security standards through registration and communication obligations with public authorities, mostly in the regulatory field. This is not irrelevant to penal enforcement, both regarding market abuses[240] and in a general perspective concerning AI.

European law conveys in the legal system, through the tools of transposition and implementation, an assimilation of the responsibility of the AI programmer or beneficiary with that of the manufacturer, within a civil and administrative regime. Such an approach simultaneously frames the context for potential criminal intervention.

However, civil law is not only about reparation but also prevention, at least from a European perspective. As emphasized in legal doctrine[241], the Proposal for a Regulation on Artificial Intelligence assumes the ordinary rules of imputation of responsibility to humans but aims to avoid applying them as much as possible. The damage should indeed be avoided through the implementation of the duty of human oversight, whereby intelligent systems must be designed and developed in a way that allows for human supervision (Article 14) in a context of continuous monitoring (Article 13). In this perspective, alongside the proposed Regulation, there is the proposal for a Directive on artificial intelligence liability dated September 28, 2022, which excludes any criminal implications and distinguishes, solely from a civil perspective, objective liability for high-risk systems and liability based on fault/negligent liability for low-risk systems.

On the administrative level, Article 71 of the Proposal for a Regulation on Artificial Intelligence introduces monetary sanctions of up to €30,000,000 or, if the offender is a company, up to 6% of the total annual worldwide turnover of the previous financial year, both for non-compliance with the prohibition of illicit practices (Article

[239] European Commission, White Paper on Artificial Intelligence - A European Approach to Excellence and Trust, 2020, available at www.eur-lex.europa.eu

[240] It defines the state of Italian legislation after the introduction of Legislative Decree No. 107 of 2018, which is still inadequate in addressing the issues posed by high-frequency algorithmic trading. See M. Palmisano, *op. cit.*, pp. 143 et seq.

[241] The reference is also made to T.N. Poli, *Intelligenza artificiale e tutela della persona*, in N. Linciano – V. Caivano – D. Costa -P. Soccorso – T.N. Poli – G. Trovatore, *L'intelligenza artificiale nell'asset e nel wealth management*, cit., pp. 92 et seq.

5) and for violations of rules regarding data and data governance of high-risk AI systems (Article 10).

It is particularly significant that AI is perceived as a source of risk but remains an object rather than a subject. The only person held accountable for damages is the natural person, who is assumed to always remain in control. Hence, a command responsibility for AI[242].

6 Possible punitive strategies of individuals under future law (*de lege ferenda*)

Once it is understood that the policy of law concerning artificial intelligence revolves around risk management, practical indications can be derived for the perspective of reforming financial criminal law. The issues that criminal law faces in practice relate to the enforcement of criminal charges when it is not possible to identify a natural person who has acted with or through an AI system[243].

Secondly, even assuming that one or more natural persons can be identified behind the action of AI, the problem arises regarding the reduction of its action to a legally significant contribution by humans, as these individuals may have taken actions that are completely neutral in themselves. Even assuming simple negligence, one can encounter momentary and irrelevant misunderstandings among programmers, imperceptible lapses of attention, absolutely negligible calculation errors, and so on, occurring in different places and times unrelated to the offensive act. In short, the practical irreducibility of the AI's action to the natural person is combined here with legal irreducibility[244].

Given that, at least in our legal system, there is no legitimate possibility of directly holding the artificial agent accountable, nor those who have used or created it, unless resorting to the discipline of corporate liability, exploiting the provision of Article 8 of Legislative Decree 231/2001, we must consider reforming the system.

There are several options on the table, and obviously, we cannot consider those that pertain to extra-criminal aspects, which can nevertheless have a significant deterrent effect. Consider, for example, the proposal to tax individual transactions, as this would instantly cool down the tendency of high-frequency traders to generate massive orders, for operators processing thousands of transactions per second[245]. Another extra-criminal option is to impose time or quantity constraints that algorithmic

[242] This is also highlighted by A. Amidei, *Le responsabilità da intelligenza artificiale tra product liability* e *sicurezza del prodotto*, in Aa.Vv., *XXVI Lezioni di Diritto dell'Intelligenza Artificiale*, 2021, pp. 149 et seq. On the notion of product damage, see C. Piergallini, *Danno da prodotto e responsabilità penale, Profili dommatici e politico criminali*, Milano 2004, pp. 40 et seq.; Id., *La responsabilità del produttore: una nuova frontiera del diritto penale?*, in *Dir. pen. proc.*, n. 9, 2007, pp. 1125 et seq.

[243] On the inherent difficulty of effectively enforcing anti-manipulation disciplines, see S.D. Ledgerwood – P.R. Carpenter, *A Framework for the Analysis of Market Manipulation*, in *Rev. L. & Econ.*, Vol. 8, 2012, pp. 253, 260.

[244] Here, the reference to R. Abbott – A. Sarch, *op. cit.*, p. 336.

[245] J. Fullerton, *High-frequency Trading is a Blight on Markets That the Tobin Tax Can Cure*, in *The Guardian*, 4 April 2014 (https://www.theguardian.com).

operators must comply with, thereby maintaining a position in the market where they trade without being able to engage in purely instantaneous speculative strategies[246].

Outside the hypothesis of direct and exclusive responsibility of the entity, which we have already discussed, individual punishment revolves around two options:

i) the position of guarantee regarding the damage caused by artificial intelligence in the market;

ii) liability for unlawful risk.

6.1 The position of guarantee regarding the 'act' of the algorithm

On a strictly criminal level, the risk control strategy chosen at the European (and therefore Italian) level seems to lead to the obligatory path of omissive liability for the failure to prevent the adverse event caused by the artificial agent. The programmer or user would be held responsible since they have assumed a role of control over that specific intelligent system. The responsibility, therefore, would concern the criminally relevant offenses that could have been avoided through better management of the AI itself or by implementing suitable preventive mechanisms or more careful l programming at origin that would neutralize or contain the associated risks[247].

It should be clear that invoking a position of guarantee, typically in the form of control over that particular source of risks constituted by the artificial agent, does not exhaust the problems of imputation. Not only does it fail to attribute unforeseeable or unavoidable acts to the guarantor (unless avoiding to handle artificial agents altogether, which would be historically inconsistent), but especially because an algorithm or a system of algorithms that determine the emergence of an artificial intelligent entity is not an individual work but the result of teamwork, increasingly involving a larger number of individuals due to the diverse skills required and the need to converge multiple personal creativities[248]. Not to mention the scenario where the AI software is open-source and built by entities located in various parts of the world[249].

Therefore, in addition to the problem of imputing factual actions and intent to a natural person regarding the actions of the artificial entity, there is also the issue

[246] On this point, see M. Morelli, *Implementing High Frequency Trading Regulation: A Critical Analysis of Current Reforms*, in *Mich. Bus. & Entrepreneurial L. Rev.*, Vol. 6, Issue 2, 2017, pp. 201, 212.

[247] In this direction, with the identification of a *Responsible Person* (potentially also a legal entity that relies on it for its characteristic activity), based on negligence, with related registration, administrative, and insurance obligations, for cases of so-called hard AI crime, i.e., those in which an immediate and direct physical author cannot be identified, see also R. Abbott – A. Sarch, *op. cit.*, pp. 378 et seq., who then propose the establishment of a guarantee fund, funded by individuals or collectives utilising artificial intelligence, for cases where the responsible AI does not have a accountable person or that person is incapable or uninsured.

[248] This is a problem that precedes criminal intervention and concerns the personal and legal attribution of the act itself, see D.J. Gunkel, *Mind the Gap: Responsible Robotics and the Problem of Responsibility*, in *Ethics and Information Technology*, Vol. 22, 2017, pp. 307et seq.; M. Coeckelbergh, *Artificial Intelligence, Responsibility Attribution, and a Relational justification of Explainability*, in *Science and Engineering Ethics*, Vol. 26, 2020, pp. 2051 et seq.

[249] A case to which reference is made, for example, by R. Abbott – A. Sarch, *op. cit.*, pp. 323, 326.

of distributing criminal responsibility among individuals who have somehow participated in the development of the intelligent system, starting from the selection of the relevant causal contribution within a network of factors potentially capable of participating in the causal nexus[250]. Building a position of guarantee on these grounds simply means defining a responsibility-sharing centre in the event of harmful events, without actually implying reproach towards the guarantor[251].

The allocation of responsibility among multiple co-agents who cooperate with each other entails solving what Anglo-American doctrine refers to as the "many hands problem"[252]. However, there is also the issue of the "many things problem" because, increasingly, the construction and evolution of artificial intelligence involve the intervention of another artificial intelligence, which implies that the factual profiles to be considered proliferate and extend over time[253].

Indeed, this perspective is already effective in the administrative field concerning market abuse. To safeguard the order of the market from abusive misconduct, the provisions of Articles 187-*bis* and 187-*ter* TUF are applicable since they aim to punish the behaviour of the human agent, with intent, through negligence, or even merely due to negligence. The potential introduction of a new general incriminating offense for failure to control would, therefore, overlap with rules operating in certain sector - specific regulations, particularly in financial market law, which, as mentioned, already provide protection against conduct characterized by a minor psychological coefficient[254].

6.2 Criminal liability for illicit risk emanating from artificial intelligence

The second punitive option that could be adopted draws inspiration from the recognition of the inherently instrumental nature of AI[255]. Artificial intelligence does

[250] S. Beck, *Google Cars, Software Agents, Autonomous Weapons Systems. New Challenges for Criminal Law?*, in E. Hilgendorf – U. Seidel (eds.), *Robotics, Autonomics, and the Law*, Baden, 2017, p. 243, as well as G.Q. Olivares, *La Robotica ante et derecho penal*, in *Revista Electrónica de Estudios Penales y de la Seguridad*, n. 1, 2017, pp. 16 et seq.

[251] On the same line, see C. Piergallini, *op. cit.*, p. 1758.

[252] M. Taddeo – L. Floridi, *How AI can be a force for good*, in *Science*, Vol. 361, Issue 6404, 2018, p. 751, observe on the effects of decisions or actions based on AI: «*The effects of decisions or actions based on AI are often the result of countless interactions among many actors, including designers, developers, users, software, and hardware [...]. With distributed agency comes distributed responsibility*».

[253] On the issue of "many things," see M. Coeckelbergh, *op. cit.*, p. 2052.

[254] Article 2(4) of the Market Abuse Regulation (MAR) states: « The prohibitions and requirements in this Regulation shall apply to actions and omissions, in the Union and in a third country, concerning the instruments referred to in paragraphs 1 and 2».

[255] In American criminal law, the concept of innocent agency doctrine is used in this regard, whereby criminal responsibility is attributed to someone who acts through a completely innocent agent, who is therefore a kind of tool in his hands. See, for example, 18 U.S.C. § 2(b) (2019), which states, «*Whoever willfully causes an act to be done which [is a crime] is punishable as a principal*». In jurisprudence, *Rosemond v. United States*, 572 U.S. 65, 79-80 (2014). In doctrine, S.H. Kadish, *Complicity, Cause and Blame: A Study in the Interpretation of Doctrine*, in *Calif. L. Rev.*, Vol. 73, n. 2, 1985, pp. 323, 372-73, e P. Alldridge, *The Doctrine of Innocent Agency*, in *Crim. L. Forum*, Vol. 2, 1990, pp. 45, 70-71.

not act out of its own interests. Algorithms and software do not have autonomous preferences but serve a function for one or more individuals[256].

What matters is the risk involved in the use of AI in a given context. It will be necessary to determine whether the risk inherent in every type of artificial intelligence (albeit in varying forms depending on the types and sectors of activity) has been deliberately raised beyond tolerance limits.

By focusing the reproach on the risky conduct instead of the harmful event, it is possible to bypass the problem of unpredictability of the actions of artificial intelligence, the gap that arises from the choices made by AI compared to the generic instructions given by the programmer. It is necessary, therefore, to revert to the creation of knowingly dangerous offenses.

An indicium of knowing danger with respect to investments and the regular course of negotiations will be the introduction of artificial agents into exchanges with illicit instructions or insufficient safeguards regarding their propensity for disruption. The foundation of individual liability will be the assumption of an unreasonable risk, including through the omission of technical measures aimed at ensuring the proper management of an artificial intelligence system.

It will not be necessary for the individual to anticipate the production process of the event or the event itself, which is now an impossible condition in the presence of advanced algorithmic systems. It will be sufficient to create a risk capable of producing that type of event.

This second option of liability for assuming an illicit risk seems to have already been incorporated by the European legislator in the Proposal for a Regulation on Artificial Intelligence at the administrative level, with the provision of sanctions for noncompliance with the prohibition of illicit practices and violation of the conformity requirements for high-risk systems (Article 71). However, for this broader option to become effective in the context of market abuses, it is necessary for trading AI systems to be included within the scope of high-risk systems.

7 The problem of the retribution gap from a comparative perspective

In international doctrine, there is a common perception of the existence of a true retribution gap in the field of artificial intelligence[257]. The concern is not to target

[256] On this point, see B.J. Koops – M. Hildebrandt- D.O. Jaquet-Chiffelle, *Bridging the Accountability Gap: Rights for New Entities in the Information Society?*, in *Minn. J. L. Sci. & Tech*, Vol. 11, 2010, pp. 497 et seq.; and, even earlier, L. Floridi – J.W. Sanders, *In the Morality of Artificial Agents*, in Mind and Machines, Vol. 14, 2004, pp. 349 et seq.

[257] J. Danaher, *Robots, Law and the Retribution Gap*, in *Ethics and Information Technology*, Vol. 18, 2016, pp. 299 9 et seq.; subsequently, remains critical in relation to these forms of 'accessory' responsibility of the individual, J. Turner, *Robot Rules*, 2018, pp.120 et seq., which also highlights the risks of overdeterrence and chilling effect on technological research.

the person behind the algorithm solely because a responsible party must still be identified. The risk of moral scapegoating is therefore high and increases as the level of technology underlying AI advances.

Despite this potential side effect, many agree on maintaining a human-centric approach within the field of criminal law. In this regard, the principle of "human in command" has been discussed, not only in doctrine but also at the regulatory level, particularly in European soft law. The orientation is towards the creation of accountability mechanisms and security by design (referring to software explicitly designed to be secure, anticipating and minimizing risk profiles in advance that may subsequently emerge). This approach aims to ensure verifiability of algorithmic choices, minimizing the risk of errors or unforeseen consequences, and, above all, guaranteeing individuals the ability to regain control of the situation when necessary to avoid or manage risks generated by AI[258]. In fact, human control over artificial intelligence – which would then give rise to omissive criminal liability – can only be guaranteed through the imposition of design safeguards upstream and control measures downstream of algorithmic actions. Therefore, legislators should grant AI the maximum useful autonomy while maintaining a sphere of human control[259].

It is necessary to understand what solutions have been proposed to address the imputability deficit in the field of AI applied to markets.

7.1 Reflections from Anglo-American doctrine

The interaction between artificial intelligence and human agents leads to the fragmentation of responsibilities[260]. In Anglo-Saxon doctrine, someone put forth the idea of resorting to a mechanism of vicarious liability for human beings in relation to AI. However, this mechanism is not purely objective, as the human agent is held accountable not just for the mere existence of damage caused by AI, but also for the fault of the programmer.

The programmer (and possibly the user) would assume the role of the employer, and the intelligent system would be their employee, establishing a paradigm based on the concept of natural-probable consequence[261]. This mechanism is intended

[258] It is interesting to look at the proposals put forward, in a context very different from ours, by the SINGAPORE PERSONAL DATA PROTECTION COMMISSION, according to which it is necessary that, in the fields governed by artificial intelligence, the possibility for the human person to regain control of the operational scenario at any time is always guaranteed. Singapore PDPC, A Proposed Model Artificial Intelligence Framework (Jan. 2019), available at https://www.pdpc.gov.sg. In particular, it is proposed (15) to implement in all artificial agents systems similar to the black box of aircraft, in order to be able to reconstruct the AI's decision-making processes.

[259] See the document published by the High-Level Expert Group on Artificial Intelligence, established by the European Commission in June 2018, entitled *Ethical Guidelines for Trustworthy Artificial Intelligence*, April 8, 2019, available at www.europa.eu, 18; 30 et seq.; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, Building Trust in Human-Centric Artificial Intelligence, April 8, 2019, available at eurlex.europa.eu, 3 et seq.

[260] In Italian doctrine, the issue is signaled by M.B. Magro, *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, cit., p. 3.

[261] Similarly, G. Hallevy, *The Criminal Liability of Artificial intelligence Entities*, in *Akron Intellectual Property Journal*, Vol. 4, Issue 2, 2010, pp. 171 et seq.

to attribute an unintended act to the agent (therefore attributable to mere negligence or at most recklessness) which occurred within the context of an agreement to commit a different, less serious offense. Basically, it is a discipline closely related, conceptually, to Article 116 of the Italian Criminal Code[262].

Another solution, according to some scholars, could be the concept of perpetration by another. This is far from a vicarious mechanism and much closer to a strictly concurring approach, which allows for the punishment of those who use or create the artificial agent[263], provided that the intent to commit the offense can be identified. The AI system would be a sort of unconscious accomplice to the person who, through its use, aims to commit the wrongdoing.

Such formulations thus relate to the issue of potential participation between natural persons and artificial agents. Continental criminal lawyers, particularly those in the German cultural area, would be drawn to the concept of mediated authorship[264], a typical case where one subject has control over the act and another, subordinate to the first, carries it out without possessing independent imputability. Meanwhile, anglophone legal systems lean toward the paradigm of perpetration by another (or by means) or even innocent agency[265].

In our opinion, since it is not possible to equate human agents with artificial agents, it would not be correct to appeal to a concurrence paradigm, even if renewed among the participating subjects. We are dealing with a simple refinement of the *instrumentum sceleris*. Despite its peculiarity, AI remains a mere tool in the hands of the sole human author of the offense.

International criminal law echoes can be found in the pages of those who propose to import of the command responsibility model into 'common' criminal jurisdiction. Typical of hierarchical organizations of a military nature (or similar) and borrowed from Article 28 of the Rome Statute of the International Criminal Court, it ends up attributing responsibility to the individual in a position of organizational pre-eminence who knew about the ongoing offense committed by a subordinate and yet failed to take reasonable measures to prevent its perpetration[266].

[262] For its use in the field of artificial intelligence, see G. Hallevy, *Unmanned vehicles—Subordination to criminal law under the modern concept of criminal liability*, in *Journal of Law, Information and Science*, Vol. 21, 2012, p. 200. On this model of responsibility, see, for example, K.R. Bird, *Natural and probable consequences doctrine: "Your acts are my acts!"*, in *W. St. UL Rev*, Vol. 34, 2006, p. 43; previously, T.B. Robinson, *A question of intent: Aiding and abetting law and the rule of accomplice liability under section 924 (c)*, in *Michigan Law Review*, Vol. 96, 1997, p. 783.

[263] On this point, see U. Pagallo, *From automation to autonomous systems: A legal phenomenology with problems of Accountability*, in *Proceedings of the 26th international joint conference on artificial intelligence*, available at www.ijcai.org; also read C.A. De Lima Salge – N. Berente, *Is that social bot behaving unethically?*, in *Communications of the ACM*, Vol. 60, Issue, 9, 2017, p. 29.

[264] The famous work of C. Roxin, *Täterschaft und Tatherrschaft*, Hamburg, 1963 (10. Auf., Berlin, 2019), pp. 67 et seq., pp. 119 et seq. This form of participation is expressly recognized in the Spanish Penal Code of 1995 (Article 28), as well as in the statute of the International Criminal Court, Article 25(3)(a).

[265] On "innocent agency" and "perpetrator through another person", A.P. Simester – J.R. Spencer – G.R. Sullivan – G.J. Virgo, *Simester and Sullivan's Criminal Law. Theory and Doctrine*, Oxford, 2013, pp. 205 et seq.

[266] According to A. McAllister, *Stranger than science fiction: The rise of AI interrogation in the dawn of autonomous robots and the need for an additional protocol to the UN convention against torture*, in *Minnesota Law Review*, Vol. 101, 2017, pp. 2527 et seq., the concept would also be applicable to cases of unlawful acts committed by artificial intelligences.

Applied to the unlawful act of AI, this solution would make it easier to attribute liability to the individual as it does not require such individual, identified as the one possessing a function that is more directional than directive over the artificial agent, to demonstrate any specific intent regarding the commission of the criminal act. It suffices for him to have awareness (knowledge) of the act's realization within the organizational scope of his competence, where the artificial subject operates[267].

7.2 Overview of US jurisprudence

Turning to the US scenario, specifically the jurisprudential framework, the most applied provisions have been those aimed at contrasting market manipulation. For instance, the responsibility for fraudulent artificial representation of reality has been invoked under Section 10(b) of the Exchange Act and Rule 10b-5 promulgated by the SEC, which have been recognized by jurisprudence, albeit without explicit regulatory *placet*, as potential sources of civil actions since 1971[268].

Alternatively, attention is drawn to the possibility of invoking Section 9 of the Exchange Act, which differs from the previous provisions in that it requires demonstrating the specific intent to induce the purchase or sale of financial instruments by others or to create a false appearance of securities' performance. Consequently, both private individuals and prosecutors rarely invoke this provision in market manipulation proceedings[269].

The first action for market manipulation, specifically "marking the close" carried out by HFT (High Frequency Trading), was undertaken by the SEC on October 16, 2014, for violation of Rule 10b-5[270]. Class actions have also been initiated, as in the leading case of City of Providence v BATS Global Markets, Inc. [271]

Indeed, the manipulative strategies employed through HFT perfectly meet the artificiality requirements set forth in the mentioned regulations, as they generate a distorted representation of the market reality for slow traders, thus satisfying the requirements for conviction in civil actions[272].

A mention should be made of Section 747 of the Dodd-Frank Wall Street and Consumer Protection Act, a federal law enacted in 2010 under the Obama administration following the 2008 economic crisis with the aim of amending the Commodity

[267] For an initial approach to the topic, see D. Amoroso - G. Tamburrini, *I sistemi robotici ad autonomia crescente tra etica e diritto: quale ruolo per il controllo umano?*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1, 2019, pp. 33 et seq. For all, on this paradigm, in its original context, i.e., international criminal law, see C. Meloni, *Command Responsibility in International Criminal Law*, The Hague, 2010, 31 et seq.

[268] See Superintendent of Insurance of New York v Bankers Life & Casualty Co, 404 US 6, 13 n 9 (1971).

[269] See on this point, M.K. Multer, *Open-Market Manipulation under SEC Rule 10b-5 and Its Analogues: Inappropriate Distinctions, Judicial Disagreement and Case Study; Ferc's Anti-manipulation Rule*, in *Sec Reg L. J.*, Vol. 39, 2011, p. 106.

[270] SECURITIES AND EXCHANGE COMMISSION, *SEC Charges New York-Based High Frequency Trading Firm with Fraudulent Trading to Manipulate Closing Prices* (Oct 16, 2014), available at http://perma.cc.

[271] *Complaint for Violation of the Federal Securities Laws, Civil Action No 14-2811* (SDNY filed Apr 18, 2014). In this regard, see T.E. Levens, *op. cit.*, p. 1534.

[272] This is noted byT.E. Levens, *op. cit.*, pp.1546 et seq.

Exchange Act and introduce a provision in the US legal system that penalizes any form of trading that may constitute spoofing, i.e., the placement of orders with immediate cancellation before execution if there is evidence of the operator's intent (7 U.S.C. § 6c(a)(5) (c))[273]. As known, the CFTC has based certain legal actions, both civil and criminal charges, on Section 6c(a) (5)(C) concerning algorithmic trading, as seen in the well-known *Coscia* case[274].

The recurring challenge of proving intent has also emerged in this recent legal case. The jurisprudence (specifically the Seventh Circuit Court of Appeals) has lamented that this requirement is somewhat limiting in terms of the potential applicability of the provision. However, despite this, it confirmed the defendant's conviction in criminal proceedings[275].

7.3 Technical and regulatory initiatives of US regulatory authorities

The SEC has not only acted through sanctions but also through regulatory activities and technological implementation of its enforcement activities in the markets, despite operational difficulties arising from a level of human and technological resources that are insufficient to keep pace with the computerised evolution of trading systems. This was highlighted, for example, by the former SEC Chair Mary Jo White in her testimony to the US Congress in 2013[276].

[273] Cfr. 7 U.S.C. § 6c(a)(5)(C), as discussed by M. Woodward, *The Need for Speed: Regulatory Approaches to High Frequency Trading in the United States and the European Union*, in *Vand. J. Transnat'l L.*, Vol. 50, n. 5, 2017, pp. 1359 et seq. The provision reads as follows «*It shall be unlawful for any person to engage in any trading, practice, or conduct on or subject to the rules of a registered entity that—*

(A) violates bids or offers;

(B) demonstrates intentional or reckless disregard for the orderly execution of transactions during the closing period; or

(C) is, is of the character of, or is commonly known to the trade as, "spoofing" (bidding or offering with the intent to cancel the bid or offer before execution)» (Added emphasis).

[274] *U.S. v. Coscia*, 100 F.Supp.3d 653, 659 (N.D. Ill. 2015), aff'd, 177 F.Supp.3d 1087 (N.D. Ill. 2016), where the Court also denied that the provision introduced by the Dodd-Frank Act was unconstitutionally vague. On the efforts of the CFTC in terms of HFT enforcement, see the overview by M. Woodward, *op. cit.*, pp. 1382 et seq.

[275] *Coscia*, 866 F.3d. al punto 794, where it can be read: «*The text of the anti-spoofing provision requires that an individual place orders with "the intent to cancel the bid or offer before execution." 7 U.S.C. § 6c(a)(5)(C). This phrase imposes clear restrictions on whom a prosecutor can charge with spoofing; prosecutors can charge only a person whom they believe a jury will find possessed the requisite specific intent to cancel orders at the time they were placed. Criminal prosecution is thus limited to the pool of traders who exhibit the requisite criminal intent*». According to scholars as well, proving the central element of financial fraud, i.e., intent, is truly elusive in the context of cyber transactions, see cfr. G. Scopino, *op. cit.*, p. 233; also T.C.W. Lin, *The New Market Manipulation*, cit., p. 1301, notes that intent is absent in a context where human involvement is limited to the initial implementation of the algorithm and its entry into the market, and the AI lacks direction from a physical operator and continues to modify its trading strategies.
On the lack of enforcement in the American market concerning disruptions related to the use of HFT, see O. Cosme Jr., *Regulating High-Frequency Trading: The Case for Individual Criminal Liability*, in *J. Crim. L. & Criminology*, Vol. 109, Issue 2, 2019, pp. 386 et seq. Many authors in North American literature have highlighted how it is difficult to expect the law, not only criminal law but also company and market-related law, which naturally refers to individuals or at most entities, to apply to artificial intelligence systems. Among the many reflections in this regard, see S. Chopra – L.F. White, *A Legal Theory for Autonomous Artificial Agents*, Ann Arbor, 2011, 153 et seq.; as well as the pioneering considerations of L.B. SOLUM, op. cit., pp.1231-33.

[276] B. Protess, *White Makes Case for Bigger S.E.C. Budget*, in *N.Y.* TIMES, 7 maggio 2013.

On the technological side, mechanisms such as circuit breakers and execution throttles, like those implemented by trading venues in Italy, have been gradually implemented. These mechanisms were also discussed in relation to derivatives within the Commodity Futures Trading Commission (CFTC). They are essential safeguards to prevent manipulative practices such as order stuffing, where a massive number of orders are entered into the market and quickly cancelled before execution[277]. The Securities Industry and Financial Markets Association (SIFMA) has also put forth proposals in this sector to introduce "technical" protections for investors, such as predefined price fluctuation bands within reasonable limits, as well as automatic trading pauses when necessary to promote proper price discovery[278].

On the regulatory side, the so-called Limit-Up and Limit-Down rules have been established, preventing excessive fluctuations in the value of a security compared to the average price recorded in a given preceding period[279]. Furthermore, as early as 2014, the SEC approved the Regulation Systems Compliance and Integrity (SCI) rule, which imposes strict compliance and integrity monitoring and documentation requirements on most trading platforms[280].

With the aim of improving market transparency, Rule 613 adopted by the SEC can provide essential support. It requires markets and the Financial Industry Regulatory Authority (FINRA)[281] to create and maintain the Consolidated Audit Trail (CAT), a tool designed to track the order lifecycle of all financial transactions. This enables the retrospective- *ex post* reconstruction of the etiology and phenomenology of potentially manipulative conduct carried out simultaneously across multiple markets, including by algorithmic traders. The CAT is particularly useful in facilitating private enforcement in the markets, including class actions by investors[282]. To monitor trades, the SEC established the Market Information Data Analytics System (MIDAS)[283] within its structure in 2013. Since 2010, a rule has prohibited naked access, previously used by HFT firms

[277] In this regard, see the document prepared by the CFTC, *Concept Release on Risk Controls and System Safeguards for Automated Trading Environments*, 78 FR 56542-01 (proposed Sept. 12, 2013), available at http://www.cftc.gov.

[278] See SIFMA, Flash Crash Resource Center, in http://www.sifma.org.

[279] FINRA Rules, Rule 6190; NMS Plan to Address Extraordinary Market Volatility (as modified by SEC *Approval Order*, *Exchange Act Release* No.77679) 11 (2016), http://www.finra.org. Observers such as Charles Korsmo (C. Korsmo, *High-Frequency Trading: A Regulatory Strategy*, in *U. Rich. L. Rev.*, Vol. 48, 2014, pp. 523, 608) place great confidence in these measures, noting that «circuit breakers are the most straightforward way to prevent a repeat of the major dislocations of the Flash Crash». Along the same lines, M.B. Fox-Glosten – G.V. Rauterberg, *The New Stock Market: Sense and Nonsense*, in *Duke L. J. 191*, Vol. 65, 2015, pp. 272 et seq.

[280] See 17 C.F.R. §§ 242.1000-07 (2017). Under this regulation, trading venues must promptly notify the SEC of previously unknown technological issues. The SCI regulation does not directly concern HFT but encourages trading venues to closely monitor their activity. See Regulation SCI Adopting Release, Exchange Act Release No. 73639, 79 Fed. Reg. 72252, 72410 (Dec. 5, 2014). For a list of doctrinal proposals and initiatives actually taken by the SEC to improve HFT monitoring, see M. Morelli, *op. cit.*, pp. 220 et seq.

[281] This is the independent self-regulatory authority of the U.S. financial sector. Specifically, FINRA is a nonprofit organization authorized by the U.S. government, tasked with overseeing the activities of U.S. financial entities.

[282] Press Release, SEC, *SEC Approves New Rule Requiring Consolidated Audit Trail to Monitor and Analyze Trading Activity* (July 11, 2012), http://www.sec.gov.

[283] Press Release, SEC, *SEC Launches Market Structure and Data Analysis Website* (Oct. 9, 2013), https://www.sec.gov.

to access markets through the credentials of a broker registered with the SEC, thereby concealing their presence in the market[284].

Scholars have long confirmed that the most important provisions in contrasting algorithmic abuses are indeed the SEC's so-called Bedrock Rule (10b-5) [285] and the CFTC's[286] Rule 180.1[287]. Additionally, they have suggested that disciplines such as the Market Access Rule[288] can be employed to enhance preventive market supervision and indirectly counter new forms of manipulation without delving into the thorny issue of the subjective element of physical operators[289].

7.4 The UK Scenario

After the United Kingdom's exit from the European Union, a comparison has become relevant with the system across the Channel, which is no longer subject to the integrative action of EU institutions, particularly ESMA. The main reference here is the section 90(1) of the UK Financial Services Act 2012, which, although not specifically referring to algorithmic trading, can be applied to punish those who engage in HFT strategies that create a false or misleading impression of the price or value of an issuer or financial instrument[290]. This offense is punishable by imprisonment and fines. Previously, the section 397(3) of the Financial Services and Markets Act 2000 required

[284] Risk Management Controls for Brokers or Dealers with market Access, Exchange Act Release No. 34-63241, 75 Fed. Reg. 69791 (Nov. 3, 2010) (codified at 17 C.F.R. § 240.15c3-5).

[285] 17 C.F.R. § 240.10b-5 (2017).

[286] In such terms, with reference to Rule 10b-5 Coffee, Introduction. Mapping the Future of Insider Trading Law. Of Boundaries, Gaps, and Strategies, in Colum. Bus. L. Rev., 2013 281, 317; in case law, still on rule 10b-5.

[287] 17 C.F.R. § 180.1 (2017).

[288] Consider section 15 U.S.C. § 78o(b)(4)(E) (2012) alla section 17 C.F.R. § 240.15c3-5 (2017) and section 17 C.F.R. § 166.3 (2017); in case law, In re FX Direct Dealer, LLC, CFTC No. 13-34, 2013 WL 11069513, 1 (Sept. 18, 2013); In re Forex Capital Mkts., LLC, CFTC No. 12-01, 2011 WL 4689390, 1 (Oct. 3, 2011).

[289] T.C.W. Lin, The New Market Manipulation, cit., p. 1301.

[290] The provision titled Misleading Impressions, states: «*A person ("P") who does any act or engages in any course of conduct which creates a false or misleading impression as to the market in or the price or value of any relevant investments commits an offence if—*

(a) P intends to create the impression, and

(b) the case falls within subsection (2) or (3) (or both)».

The subsequent subsections 2, 3 e 4 state: «*The case falls within this subsection if P intends, by creating the impression, to induce another person to acquire, dispose of, subscribe for or underwrite the investments or to refrain from doing so or to exercise or refrain from exercising any rights conferred by the investments.*

(3) The case falls within this subsection if—

(a) P knows that the impression is false or misleading or is reckless as to whether it is, and

(b) P intends by creating the impression to produce any of the results in subsection (4) or is aware that creating the impression is likely to produce any of the results in that subsection.

(4) Those results are—

(a) the making of a gain for P or another, or

(b) the causing of loss to another person or the exposing of another person to the risk of loss». For this provision and its relation to *HFT*, see J. Fisher – A. Clifford – F. Dinshaw – N. Werle, *Criminal Forms of High Frequency Trading on the Financial Markets*, in *Law & Fin. Mkt. Rev.*, Vol. 9, 2015, pp. 113 et seq.

proof of inducing a third party to engage in investment conduct, which effectively prevented the application of the provision during its 12-year enforcement.

The removal of this requirement in the current offense, in the opinion of scholars, should facilitate its easier enforcement. Moreover, from a mental element perspective, it does not only require intention and awareness of the false and misleading nature of one's behaviour towards others, but also recklessness is sufficient[291].

Nonetheless, the Financial Conduct Authority (FCA), responsible for market supervision in the UK, has increased its controls on HFT by relying on section 118 of the FSMA, which prohibits market abuse. This was evident in cases such as *Coscia* (within UK jurisdiction)[292] and *Da Vinci*[293], concluded in 2015 before the High Court of Justice following FCA's legal action, as well as the previous case of *Swift trade*[294]. These disruptions primarily involved the layering technique[295], and while meeting the criteria for criminal prosecution, the regulatory authority chose to pursue civil action[296].

A substantially similar case occurred in 2017 with Paul Axel Walter, resulting in an administrative sanction imposed by the FCA against an employee of Bank of America Merrill Lynch International Limited (BAML) for implementing a strategy in 2014 that involved placing orders aiming to induce other market participants who followed the price movements of the securities to increase or decrease the quotations, thereby benefiting from the price variation[297].

[291] In this sense J. Fisher – A. Clifford – F. Dinshaw – N. Werle, *op. cit.*, p. 115.

[292] Financial Conduct Authority, *Final Notice to Michael Coscia* (3 July 2013), 3, available at https://www.fca.org.uk/static/documents/finalnotices/coscia.pdf.

[293] For the decision of the case, see https://www.fca.org.uk

[294] See Financial Services Authority, *Decision Notice 2011: 7722656 Canada Inc formerly carrying on business as Sunft Trade Inc* (6 May 2011), https://vw.fca.org.uk; also Financial Conduct Authority, *Final Notice 2014: 7722656 Canada Inc formerly carrying on business as Swift Trade Inc* (24 January 2014), https://vw.fca.org.uk/static/documents/final-notices/7722656-canada-inc.pdf.

[295] It refers to a technique that involves placing a hidden order (not visible in the trading book) for buying or selling and another visible order in the book on the opposite side (selling/buying) to induce other traders to believe that the market is moving towards a price decline and act accordingly. For a description of the three cases, see G. Ruta, *op. cit.*, pp. 67 et seq. In the *Da Vinci case*, the alleged manipulative conduct falls within the category of Layering or Spoofing, for which the judge provided the following definitions: Layering involves the practice of placing relatively large orders on one side of the exchange book without a genuine intention of executing them. The orders are placed at prices that are unlikely to attract counterparties, at least as intended by the placer, but are still capable of causing a price change for the stock because of market adjustment due to an apparent shift in the balance between supply and demand. This movement is followed by the execution of a trade on the other side of the order book, resulting in a profit. This cycle is repeated multiple times. From this description, it is evident that Layering refers to the placement of multiple orders designed not to be traded on one side of the book, while Spoofing refers to the fact that this placement creates a false impression about the trader's true commercial intentions.

[296] For further reflection on this point, see J. Fisher – A. Clifford – F. Dinshaw – N. Werle, *op. cit.*, p. 117.

[297] The complete reference of the case can be found at the following link: https://www.fca.org.uk/publication/final-notices/paul-axel-walter-2017.pdf. It is particularly interesting that the manipulation was made possible by exploiting the use of algorithms by other market participants. Specifically, the employee took advantage of algorithms used by other traders to monitor the best bids, attracting them towards their own quotes and then trading at higher or lower prices.

Conclusions

The work focuses on the distinction between weak AI systems and strong AI systems: while the former rely on pre-established instructions from manufacturers, programmers, or users, the latter possess self-learning capabilities and produce autonomous and unpredictable outputs compared to the initial inputs.

The diffusion of such technologies in the financial market, particularly in trading rather than the dissemination and circulation of insider information, raises concerns about the resilience of the regulatory framework. It specifically questions the attribution of financial misconduct committed with the involvement of artificial agents and necessitates an examination of whether Regulation (EU) MAR is suitable for encompassing illicit behaviour perfected using artificial intelligence systems, whose autonomy and unpredictability may result in areas of non-punishment.

Indeed, while existing legal rules can be broadly applied to contrast illicit conduct by weak AI systems, the imputation of responsibility for strong AI systems requires the adoption of new - *ex novo* criteria that effectively safeguard the proper functioning of exchanges.

The capacity of strong AI systems appears to undermine the application of the principle of technological neutrality in regulation ("same risk, same activity, same treatment") and the achievement of a level playing field, which the entire discipline of financial intermediation seeks to attain. With autonomous artificial intelligence, new protective needs arise against a regulatory framework focused solely on human conduct (commission or omission). It is not always possible to identify human involvement in causing harm, and therefore, the existing regulations do not seem fully adequate in addressing «the risks and significance of the risks» posed by new trading methods for clients and the financial system. The European Parliament Resolution on Financial Technology dated May 17, 2017, also expresses this view, highlighting that the principle of technological neutrality does not allow the entire financial sector to be subject to identical regulations for both traditional and digital activities.

It has been observed that strong AI systems can manipulate the market, both by rapidly placing and cancelling execution orders within milliseconds and through dynamics that are less rapid but still difficult to comprehend due to the opacity of the algorithmic black box. The commission of illicit acts, therefore, entails difficulties in providing evidence to identify the responsible party, ascertain guilt or intent, and establish causal links. However, especially regarding cases of trade-based manipulation, the provisions of MAR restrain (perhaps inadvertently) the use of strong AI systems by requiring all parties whose conduct impacts price formation to be able to provide justifications for their actions. Paradoxically, strong AI systems, being black boxes, fail to fulfil this requirement.

Even in the hypothetical perspective of enabling the conscious use of such systems, which potentially yield economic benefits for society, the study identifies three alternative solutions aimed at suppressing the conduct of AI systems that, acting autonomously and unpredictably compared to the producer, programmer, or user, engage in harmful behaviours or specifically undermine market integrity. However, each of these solutions presents specific critical aspects depending on the areas of legislation involved because of non-human agents' illicit behaviour.

The first proposal entails granting legal personality to more advanced artificial intelligence systems. Nevertheless, assigning a legal function like that established for legal persons would be a mere *fictio juris* that would not solve the problem - particularly challenging in criminal and administrative contexts - of attributing responsibility traditionally based on criteria of fault and intent, nor that of enforcing imposed sanctions. The difficulties of applying sanctions to an artificial agent must be carefully evaluated, as well as the fact that, particularly concerning pecuniary sanctions and compensation for damages, configuring legal personality for AI systems would still require identifying entities required to establish a separate estate for this purpose.

The second proposed solution aims to overcome the difficulties associated with directly attributing responsibility to the artificial agent by instead attributing the materially committed offenses to the objective responsibility of the person who (producer, programmer, or even user), in deploying the AI system, created the risk - later actually occurred - of the illicit act, irrespective of awareness of such risk. However, it is evident that this solution, albeit hardly compatible with traditional principles of criminal imputation, could significantly compromise the drive for technological innovation in the relevant sector, even if exclusively adopted in civil or administrative fields.

The third proposal entails a departure from the concept of responsibility itself, focusing on socializing the damage (*recte*, its cost), shifting the burden not so much onto the individual but rather onto the community as a whole. This approach has the advantage of not curbing technological development and simultaneously fostering a more efficient economic system. However, this option also presents some disadvantages, including potential impacts of mutualization on market dynamics.

Within the EU, a solution that does not inhibit technological development but prevents the widespread diffusion of illicit acts committed by AI systems could lie in the already incorporated proposal of the Regulation (EU) on Artificial Intelligence. It seeks to reconcile the use of artificial intelligence with the protection of fundamental rights through a risk-based approach combining the application of the precautionary and preventive principles for AI systems with unacceptable and high risks, respectively.

To attribute responsibility to the producer, programmer, or user, it should not be necessary that these entities foresee the event or its possible occurrence; it should suffice that they create a risk capable of causing the event.

In the financial field, applying this *regula iuris* could lead to the expansion of activities and services qualified as "high risk", including trading, with the corresponding obligation for the entities in the production chain to comply with a series of requirements; failure to do so would result in administrative liability.

Whichever solution is chosen, it must strike a balance between not excessively constraining technological development and the need to ensure adequate levels of protection for the proper functioning of the market and, more generally, the equal dignity of reintegrating the legal positions harmed by the actions of artificial agents.

Bibliography

AA.VV., *Intelligenza artificiale nel credit scoring. Analisi di alcune esperienze nel sistema finanziario italiano*, in *Questioni di Economia e Finanza* (*Occasional Papers*), Banca d'Italia (bancaditalia.it), n. 721, ottobre 2022.

ABBOTT R. – SARCH A., *Punishing Artificial Intelligence: Legal Fiction or Science Fiction*, in *UC Davis Law Rev.*, Vol. 53, 2019, pp. 323 ss.

ABRIANI M., *Gli algoritmi minacciano il libero arbitrio?*, in *MichePost*, 16 maggio 2020.

ABRIANI N. – SCHNEIDER G., *Diritto delle imprese e intelligenza artificiale*, Bologna, 2021.

ABRIANI N., *Prolegomeni a uno studio sull'impatto dell'intelligenza artificiale sulla corporate governance*, in *Il nuovo diritto delle società*, n. 3, 2020, pp. 261 ss.

ADRIAN J., *Informational Inequality? How High Frequency Traders use premier access to information to prey on institutional investors*, in *Duke L. & Techn. Rev.*, Vol. 14, n. 1, 2016, pp. 261 et seq.

AFM, *Machine Learning in Trading Algorithms – Application by Dutch Proprietary Trading Firms and Possible Risks*, March, 2023.

AGGARWAL R.K. – WU G., *Stock Market Manipulations*, in *Journal of Business*, 2006, Vol. 79, n. 4, pp. 1915 et seq.

ALGERI L., *Intelligenza artificiale e polizia predittiva*, in *Dir. pen. proc.*, n. 6, 2021, pp. 724 et seq.

ALLDRIDGE P., *The Doctrine of Innocent Agency*, in *Crim. L. Forum*, Vol. 2, 1990, pp. 45 et seq.

ALLEN F. – LITOV L. – MEI J., *Large Investors, Price Manipulation, and Limits to Arbitrage: An Anatomy of Market Corners*, in *Review of Finance*, 2006.

ALLENA M.– VACCARI S., *Diritto al silenzio e autorità di vigilanza dei mercati finanziari*, in *Riv. dir. banc.* (*rivista.dirittobancario.it*), n. 3, 2022, pp. 689 et seq.

ALPA G., *Fintech: un laboratorio per i giuristi*, in *Contr. impr.*, n. 2, 2019, pp. 377 et seq.

ALPA G., *Quale modello normativo europeo per l'intelligenza artificiale*, in *Contr. impr.*, n. 4, 2021, pp. 1003 et seq.

AMATI E., *Abusi di mercato e sistema penale*, Torino, 2012, pp. 171 et seq.

AMATI E., *L'illecito amministrativo di manipolazione del mercato e le persistenti criticità del doppio binario sanzionatorio*, in *Giur. comm.*, n. 2, 2021, pp. 263 et seq.

AMIDEI A., *Intelligenza artificiale e product liability: sviluppi del diritto dell'Unione Europea*, in *Giur. it.*, n. 7, 2019, pp. 1715 et seq.

AMIDEI A., *Le responsabilità da intelligenza artificiale tra product liability e sicurezza del prodotto*, in AA.VV., *XXVI Lezioni di Diritto dell'Intelligenza Artificiale*, 2021, pp. 149 et seq.

AMOROSO D. – TAMBURRINI G., *I sistemi robotici ad autonomia crescente tra etica e diritto: quale ruolo per il controllo umano?*, in *BioLaw Journal – Rivista di BioDiritto* (*biodiritto.org*), n. 1, 2019, pp. 33 et seq.

ANNUNZIATA F., *Abusi di mercato e tutela del risparmio*, Torino, 2006.

ANNUNZIATA F., *Un Robinson Crusoe alla borsa di Londra*, La Vita Felice, 2019.

ANNUNZIATA F., *Intelligenza artificiale e comunicazione al mercato di informazioni privilegiate*, in BOGGIO L. (a cura di), *Intelligenza artificiale e diritto dell'impresa*, *Giur. it.*, n. 8-9, 2022, pp. 2031 et seq.

ANNUNZIATA F., *Artificial intelligence and market abuse legislation. A European perspective*, Edward Elgar, 2023 (dattiloscritto, in corso di pubblicazione, consultato per gentile concessione dell'Autore).

ARDUINI S., *La "scatola nera" della decisione giudiziaria: tra giudizio umano e giudizio algoritmico*, in *BioLaw Journal – Rivista di BioDiritto* (*biodiritto.org*), n. 2, 2021, pp. 453 et seq.

ASARO P.M., *A Body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics*, in LIN P. –ABNEY K. – BEKEY G. (eds.), *Robot Ethics: The Ethical and Social Implications of Robotics*, Cambridge, 2012, pp. 169 et seq.

AVGOULEAS E., *The Mechanics and Regulation of Market Abuse*, Oxford University Press, 2005.

AZZUTTI A. – RING W.G. – STIEHL H.S., *Machine learning, market manipulation and collusion on capital markets: why the "black box" matters*, in *EBI Working Paper Series* (*ebi-europa.eu*), n. 84, 2021.

AZZUTTI A. – RING W.G. – STIEHL H.S., *Machine Learning, Market Manipulation, and Collusion on Capital Markets: Why the "Black Box" Matters*, in *U. Pa. J. Int'l L.*, Vol. 43, 2021, pp. 80 et seq.

AZZUTTI A. – RING W.G. – STIEHL H.S., *The Regulation of AI trading from an AI Life Cycle Perspective*, in *EBI Working Paper Series* (*ebi-europa.eu*), n. 130, 2022.

BACKUS M. – CONLON C. – SINKINSON M., *The common ownership hypothesis: Theory and evidence*, in *Economic Studies at Brookings*, January 2019.

BAINBRIDGE S.M., *The New Investor Cliffhanger*, in *UCLA L. Rev. Disc.*, Vol. 61, 2013, pp. 678 et seq.

BAINBRIDGE S.M., *An overview of insider trading law and policy: An introduction to the insider trading research handbook*, in *Research Handbook on Insider Trading, Stephen Bainbridge*, Edward Elgar Publishing Ltd, 2013, pp. 12-15.

BARBARO C., *Lo studio di fattibilità di un nuovo quadro normativo sulla concezione, lo sviluppo e l'applicazione dei sistemi di Intelligenza Artificiale sulla base delle norme del Consiglio d'Europa. Il lavoro del Comitato ad hoc sull'intelligenza artificiale del CdE*, in *Questione Giustizia*, 28 aprile 2021, pp. 1 et seq.

BARLAAM R., *Incidente mortale, Uber sospende test su guida autonoma*, in *Il Sole 24 ore*, 20 marzo 2018, p. 34.

BAROCAS S. – SELBST A.D., *Big Data's disparate impact*, in *Cal. Law Rev.*, Vol. 104, 2016, pp. 671 et seq.

BARONE G., *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della Risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cass. pen.*, n. 3, 2022, pp. 1180 et seq.

BARTALENA A., *O.p.a. per* delisting e insider trading*: brevi riflessioni sull'*insider *di sé stesso*, in *Banca borsa tit. cred.,* n. 6, 2018, pp. 2617 et seq.

BASILE F., *Diritto penale e intelligenza artificiale*, in *Giur. it.*, Suppl. 2019, pp. 67 et seq.

BASILE F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo* (*dirittopenaleuomo.org*), n. 10, 2019, pp. 1 et seq.

BASSINI M. – LIGUORI L. – POLLICINO O., *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in Pizzetti F.(a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

BATTELLI E., *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e tutela della persona*, in *Dir. fam. pers.*, n. 3, 2022, pp. 1096 et seq.

BAUERMEISTER T. – GROBE T., *Personen im Recht – über Rechtssubjekte und ihre Rechtsfähigkeit*, in *ZGR*, 2022, pp. 730 et seq.

BECK S., *Google Cars, Software Agents, Autonomous Weapons Systems. New Challenges for Criminal Law?*, in HILGENDORF E. – SEIDEL U. (eds.), *Robotics, Autonomics, and the Law*, Baden, 2017, pp. 227 et seq.

BENABOU R. – LAROQUE G., *Using Privileged Information to Manipulate Markets: Insiders, Gurus and Credibility*, in *Quarterly Journal of Economics*, 1992.

BENCINI M. – TODINI V., *Gli abusi di mercato*, in BENCINI M. – FANFANI L. – PELIZZARI S. – TODINI V., *Profili penali della tutela del risparmio. Truffa, abusi di mercato e gestione patrimoniale*, Milano, 2021, pp. 153 et seq.

BENFATTO L., *Microsoft blocca il* software Tay*: era diventato razzista e xenofobo*, in *Il Sole 24 ore Tecnologia*, 25 marzo 2016.

BERTANI M., Trading algoritmico *ad alta frequenza e tutela dello* slow trader, in *Analisi giur. econ.*, n. 1, 2019, pp. 261 et seq.

Bevivino G., *Situazioni giuridiche "soggettive" e forme di tutela delle intelligenze artificiali*, in *Nuova giur. civ. comm.*, n. 4, 2022, pp. 899 et seq.

Bhattacharya U., *Insider trading controversies: A literature review*, in *Annu. Rev. Financ. Econ.* Vol. 6, n. 1, 2014, pp. 385-403.

Bhattacharya U. – Hazem D., *The world price of insider trading*, in *The journal of Finance*, Vol. 57, n. 1, 2002, pp. 75-108.

Biais B. – Foucault T., *HFT and market quality*, in *Bankers, Markets & Investors*, Vol. 128, n. 1, 2014, pp. 5-19.

Bindi E.– Luccarelli P. – Pisaneschi A., *Le sanzioni della Banca d'Italia* e *della Consob*, in *Giur. comm.*, n. 3, 2021, pp. 553 et seq.

Bird K.R., *Natural and probable consequences doctrine: "Your acts are my acts!"*, in *W. St. UL Rev*, Vol. 34, 2006, pp. 43 et seq.

Black B., *Behavioral Economics and Investor Protection: Reasonable Investors, Efficient Markets*, in *Loy. U. Chi. L.J.*, Vol. 44, 2013, pp. 1493 et seq.

Bocchini E., *Contro la "soggettivizzazione" dell'intelligenza artificiale*, in *Il Nuovo Dir. Soc.*, n. 2, 2023, pp. 195 et seq.

Bollen J. – Mao H. – Zeng X., *Twitter mood predicts the stock market*, in *Journal of computational science*, Vol. 2, n. 1, 2011, pp. 1-8.

Borsari R., *Intelligenza artificiale* e *responsabilità penale: prime considerazioni*, in *Rivista di diritto dei media* (*medialaws.eu*), n. 3, 2019, pp. 262 et seq.

Bottazzini P., *Intelligenza artificiale. I sei big dettano le regole*, in *Pagina 99*, 8 ottobre 2016, pp. 20-21.

Bracke P. – Datta A. – Jung C. – Sen S., *Machine Learning exlainability in finance: an application to default risk analysis*, in *Staff Working Paper*, Bank of England, August 2019.

Buchard C., *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. it. dir. proc. pen.*, n. 4, 2019, pp. 1909 et seq.

Buckley R.P. –Arner D.W. – Zetzsche D.A. – Selga E., *The Dark Side of Digital Financial Transformation: The new Risks of FinTech and the Rise of RegTech*, in *EBI* (*European Banking Institute*), *Working Paper Series*, n. 54, 2019, pp. 1 et seq.

Cadorin F., *OPA per il* "delisting" *fra* "insider" *di se stesso ed efficienza del mercato*, in *Giur. comm.*, n. 1, 2019, pp. 105 et seq.

Caivano V. – Ciccarelli S. – Di Stefano G. – Fratini M. – Gasparri G. – Giliberti M. –Linciano N. – Tarola I., *Il Trading ad alta frequenza*, in *Discussion papers CONSOB* (consob.it), n. 5, 2012.

Caivano V., *The impact of high-frequency trading on volatility. Evidence from the Italian market*, in *Quaderni di finanza CONSOB* (consob.it), n. 80, marzo 2015.

CALANDRA BUONAURA V., *Sub art. 184*, in *Commentario breve al Testo Unico della Finanza*, Padova, 2020, pp. 1228 et seq., especially pp. 1236-1241.

CALIFANO L., *La libertà di manifestazione del pensiero ... in rete; nuove frontiere di esercizio di un diritto antico.* Fake news, hate speech *e profili di responsabilità dei* social network, in *federalismi.it*, n. 26, 2021, pp. 1 et seq.

CALZOLARI L., *La collusione fra algoritmi nell'era dei* big data*: l'imputabilità alle imprese delle "intese 4.0" ai sensi dell'art. 101 TFUE*, in *Rivista di diritto dei media* (*medialaws.eu*), n. 3, 2018, pp. 21 et seq.

CAMERER C.F., *Can Asset Markets Be Manipulated? A field Experiment with Racetrack Betting*, in *Journal of Political Economy*, 1988.

CANEPA A., Social media *e* fin-influencers *come nuovi fonti di vulnerabilità digitale nell'assunzione delle decisioni di investimento*, in *Riv. trim. dir. econ.* (*fondazionecapriglione.luiss.it*), Suppl. al n. 1, 2022, pp. 307 et seq.

CANESCHI G., Nemo tenetur se detegere *anche nei procedimenti amministrativi sanzionatori? La parola alla Corte di giustizia*, in *Cass. pen.*, n. 2, 2020, pp. 579 et seq.

CANZIO G., *Intelligenza artificiale e processo penale*, in *Cass. pen.*, n. 3, 2021, pp. 797 et seq.

CAPPELLINI A., *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale*, in *disCrimen* (*discrimen.it*), 27 marzo 2019, pp. 1 et seq.

CAPPELLINI A., *Profili penalistici delle* self-driving cars, in *Dir. pen. cont.* (*archiviodpc.dirittopenaleuomo.org*), n. 2, 2019, pp. 325 et seq.

CARCATERRA A., *Macchine autonome e decisione robotica*, in A. Carleo (a cura di), *Decisione robotica*, Bologna, 2019, pp. 38 et seq.

CARLINI V., *I robot e le scelte oscure spesso inspiegabili per l'uomo*, in *Il Sole 24 ore*, 21 febbraio 2018, pp. 1 e 25.

CASONATO C. – MARCHETTI B., *Prime osservazioni sulla proposta di regolamento della Commissione UE in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto* (*biodiritto.org*), n. 3, 2021, pp. 415 et seq.

CATALANO S., *La vicenda decisa dalla sentenza n. 84 del 2021 della Corte costituzionale: un esempio di "buon dialogo" fra Corti*, in *Forum di Quad. cost.* (*forumcostituzionale.it*), n. 4, 2021, pp. 295 et seq.

CAZZELLA G., *Tecnologia e intelligenza artificiale nei mercati finanziari; le ricadute penali della "*new market manipulation*"*, Tesi di Laurea, Università Cattolica del Sacro Cuore – Milano, 2019/2020,

CELOTTO A., *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi giur. econ.*, n. 1, 2019, pp. 47 et seq.

CHOPRA S. – WHITE L.F., *A Legal Theory for Autonomous Artificial Agents*, Ann Arbor, 2011.

Christensen H.B. – Luzi H. – Christian L., *Capital-market effects of securities regulation: Prior conditions, implementation, and enforcement*, in *The Review of Financial Studies*, 29.11.2016, pp. 2885-2924.

Cirillo G.P., *I soggetti giuridici digitali*, in *Contr. impr.*, n. 2, 2020, pp. 573 et seq.

Coduti D., *Il diritto al silenzio nell'intreccio tra diritto nazionale, sovranazionale e internazionale: il caso D.B. c. Consob*, in *federalismi.it*, n. 22, 2021, pp. 121 et seq.

Coeckelbergh M., *Artificial Intelligence, Responsibility Attribution, and a Relational justification of Explainability*, in *Science and Engineering Ethics*, Vol. 26, 2020, pp. 2051 et seq.

Colangelo G., *Artificial Intelligence and Anticompetitive Collusion: From the 'Meeting of Minds' towards the 'Meeting of ALgorithms'*, in *Stanford-Vienna TTLF Working Paper*, No. 74 (http://ttlf.standford.edu.).

Comandé G., *Intelligenza artificiale e responsabilità tra* liability e accountability. *Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi giur. econ.*, n. 1, 2019, pp. 169 et seq.

Consulich F. – Mucciarelli F., *Informazione e tutela penale dei mercati finanziari nello specchio della normativa eurounitaria sugli abusi di mercato*, in *Soc.*, n. 2, 2016, pp. 179 et seq.

Consulich F., *Il nastro di Mobius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca borsa tit. cred.*, n. 2, 2018, pp. 195 et seq.

Consulich F., *Il principio di autonomia della responsabilità dell'ente. Prospettive di riforma dell'art. 8*, in *Rivista 231*, n. 4, 2018, pp. 197 et seq.

Consulich F., *Il prisma del* ne bis in idem *nelle mani del Giudice eurounitario*, in *Dir. pen. proc.*, n. 7, 2018, pp. 949 et seq.

Consulich F., *La giustizia e il mercato*, Milano, 2010.

Consulich F., *Manipolazione dei mercati e diritto eurounitario*, in *Soc.*, n. 2, 2016, pp. 203 et seq.

Contaldi G., *Intelligenza artificiale e dati personali*, in *Ord. int. dir. um.*, n. 5, 2021, pp. 1193 et seq.

Contissa G. – Lasagni G. – Sartor G., *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di Internet*, n. 4, 2019, pp. 619 et seq.

Cosme Jr. O., *Regulating High-Frequency Trading: The Case for Individual Criminal Liability*, in *J. Crim. L. & Criminology*, Vol. 109, Issue 2, 2019, pp. 386 et seq.

Council of Europe Study, *Responsibility and IA*, 2019.

Crisci S., *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm.*, n. 10, 2018, pp. 1787 et seq.

CUPELLA M., *I mercati finanziari a confronto con nuove tecnologie e Social Media: le prospettive penalistiche dell'*Affaire GameStop, in *Bocconi Legal Papers*, n. 16, 2021, pp. 145 et seq.

D'ALESSANDRO F., *Market Abuse*, in CERA M. – PRESTI G. (a cura di), *Il testo unico finanziario*, Vol. II, Bologna, 2020, pp. 2166 et seq.

DA ROLD C., *Quando gli algoritmi sbagliano spesso sono solo disinformati*, in *Il Sole 24 ore*, 18 settembre 2022, p. 14.

DANAHER J., *Robots, Law and the Retribution Gap*, in *Ethics and Information Technology*, Vol. 18, 2016, pp. 299 et seq.

DAVOLA A. – PARDOLESI R., *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?*, in *Danno resp.*, n. 5, 2017, pp. 616 et seq.

DE FELICE M., *Decisione robotica negoziale. Nuovi «punti di presa» sul futuro*, in Carleo A., *Decisione robotica*, Bologna, 2019, p. 192.

DE JONG F. – RINDI B., *The microstructure of financial markets*, Cambridge University Press, 2009.

DE LIMA SALGE C.A. – BERENTE N., *Is that social bot behaving unethically?*, in *Communications of the ACM*, Vol. 60, Issue 9, 2017, pp. 29-31.

DENOZZA F., *La nozione di informazione privilegiata tra "*Shareholder Value*" e "*Socially Responsible Investing*"*, in *Giur. comm.*, n. 5, 2005, pp. 593 et seq.

DEODATO C., *Sanzioni formalmente amministrative e sostanzialmente penali: i problemi procedurali connessi all'applicazione delle sanzioni Consob in materia di materia di* market abuse *(e alcune soluzioni)*, in *federalismi.it*, n. 23, 2019, pp. 1 et seq.

DI CIOMMO F., *La conclusione e l'esecuzione automatizzata dei contratti (*smart contract*)*, in CASSANO G. – DI CIOMMO F. – RUBINO DE RITIS M. (a cura di), *Banche, intermediari e* FinTech, Milano, 2021, pp. 79 et seq.

DI CIOMMO F., Smart contract *e (non-) diritto. Il caso dei mercati finanziari*, in *Nuovo diritto civile*, n. 1, 2019, pp. 257 et seq.

DIAMANTIS M.E., *The Extended Corporate Mind: When Corporations Use AI to Break the Law*, in *North Carolina Law Review*, Vol. 98, n. 4, 2020, pp. 898 et seq.

DOMIGOS P., *The Master Algorithm*, New York, 2015.

DONATI F., *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, in *Dir. Un. eur.*, nn. 3-4, 2021, pp. 453 et seq.

DONATI F., *Intelligenza artificiale e giustizia*, in *Riv. AIC* (*rivistaaic.it*), n. 1, 2020, pp. 415 et seq.

DONATI F., *L'art. 21 della Costituzione settanta anni dopo*, in *Rivista di diritto dei media* (*medialaws.eu*), n. 1, 2018, pp. 93 et seq.

DUFF R.A., *The Realm of Criminal Law*, Oxford, 2018.

DUFFEE D. – FOUCAULT T. – VELDKAMP L. – VIVES X., *Technology and Finance*, CEPR, 2022.

ENRIQUES L. - ZETZSCHE D.A., *Corporate Technologies and the Tech Nirvana Fallacy*, *ECGI Law Working Paper*, March 2020

EUROPEAN COMMISSION, *Ethics Guidelines for Trustworthy AI*, 2018.

FAMA E.F., *Efficient Capital Markets. A Review of Theory and Empirical Work*, in *Journal of Finance*, Vol. 25, 1970, pp. 373 et seq.

FARES G., *Diritto al silenzio, soluzioni interpretative e controlimiti: la Corte costituzionale chiama in causa la Corte di giustizia*, in *dirittifondamentali.it*, n. 1, 2020, pp. 57 et seq.

FEDERICI D., Insider *di sé stesso e abuso di informazioni privilegiate: la Corte di Cassazione conferma la punibilità anche del creatore della notizia*, in *Sistema Penale* (*sistemapenale.it*), 13 ottobre 2021.

FILIPPELLI M., *La collusione algoritmica*, in *Orizz. dir. comm.* (*orizzontideldirittocommerciale.it*), fasc. speciale, 2021, pp. 375 et seq.

FINOCCHIARO G., *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ.*, n. 2, 2018, pp. 441 et seq.

FINOCCHIARO G., *Intelligenza artificiale e protezione dei dati personali*, in *Giur. it.*, n. 7, 2019, pp. 1670 et seq.

FINOCCHIARO G., *Intelligenza artificiale e responsabilità*, in *Contr. impr.*, n. 2, 2020, pp. 713 et seq.

FINOCCHIARO G., *La conclusione del contratto telematico mediante i software agents: un falso problema giuridico?*, in *Contr. impr.*, n. 2, 2002, pp. 500 et seq.

FINOCCHIARO G., *La proposta di Regolamento sull'intelligenza artificiale: il modello basato sulla gestione del rischio*, in *Dir. inf.*, n. 2, 2022, pp. 303 et seq.

FISCHEL D.R. – ROSS D.J., *Should the Law Prohibit Manipulation in Financial Markets*, in *Harvard Law Review*, Vol. 105, 1991, pp. 503 et seq.

FISHER J. – CLIFFORD A. – DINSHAW F. – WERLE N., *Criminal Forms of High Frequency Trading on the Financial Markets*, in *Law & Fin. Mkt. Rev.*, Vol. 9, 2015, pp. 113 et seq.

FISHMAN M.J. – HAGERTY K.M., *Insider Trading and the Efficiency of Stock Prices*, in *The Rand Journal of Economics*, Vol. 23, No. 1 (Spring1992), pp. 106 et seq.

FLICK G.M. – NAPOLEONI V., *Cumulo tra sanzioni penali e amministrative: doppio binario o binario morto? "Materia penale", giusto processo e ne bis in idem nella sentenza della Corte Edu, 4 marzo 2014, sul market abuse*, in *Riv. AIC* (*rivistaaic.it*), n. 3, 2014, 11 luglio 2014, nonché in *Riv. soc.*, n. 5, 2014, pp. 953 et seq.

FLORIDI L. – SANDERS J.W., *In the Morality of Artificial Agents*, in *Mind and Machines*, Vol. 14, 2004, pp. 349 et seq.

Foucalt T. – Pagano M. – Röell A., *Market liquidity: theory, evidence, and policy*, Oxford University Press, USA, 2013.

Fox-Glosten M.B. – Rauterberg G.V., *The New Stock Market: Sense and Nonsense*, in *Duke L. J. 191*, Vol. 65, 2015, pp. 272 et seq.

Frosini T.E., *L'orizzonte giuridico dell'intelligenza artificiale*, in *Dir. inf.*, n. 1, 2022, pp. 465 et seq.

Fullerton J., *High-frequency Trading is a Blight on Markets That the Tobin Tax Can Cure*, in *The Guardian*, 4 April 2014 (https://www.theguardian.com).

Fusaro A., *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo*, in *Nuova giur. civ. comm.*, n. 6, 2020, pp. 1344 et seq.

Gaggi M., *Perché l'intelligenza artificiale spaventa i re della tecnologia*, in *Corriere della Sera*, 30 marzo 2023, pp. 1-22.

Garber P.M., *Famous First Bubbles*, The MIT Press, 2000.

Gargantini M. – Siri M., *Il "prezzo dei prezzi". Una soluzione di mercato ai rischi dell'*high frequency trading*?*, in *Riv. soc.*, n. 5-6, 2019, pp. 1100 et seq.

Gatta G.L., "Nemo tenetur se detegere" *e procedimento amministrativo davanti alla Consob per l'accertamento dell'abuso di informazioni privilegiate: la Cassazione solleva questione di legittimità costituzionale dell'art. 187-*quinquiesdecies *T.U.F.*, in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*), 27 aprile 2018.

Genovese A., *Il controllo del giudice sulla regolazione finanziaria*, in *Banca borsa tit. cred.*, n. 1, 2017, pp. 49 et seq.

Ghetti R., *Robo-advice: automazione e determinismo nei servizi di investimento ad alto valore aggiunto*, in *Banca borsa tit. cred.*, n. 4, 2020, pp. 540 et seq.

Ghidini G., *Ma chi paga i danni. Se il robot combina guai?*, in *Corriere della Sera*, 13 febbraio 2023, p. 6.

Giannini A., *Intelligenza artificiale, human oversight e responsabilità penale: prove d'impatto a livello europeo*, in *disCrimen* (*discrimen.it*), 21 novembre 2022, pp. 1 et seq.

Giudici P. – Raffinetti E., *Shapley-Lorenz eXplainable artificial intelligence. Expert systems with applications*, Vol. 167, 2021, pp. 114104.

Godell J.W. – Kumar S. – Lim W.M. – Pattnaik D., *Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters from bibliometric analysis*, in *Journal of Behavioral and Experimental Finance*, Vol. 32, 2021, pp. 100577.

Goshen Z. – Parchomovsky G., *The Essential Role of Securities Regulation*, in *Duke L.J.*, Vol. 55, 2006, pp. 733 et seq.

GRECO G.L., Credit scoring *5.0 tra* Artificial Intelligence Act *e Testo Unico Bancario*, in *Riv. trim. dir. econ.* (*fondazionecapriglione.luiss.it*), Suppl. n. 3, 2021, pp. 74 et seq.

GROSSMAN S. – STIGLITZ J., *Information and competitive price system*, in *American Economic Review*, 1976.

GUBLER Z.J., *Reconsidering the Institutional Design of Federal Securities Regulation*, in *William Mary L. Rev.*, Vol. 56, Issue 2, 2014, pp. 409 et seq.

GUNKEL D.J., *Mind the Gap: Responsible Robotics and the Problem of Responsibility*, in *Ethics and Information Technology*, Vol. 22, 2017, pp. 307 et seq.

HALDANE A., *The age of asset management?." Speech at the London Business School 4.4*, 2014.

HALLEVY G., *The Basic Models of Criminal Liability of AI Systems and Outer Circles*, 11 June 2019 (su SSRN: https://ssrn.com/abstract=3402527).

HALLEVY G., *The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control*, in *Akron Intellectual Property Journal*, Vol. 4, Issue 2, 2010, pp. 170 et seq.

HALLEVY G., *The Criminal Liability of Artificial intelligence Entities*, in *Akron Intellectual Property Journal*, Vol. 4, Issue 2, 2010, pp. 171 et seq.

HALLEVY G., *Unmanned vehicles—Subordination to criminal law under the modern concept of criminal liability*, in *Journal of Law, Information and Science*, Vol. 21, 2012, p. 200.

HANSEN J., *Ci sono anche i pc delinquenti*, in *ItaliaOggi*, 11 maggio 2019, pp. 1 e 11.

HART H.L.A., *Punishment and Responsibility: Essays in the Philosophy of Law*, Oxford, 2008.

HAYEK F.A., *The Use of Knowledge in Society*, in *The Amer. Econ. Rev.*, Vol. 35, n. 4, 1945, pp. 519 et seq.

HILGENDORF E., *Autonome Systeme, künstliche Intelligenz und Roboter*, in *Festschrift für Thomas Fischer*, München, 2018, pp. 111 et seq.

HILLION P. – SUOMINEN M., *The Manipulation of Closing Prices*, in *Journal of Financial Markets*, 2004, p. 7.

HOFFMAN D.A., *The "Duty" to Be a Rational Shareholder*, in *Minn. L. Rev.*, Vol. 90, 2006, pp. 537 et seq.

HU H.T.C., *Too Complex to Depict? Innovation, 'Pure Information,' and the SEC Disclosure Paradigm*, in *Texas L. Rev.*, Vol. 90, n. 7, 2012, pp. 1705 et seq.

HU Y., *Robot Criminals*, in *Univ. Mich. Journal of Law Reform*, Vol. 52, n. 2, 2019, pp. 487 et seq.

HUANG P.H., *Moody Investing and the Supreme Court: Rethinking the Materiality of Information and the Reasonableness of Investors*, in *Sup. Ct. Econ. Rev.*, Vol. 13, 2005, pp. 99 et seq.

HULL J., *Opzioni futures e altri derivati*, Pearson, 2022.

IRTI N., *L'ordine giuridico del mercato*, Roma-Bari, 2003.

IRTI N., *Scambi senza accordo*, in *Riv. trim. dir. proc. civ.*, n. 2, 1998, pp. 347 et seq.

JIANG G. – MAHONEY P.G.– MEI J., *Market Manipulation: A Comprehensive Study of Stock Pools*, in *Journal of Financial Economics*, 2005, p. 77.

KADISH S.H., *Complicity, Cause and Blame: A Study in the Interpretation of Doctrine*, in *Calif. L. Rev.*, Vol. 73, n. 2, 1985, pp. 323 et seq.

KAPLAN J., *Artificial Intelligence: What Everyone Needs to Know*, Oxford, 2016.

KERJAN E.M., *An Idea Whose Time Has Come*, in Kerjan E.M., *The Irrational Economist: Making Decisions in a Dangerous Word*, New York, 2010.

KERKEMEYER A., *Herausforderungen des Blockchain-Netzwerks für das Kapitalmarktrecht*, in *ZGR*, 2020, p. 673.

KING M. – ROELL A. – KAY J. – WYPLOSZ C., *Insider trading*, in *Econ. Pol.*, 1988.

KIRCHER A.S., *Corporate Criminal Liability Versus Corporate Securities Fraud Liability: Analyzing the Divergence in Standards of Culpability*, in *Am. Crim. L. Rev.*, Vol. 46, 2009, pp. 157 et seq.

KIRILENKO A. - A.S. KYLE – M. SAMADI – T. TUZUN, *The flash crash: High-frequency trading in an electronic market*, in *The Journal of Finance*, Vol. 72, n. 3, 2017, pp. 967-998.

KONERTZ R. – SCHÖNHOF R., *Das technische Phäneomen "Künstliche Intelligenz" im allgemeinen Zivilrecht*, Baden-Baden, 2020.

KOOPS B.J. – HILDEBRANDT M. – JAOUET-CHIFFELLE D.O., *Bridging the Accountability Gap: Rights for New Entities in the Information Society?*, in *Minn. J. L. Sci. & Tech*, Vol. 11, 2010, pp. 497 et seq.

KORSMO C., *High-Frequency Trading: A Regulatory Strategy*, in *U. Rich. L. Rev.*, Vol. 48, 2014, pp. 523 et seq.

KRIPKE H., *The Mith of Informed Layman*, in *Bus. Law.*, Vol. 2, n. 2, 1973, pp. 631 et seq.

KYLE AS., *Continuous auctions and insider trading*, in *Econometrica*, 1985.

KYLE AS., *Informed speculation with imperfect competition*, in *Review of Economic Studies*, 1989.

LA FAVE W.R., *Substantive Criminal Law*, Eagan, 2018.

LANA A., *Alexa sfida una bimba a inserire una moneta nella presa elettrica: Amazon aggiorna il* software, in *Corriere della sera*, 29 dicembre 2021.

LEANZA C., *Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel Terzo Millennio*, in *Resp. civ. prev.*, n. 3, 2021, pp. 1011 et seq.

LEDERMAN E., *Models for Imposing Corporate Criminal Liability: From Adaptation and Imitation Toward Aggregation and the Search for Self-Identity*, in *Buff. Crim. L. Rev.*, Vol. 4, 2000, pp. 641, 654 et seq.

LEDGERWOOD S.D. – CARPENTER P.R., *A Framework for the Analysis of Market Manipulation*, in *Rev. L. & Econ.*, Vol. 8, 2012, pp. 253 et seq.

LEGG S.– HUTTER M., *A collection of definitions of intelligence*, in *Frontiers in Artificial Intelligence and Applications*, Vol. 157, 2007, pp. 17 et seq. (https://arxiv.org).

LEVENS T.E., *Comment, Too Fast, Too Frequent? High Frequency Trading and Security Class Actions*, *U. Chi. L. Rev.*, Vol. 82, 2015, pp. 1515 et seq.

LEVINE R. - CHEN L. – LAI W., *Insider trading and innovation*, in *The Journal of Law and Economics*, Vol. 60, n. 4, 2017, pp. 749-800.

LEWIS M., *Flash Boys: A Wall Street Revolt*, New York-London, 2014.

LI X. – PANGJING W. – WENPENG W., *Incorporating stock prices and news sentiments for stock market prediction: A case of Hong Kong*, in *Information Processing & Management*, Vol. 57, n. 5, 2020, pp. 102212.

LIN T.C.W., *Artificial intelligence, finance, and the law*, in *Fordham Law Rev.*, Vol. 88, Issue 2, pp. 531 et seq.

LIN T.C.W., *Reasonable Investor(s)*, in *Boston Univ. L. Rev.*, Vol. 95, 2015, pp. 461 et seq.

LIN T.C.W., *The New Investor*, in *UCLA L. Rev.*, Vol. 60, 2013, pp. 678 et seq.

LIN T.C.W., *The new market manipulation*, in *Emory Law Journal*, Vol. 66, Issue 6, pp. 1252 et seq.

LIN T.C.W., *Vistas of Finance*, in *UCLA L. Rev. Disc.*, Vol. 61, 2013, pp. 78 et seq.

LINA D., *Could AI Agents Be Held Criminally Liable*, in *South Carolina L. Rev.*, Vol. 69, Issue 3, 2018, pp. 677 et seq.

LINCIANO N. – CAIVANO V. – COSTA D. – SOCCORSO P. – POLI T.N. – TROVATORE G., *L'intelligenza artificiale nell'asset e nel wealth management*, *Quaderni FinTech*, Consob, n. 9, 2022.

LOBIANCO R., *Veicoli a guida autonoma e responsabilità civile: regime attuale e prospettive di riforma*, in *Resp. civ. prev.*, n. 3, 2020, pp. 724 et seq. (Parte I), e n. 4, 2020, pp. 1080 et seq. (Parte II)

LOGLI A., *Poteri istruttori della Consob* e nemo tenetur se detegere, in *Giur. comm.*, n. 2, 2020, pp. 230 et seq.

LOMBARDO S., *L'*insider *di se stesso alla luce della decisione della Corte di Cassazione (civile)*, in *Giur. comm.*, n. 4, 2018, pp. 666 et seq.

Longo A., *Il robot che rompe paga. Stretta europea sui produttori*, in *la Repubblica*, 2 ottobre 2022, p. 28.

Longo M., *Allarme* social network*. Così insidiano le Borse*, in *Il Sole 24 ore*, 22 marzo 2018, pp. 1 e 3.

Loss L., *Fundamentals of Securities Regulation*, Boston MA, 1988.

Lübke J., *Preisabstimmung durch Algorithmen*, in *ZHR*, Vol. 185, 2021, pp. 723 et seq.

Lucantoni P., *L'*high frequency trading *nel prisma della vigilanza algoritmica del mercato*, in *Analisi giur. econ.*, n. 1, 2019, pp. 297 et seq.

Lucantoni P., *Mercato dei capitali, pandemia e informazione al mercato: il dibattito sull'evoluzione della disciplina degli abusi di mercato*, in *Banca borsa tit. cred.*, n. 4, 2022, pp. 549 et seq.

Luciani M., *La decisione giudiziaria robotica*, in *Riv. AIC* (*rivistaaic.it*), n. 3, 2018, 872 et seq.

Lupoi A., *La negoziazione algoritmica ad alta frequenza e la struttura dei mercati: due casi negli Stati Uniti*, in *Riv. dir. comm. e dir. gen. obbl.*, n. 1, 2019, pp. 1 et seq.

MacLeod Heminway J., *Female Investors and Secuities Fraud: Is the Reasonable Investor a Women?*, in *Wm. & Mary J. Women & L.*, Vol. 15, 2009, pp. 291 et seq.

Madden T.M., *Significance and the Materiality Tautology*, in *J. Bus. & Tech. L.*, Vol. 10, 2015, pp. 217 et seq.

Maggino F. – Cicerchia G., *Algoritmi, etica e diritto*, in *Dir. inf.*, n. 6, 2019, pp. 1161 et seq.

Magro M.B., *Biorobotica, robotica e diritto penale*, in Provolo D. – Riondato S. – Yenisey F., *Genetics, robotics, law punishment*, Padova, 2014, pp. 499 et seq.

Magro M.B., *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, in *Leg. pen.* (*legislazionepenale.eu*), 10 maggio 2020, pp. 1 et seq.

Magro M.B., *Robot, cyborg e intelligenze artificiali*, in Cadoppi A. – Canestrari S. – Manna A. –Papa M., *Cybercrime*, Torino, 2019, pp. 1180 et seq.

Manne HG., *Insider trading and the stock market*, New York Free Press, 1966.

Manne HG., *Insider trading, virtual markets, and the dog that did not bark*, in *J. Corp. Law*, 2005.

Manzini P., *Algoritmi collusivi e diritto antitrust europeo*, in *Mer. Conc. Reg.*, n. 1, 2019, pp. 163 et seq.

Marinucci G., *Innovazioni tecnologiche e scoperte scientifiche: costi e tempi di adeguamento delle regole di diligenza*, in *Riv. it. dir. proc. pen.*, n. 1, 2005, pp. 29 et seq.

Markham J.W., *Law Enforcement and the History of Financial Market Manipulation*, New York, 2014.

Martínez-Miranda E. – McBurney P. – Howard M.J.W., *Learning unfair trading: A market manipulation analysis from the reinforcement learning perspective*, 2016 IEEE.

Mattassoglio F., *La valutazione "innovativa" del merito creditizio del consumatore e le sfide per il regolatore*, in *Dir. banca*, n. 2, 2020, pp. 187 et seq.

Matthias A., *The responsibility gap: Ascribing responsibility for the actions of learning automata*, in *Ethics Inf. Tech.*, n. 6, 2004, pp. 175 et seq.

Maugeri M., *Offerta pubblica di acquisto e informazioni privilegiate*, in *Riv. dir. comm.*, n. 2, 2018, pp. 267 et seq.

Maugeri M., *Cripto-attività e abusi di mercato*, in *Oss. dir. civ. e comm.*, Speciale/2022, pp. 413 et seq.

McAllister A., *Stranger than science fiction: The rise of AI interrogation in the dawn of autonomous robots and the need for an additional protocol to the UN convention against torture*, in *Minnesota Law Review*, Vol. 101, 2017, pp. 2527 et seq.

Mccarthy J., *What Is Artificial Intelligence?*, 12 novembre 2007, (www.formal.stanford.edu).

McGowan M.J., *The Rise of Computerized High Frequency Trading: Use and Controversy*, in *Duke L. & Techn. Rev.*, Vol. 9, 2010, pp. 1 et seq.

McNamara S.R., *The Law and Ethics of High-Frequency Trading*, in *Minn. J.L. Sci. & Tech.*, Vol. 17, Issue 1, 2016, pp. 135 et seq.

Meloni C., *Command Responsibility in International Criminal Law*, The Hague, 2010, pp. 31 et seq.

Michetti M., *Diritto al silenzio* e insider trading*: il confronto tra Roma e Lussemburgo prosegue sulla via del dialogo (Corte costituzionale, sentenza n. 84/2021)*, in *Consulta online* (*giurcost.org*), n. 3, 2021, pp. 758 et seq.

Milia C., *Essays in Market Manipulation and Insider Trading*, PhD Thesis, Bocconi University, 2008.

Mill J.S., *Principles of Political Economy*, London: Longmans, Green and Co., 1921.

Mobilio G., *L'intelligenza artificiale e i rischi di una "*disruption*" della regolamentazione giuridica*, in *BioLaw Journal – Rivista di BioDiritto* (*biodiritto.org*), n. 2, 2020, pp. 401 et seq.

Montalenti P., *Abusi di mercato e procedimento Consob: il caso Grande Stevens e la Sentenza CEDU*, in *Giur. comm.*, n. 3, 2015, pp. 478 et seq.

Morelli M., *Implementing High Frequency Trading Regulation: A Critical Analysis of Current Reforms*, in *Mich. Bus. & Entrepreneurial L. Rev.*, Vol. 6, Issue 2, 2017, pp. 201 et seq.

MOSCO G.D., *L'intelligenza artificiale nei consigli di amministrazione*, in *Analisi giur. econ.*, n. 1, 2019, pp. 247 et seq.

MOSTACCI E., *L'intelligenza artificiale in ambito economico e finanziario*, in *DPCE online*, n. 1, 2022, pp. 361 et seq.

MOTTURA C., *Decisione robotica negoziale e mercati finanziari*, in CARLEO A., *Decisione robotica*, Bologna, 2019, pp. 265 et seq.

MUCCIARELLI F., *Sub art. 184*, in FRATINI M. – GASPARRI G. (a cura di), *Il testo unico della finanza*, Torino, 2012, pp. 2319 et seq.

MULTER M.K., *Open-Market Manipulation under SEC Rule 10b-5 and Its Analogues: Inappropriate Distinctions, Judicial Disagreement and Case Study; Ferc's Anti-manipulation Rule*, in *Sec Reg L. J.*, Vol. 39, 2011, p. 106.

NAPOLI C., *Algoritmi, intelligenza artificiale e formazione della volontà pubblica: la decisione amministrativa e quella giudiziaria*, in *Riv. AIC* (*rivistaaic.it*), n. 3, 2020, pp. 318 et seq.

NYHOLM S. – SMIDS J., *The Ethics of Accident-Algorithms for Self-Driving Cars: an Applied Trolley Problem?*, in *Ethical Theory and Moral Practice*, n. 19, 2016, pp. 1275 et seq.

OBERMEYER Z. – POWERS B. – VOGELI C. – MULLAINATHAN S., *Dissecting racial bias in an algorithm used to menage the health of populations*, in *Science Magazine*, 25 octuber 2019, Vol. 366, Issue 6464, pp. 447 et seq.

OLIVARES G.Q., *La Robotica ante et derecho penal*, in *Revista Electrónica de Estudios Penales y de la Seguridad*, n. 1, 2017, pp. 16 et seq.

OPPO G., *Disumanizzazione del contratto*, in *Riv. dir. civ.*, 1998, pp. 525 et seq.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *Algorithms and collusion. Competition Policy in the Digital Age*, 2017.

PAGALLO U., *From automation to autonomous systems: A legal phenomenology with problems of Accountability*, in *Proceedings of the 26th international joint conference on artificial intelligence*, in www.ijcai.org.

PAGELLA C., *L'inafferrabile concetto di "connessione sostanziale e temporale sufficientemente stretta": la Cassazione ancora sul* ne bis in idem e insider trading, in *Sistema penale* (*sistemapenale.it*), 9 gennaio 2020.

PAGELLA C., *Riflessi applicativi del principio di proporzione del trattamento sanzionatorio complessivamente irrogato per i fatti di* market abuse *e punibilità dell'*insider *di sé stesso: la Corte di Appello di Milano sul caso Cremonini*, in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*), 20 giugno 2019.

PALMISANO M., *L'abuso di mercato nell'era delle nuove tecnologie*, in *Dir. pen. cont.*, n. 2, 2019, pp. 129 et seq.

PANATTONI B., *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, in *Dir. inf.*, n. 2, 2021, pp. 317 et seq.

PAPA M., Future crimes*: intelligenza artificiale* e *rinnovamento del diritto penale*, in *dis-Crimen* (*discrimen.it*). 4 marzo 2020, pp. 9 et seq.

PARACAMPO M.T., *Robo-advisor, consulenza finanziaria* e *profili regolamentari: quale soluzione per un fenomeno in fieri?*, in *Riv. trim. dir. econ.* (*fondazionecapriglione.luiss.it*), n. 4, Suppl. 1, 2016, pp. 256 et seq.

PASCERI G., *Intelligenza artificiale, algoritmo* e machine learning, Milano, 2021.

PASQUALE F., *The black-box society: The secret algorithms that control money and information*, Cambridge-London, 2015.

PASSI C., *Esiste il* Self-insider*, ma va scagionato! Riflessioni intorno alla sua qualificazione giuridica*, in *Soc.*, n. 4, 2021, pp. 455 et seq.

PELLECCHIA E., *Profilazione* e *decisioni automatizzate al tempo della* black box society*: qualità dei dati* e *leggibilità dell'algoritmo nella cornice della* responsible research and innovation, in *Nuove leg. civ. comm.*, n. 5, 2018, pp. 1210 et seq.

PERRONE A., *Intelligenza artificiale* e *servizi di investimento*, in COSTA C. –MIRONE A.–PENNISI R.–SANFILIPPO P.M. –VIGO R. (a cura di), *Studi di diritto commerciale per Vincenzo Di Cataldo*, Vol. II, Torino, 2021, pp. 711 et seq.

PIERGALLINI C., *Danno da prodotto* e *responsabilità penale, Profili dommatici* e *politico criminali*, Milano, 2004.

PIERGALLINI C., *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato*, in *Riv. it. dir. proc. pen.*, n. 4, 2020, pp. 1743 et seq.

PIERGALLINI C., *La responsabilità del produttore: una nuova frontiera del diritto penale?*, in *Dir. pen. proc.*, n. 9, 2007, pp. 1125 et seq.

PISA P., *Il 'Nobel' dell'informativa lascia Google. "L'intelligenza artificiale è pericolosa"*, in *La Repubblica*, 3 maggio 2023, p. 14.

PISANESCHI A., *Le sanzioni amministrative della Consob* e *della Banca d'Italia: gli indirizzi delle giurisdizioni sovranazionali* e *le problematiche applicative interne*, in *Riv trim. dir. econ.*, n. 2, 2020, Suppl., pp. 81 et seq.

PITRUZZELLA G., *La libertà di informazione nell'era di Internet*, in *Rivista di diritto dei media* (*medialaws.eu*), n. 1, 2018, pp. 19 et seq.

POLLICINO O. – DE GREGORIO G. – PAOLUCCI F., *La proposta di Regolamento sull'intelligenza artificiale: verso una nuova governance europea*, in *Privacy & Data Protection Technology Cybersecurity*, n. 3, 2021.

POWER M., *What happens when a software bot goes on a darknet shopping spree?*, reperibile alla seguente url https://www.theguardian.com).

Proietti G., *Intelligenza artificiale: una prima analisi della proposta di regolamento europeo*, in *dirittobancario.it*, maggio 2021.

Proietti G., *La responsabilità nell'intelligenza artificiale* e *nella robotica*, Milano, 2020.

Proietti G., *Sistemi di Intelligenza Artificiale* e *Responsabilità: la proposta di AI Liability Directive*, in *dirittobancario.it*, 6 ottobre 2022.

Protess B., *White Makes Case for Bigger S.E.C. Budget*, in *N.Y. TIMES*, 7 maggio 2013.

Provenzano P., *Illecito amministrativo* e *retroattività "*in bonam partem*": da eccezione alla regola a regola generale*, in *Banca borsa tit. cred.*, n. 1, 2020, pp. 52 et seq.

Puorro A., High Frequency Trading*: una panoramica*, in *Questioni di economia* e *Finanza* (*Occasional Paper*), Banca d'Italia (bancaditalia.it), n. 198, settembre 2013.

Rabitti M., *Intelligenza artificiale* e *finanza. La responsabilità civile tra rischio* e *colpa*, in *Riv. trim. dir. econ.* (*fondazionecapriglione.luiss.it*), Suppl. n. 2 al n. 3/2021, p. 300.

Raffaele F., *Ritorno Futuro 3: l'"insider di se stesso" all'esame della Cassazione* e *il nuovo tentativo di ipostatizzare il* market egalitarianism, in *Giur. comm.*, n. 4, 2019, pp. 778 et seq.

Ratti M., *Riflessioni in materia di responsabilità civile e danno cagionato da dispositivo intelligente alla luce dell'attuale scenario normativo*, in *Contr. impr.*, n. 3, 2020, pp. 1174 et seq.

Resta G., *Cosa c'è di 'europeo' nella proposta di Regolamento UE sull'intelligenza artificiale*, in *Contr. impr.*, n. 2, 2002, pp. 323 et seq.

Riondato S., *Robotica* e *diritto penale (robot, ibridi, chimere, "animali tecnologici")*, in Provolo D.– Riondato S. –Yenisey F., *Genetics, robotics, law punishment*, Padova, 2014, pp. 599 et seq.

Robinson T.B., *A question of intent: Aiding and abetting law and the rule of accomplice liability under section 924 (c)*, in *Michigan Law Review*, Vol. 96, 1997, pp. 783 et seq.

Rodriguez-Sickert C., *Homo Economicus*, in Peil J. – Van Staveren I. (eds), *Handbook of Economics and Ethics*, The Hague, 2009, p. 223.

Roxin C., *Täterschaft und Tatherrschaft*, Hamburg, 1963.

Ruffolo U. – Al Mureden E., Autonomous vehicles *e responsabilità nel nostro sistema ed in quello statunitense*, in *Giur. it.*, n. 7, 2019, pp. 1704 et seq.

Ruffolo U., *Intelligenza artificiale, machine learning, responsabilità da algoritmo*, in *Giur. it.*, n. 1, 2019, pp. 1696-1697.

Ruffolo U., *L'intelligenza artificiale in sanità: dispositivi medici, responsabilità* e *"potenziamento"*, in *Giur. it.*, n. 2, 2021, pp. 502 et seq.

Ruffolo U., *La "personalità elettronica"*, in Ruffolo U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, pp. 213 et seq.

Russell S. – Norvig P., *Artificial Intelligence: A Modern Approach*, Hoboken, 2021.

Ruta G., *I.A. nei reati economici e finanziari*, in Aa.Vv., *Intelligenza artificiale e giurisdizione penale*, Atti del Workshop della Fondazione Vittorio Occorsio, Università Mercatorum, Roma, 19 novembre 2021, pp. 58 et seq.

Sabella M., Flash crash *in Borsa, l'algoritmo che affonda Piazza Affari per 5 minuti: cos'è successo*, in *Corriere della sera*, 2 maggio 2022.

Sadaf R. - McCullagh O. – Grey C. – King E. - Sheehan B. – Cunneen M., *Algorithmic Trading, High-frequency Trading: Implications for MiFID II and Market Abuse Regulation (MAR) in the EU*, 2021, in www.ssrn.com, pp. 1 et seq.

Salanitro U., *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, in *Riv. dir. civ.*, n. 6, 2020, pp. 1246 et seq.

Salvadori I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. proc. pen.*, n. 1, 2021, pp. 83 et seq.

Santangelo A., *Una soluzione "di favore" per l'*insider *di se stesso: la* rule of lenity *quale criterio di risoluzione di casi difficili*, in *Dir. pen. proc.*, n. 10, 2022, pp. 1343 et seq.

Sartori F., *La consulenza finanziaria automatizzata: problematiche e prospettive*, in *Riv. trim. dir. econ.* (*fondazionecapriglione.luiss.it*), n. 3, 2018, pp. 253 et seq.

Sassi S., *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, *Analisi giur. econ.*, n. 1, 2019, pp. 109 et seq.

Scheau M.C. – Arsene L. – Popescu G., *Artificial Intelligence/Machine Learning Challenges and Evolution*, in *Int' J. Info. Sec. Cybercrime*, Vol. 7, Issue 1, 2018, pp. 11 et seq.

Schepisi C., *Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione*, in *I Post di AISDUE* (*aisdue.eu*), IV, 2022, Sezione "Atti convegni AISDUE", n. 16, 28 marzo 2022 Quaderni AISDUE, pp. 330 et seq.

Schwalbe U., *Algorithms, Machine Learning, and Collusion*, June 2018, in www.ssrn.com, pp. 1 et seq.

Scodetta M., *Il* ne bis in idem *"preso sul serio": la Corte EDU sulla illegittimità del doppio binario francese in materia di abusi di mercato (e i possibili riflessi nell'ordinamento italiano)*, in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*), 17 giugno 2019.

Scoletta M., *Uno più uno anche a Roma può fare due: la illegittimità costituzionale del doppio binario sanzionatorio del doppio binario punitivo in materia di diritto d'autore*, in *Sistema penale* (*sistemapenale.it*), 23 giugno 2022.

SCOPINO G., *Do Automated Trading Systems Dream of Manipulating the Price of Futures Contracts? Policing Markets for Improper Trading Practices by Algorithmic Robots*, in *Florida L. Rev.*, Vol. 67, 2015, pp. 221 et seq.

SEYFERT R., *Algorithms as Regulatory Objects*, in *Information Communication and Society*, 2021, https://doi.org/10.1080/1369118X.2021.1874035, pp. 1 et seq.

SEMINARA S., *Disclose or Abstain? La nozione di informazione privilegiata tra obblighi di comunicazione al pubblico e divieti di* insider trading*. Riflessioni sulla determinatezza delle fattispecie sanzionatorie*, in *Banca borsa tit. cred.*, n. 3, 2008, p. 337.

SEMINARA S., *Il diritto penale del mercato mobiliare*, Torino, 2022.

SEMINARA S., *L'informazione privilegiata*, in CERA M. – PRESTI G. (a cura di), *Il testo unico finanziario*, Vol. II, Bologna, 2020, pp. 2124 et seq.

SERRAO D'AQUINO P., *La responsabilità civile per l'uso di sistemi di intelligenza nella Risoluzione del Parlamento europeo del 20 ottobre 2020: "Raccomandazione alla Commissione sul regime di responsabilità civile e intelligenza artificiale"*, in *DPER online*, n. 1, 2021, pp. 248 et seq.

SEVERINO P., *Intelligenza artificiale e diritto penale*, in RUFFOLO U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, pp. 531 et seq.

SFORZA I., Il nemo tenetur se detegere *nelle audizioni Consob e Banca d'Italia: uno statuto ancora da costruire*, in *Sistema penale* (*sistemapenale.it*), n. 2, 2022, pp. 83 et seq.

SIDERI M., *«L'intelligenza artificiale» sta diventando cosciente. In Google scoppia un caso*, in *Corriere della Sera*, 14 giugno 2022, p. 33.

SIMESTER A.P. – SPENCER J.R. – SULLIVAN G.R. – VIRGO G.J., *Simester and Sullivan's Criminal Law. Theory and Doctrine*, Oxford, 2013.

SIMMLER M. – FRISCHKNECHT R., *A taxonomy of human-machine collaboration: capturing automation and technical autonomy*, in *Ai & Society*, Vol. 36, 2021, pp. 239 et seq.

SLEMMER D.W., *Artificial Intelligence & Artificial Prices: Safeguarding Securities Markets from Manipulation by Non-Human Actors*, in *Brook. J. Corp. Fin. & Com. L.*, Vol. 14, Issue 1, 2019, pp. 149 et seq.

SOKOL N.E., *High Frequency Litigation: SEC Responses to High Frequency Trading as a Case Study in Misplaced Regulatory Priorities*, in *Science and Techn. L. Rev.*, Vol. 17, n. 2, 2016, pp. 402 et seq.

SOLUM L.B., *Legal Personood for Artificial Intelligences*, in *North Carolina L. Rev.*, Vol. 70, n. 4, 1994, pp. 1231 et seq.

SPERA P., voce *Intelligenza artificiale*, in ZACCARI G.– PERRI P. (a cura di), *Dizionario Legal Tech*, Milano, 2020, pp. 535 et seq.

Steinberg M.I., *The Sec and the Securities Industry Respond to September 11*, in *International Lawyer*, Vol. 36, n. 1, 2002, pp. 131 et seq.

Strampelli G., *L'informazione societaria a quindici anni dal T.U.F.: profili evolutivi e problemi*, in *Riv. soc.*, n. 5, 2014, pp. 991 et seq.

Taddeo M. – Floridi L., *How AI can be a force for good*, in *Science*, Vol. 361, Issue 6404, 2018, pp. 751-752.

Talamo V.C., *Sistemi di intelligenza artificiale: quali scenari in sede di accertamento della responsabilità penale?*, in *ilPenalista*, 3 luglio 2020.

Tetlock P.C. – Saar M. – Tsechansky M. –Mackassy S., *More Than Words: Quantifying Language to Measure Firms' Fundamentals, in The Journal of Finance*, Vol. 63, 2008, pp. 1437-1467.

Teubner G., *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi* (trad. it. a cura di P. Femia), Napoli, 2019.

Teubner G., *Digitale Rechtssubjekte?*, in *AcP*, Vol. 218, 2018, pp. 155 et seq.

Thomas W.R., *The Ability and Responsibility of Corporate Law to Improve Criminal Punishment*, in *Ohio St. L.J.*, Vol. 78, 2017, pp. 601 et seq.

Tiganò V., *L'estensione del principio costituzionale della retroattività favorevole in materia penale alle sanzioni amministrative punitive contro gli abusi di mercato*, in *Banca borsa tit. cred.*, n. 1, 2020, pp. 62 et seq.

Trezza R., *Intelligenza artificiale e persona umana: la multiforme natura degli algoritmi e la necessità di un "vaglio di meritevolezza" per i sistemi intelligenti*, in *Ratio Iuris* (*ratioiuris.it*), 19 maggio 2022.

Tripodi A.F., *Corte europea dei diritti dell'uomo e sistemi sanzionatori in materia di abusi di mercato e di violazioni tributarie: la quiete dopo la tempesta*, in *Soc.*, n. 1, 2018, pp. 80 et seq.

Tripodi A.F., *Informazioni privilegiate e statuto penale del mercato finanziario*, Padova, 2012.

Troncone P., *Il sistema dell'intelligenza artificiale nella trama grammaticale del diritto penale. Dalla responsabilità umana alla responsabilità delle macchine pensanti: un inatteso* return trip effect, in *Cass. pen.*, n. 9, 2022, pp. 3287 et seq.

Turner J., *Robot Rules*, Berlin, 2018.

Turner J., *Robot Rules: Regulating Artificial Intelligence*, Cham, 2019.

Ventoruzzo M., *Abusi di mercato sanzioni Consob e diritti umani: il caso Grande Stevens e altri c. Italia*, in *Riv. soc.*, n. 4, 2014, pp. 693 et seq.

Ventoruzzo M., *Comparing insider trading in the United States and in the European Union: History and recent developments*, in *European Company and Financial Law Review*, Vol. 11, n. 4, 2015, pp 554-593

VENTORUZZO M., *Qualche nota su cosiddetto "insider di sé stesso" alla luce del Regolamento UE sugli abusi di mercato*, in *Soc.*, n. 6, 2018, pp. 745 et seq.

VERSTEIN A., *Benchmark Manipulation*, *B.C. L. Rev.*, Vol. 56, 2015, pp. 272 et seq.

VIGANÒ F., *Doppio binario sanzionatorio* e ne bis in idem*: verso una diretta applicazione dell'art. 50 della Carta?*, in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*), n. 3, 2014, pp. 219 et seq.

VIGANÒ F., *La Grande Camera della Corte di Strasburgo su* ne bis in idem *e doppio binario sanzionatorio*, in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*), 18 novembre 2016.

YADAV Y., *Insider Trading and Market Structure*, in *UCLA L. Rev.*, Vol. 63, 2016, pp. 978 et seq.

YADAV Y., *The Failure of Liability in Modern Markets*, in *Virginia L. Rev. Ass.*, Vol. 102, 2016, pp. 1031 et seq.

YADAV A. – VISHWAKARMA D.K., *Sentiment analysis using deep learning architectures: a review. Artificial Intelligence Review*, Vol. 53, n. 6, 2020, pp. 4335-4385.

YAFFE G., *The Voluntary Act Requirement*, in MARMOR A. (ed.), *The Routledge Companion to the Philosophy of Law*, New York, 2012.