Quaderni giuridici

AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?

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

29

maggio 2023

CONSOB
COMMISSIONE NAZIONALE
PER LE SOCIETÀ E LA BORSA

L'attività di ricerca e analisi della Consob intende promuovere la riflessione e stimolare il dibattito su temi relativi all'economia e alla regolamentazione del sistema finanziario.

I **Quaderni di finanza** accolgono lavori di ricerca volti a contribuire al dibattito accademico su questioni di economia e finanza. Le opinioni espresse nei lavori sono attribuibili esclusivamente agli autori e non rappresentano posizioni ufficiali della Consob, né impegnano in alcun modo la responsabilità dell'Istituto. Nel citare i lavori della collana, non è pertanto corretto attribuire le argomentazioni ivi espresse alla Consob o ai suoi Vertici.

I **Discussion papers** ospitano analisi di carattere generale sulle dinamiche del sistema finanziario rilevanti per l'attività istituzionale.

I **Quaderni giuridici** accolgono lavori di ricerca volti a contribuire al dibattito accademico su questioni di diritto. Le opinioni espresse nei lavori sono attribuibili esclusivamente agli autori e non rappresentano posizioni ufficiali della Consob, né impegnano in alcun modo la responsabilità dell'Istituto. Nel citare i lavori della collana, non è pertanto corretto attribuire le argomentazioni ivi espresse alla Consob o ai suoi Vertici.

I **Position papers**, curati dalla Consob anche in collaborazione con altre istituzioni, illustrano ipotesi di modifiche del quadro regolamentare o degli approcci di vigilanza e ricognizioni di aspetti applicativi della normativa vigente.

Consob

00198 Roma – Via G.B. Martini, 3

t 06.8477.1

f 06.8477612

e studi_analisi@consob.it

ISSN 2281-5236 (online)
ISSN 2281-5228 (stampa)

AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?

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

Abstract

Il testo affronta la distinzione tra sistemi di AI deboli e forti nel contesto del mercato finanziario. I sistemi di AI deboli dipendono dalle istruzioni prestabilite di produttori, programmatori o utenti, mentre i sistemi di AI forti sono dotati di capacità di auto-apprendimento e producono *output* autonomi e imprevedibili rispetto agli *input* iniziali. La diffusione di queste tecnologie nel mercato finanziario pone interrogativi sulla tenuta del quadro normativo e sull'imputazione degli illeciti finanziari compiuti con l'aiuto di questi sistemi, in particolare per i sistemi di AI forti, che richiedono criteri di imputazione della responsabilità innovativi. Inoltre, i sistemi di AI forti sembrano incrinare l'applicazione del principio di neutralità tecnologica nella regolamentazione del settore finanziario. Il testo propone tre possibili soluzioni per reprimere le condotte dannose dei sistemi di AI autonomi, ma ciascuna presenta criticità specifiche a seconda dei settori dell'ordinamento coinvolti**.

Keywords: sistemi di AI, AI deboli, AI forti, *insider trading*, manipolazione del mercato.

(*) 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.

Si ringraziano Francesca Medda e Filippo Annunziata per i commenti ricevuti. Le opinioni espresse nel presente Quaderno sono attribuibili esclusivamente agli autori e non rappresentano posizioni ufficiali della Consob, né impegnano in alcun modo la responsabilità dell'Istituto. Nel citare i contenuti del presente Quaderno, non è pertanto corretto attribuirli alla Consob o ai suoi Vertici. Errori e imprecisioni sono imputabili esclusivamente agli autori.

(**) Testo redatto da un noto sistema *online* di *chatbot*, basato su un avanzato sistema di intelligenza artificiale, in risposta alla richiesta degli autori (formulata alle ore 13:23 del 12 maggio 2023) di produrre un *abstract* del paragrafo "Conclusioni" del presente Quaderno.

Indice

CAPITOLO TERZO
Profili penalistici

Introduzione

L'innovazione tecnologica ha visto in tempi recenti la diffusione di algoritmi sempre più evoluti, capaci di sviluppare forme di autoapprendimento (*self-learning*) e di reciproca interazione con tratti di "esperienza" e di "socialità" che evocano inevitabili parallelismi con l'agire degli esseri umani. Al tempo stesso, cresce la consapevolezza della novità dei problemi sollevati dall'utilizzo dell'intelligenza artificiale.

Si tratta, anzitutto, di problemi *definitori*. I sistemi di intelligenza artificiale (di seguito verranno usate, indifferentemente, le espressioni AI, sistema di intelligenza artificiale, agente artificiale, intelligenza artificiale) si sottraggono, infatti, a formulazioni linguistiche univoche in ragione della varietà delle configurazioni assunte. Sotto questo profilo, pertanto, l'espressione «intelligenza artificiale» rappresenta al più un concetto "riassuntivo", la cui utilità risiede nell'aggregare sul piano lessicale programmi che utilizzano differenti *metodi* ma che appaiono tutti accomunati dal medesimo *elemento funzionale*: la capacità di elaborare quantità enormi di dati in tempi estremamente ravvicinati, minimizzando i tempi di latenza e contribuendo così alla soluzione efficiente di problemi che normalmente richiederebbero il concorso di diversi attori umani muniti di competenze eterogenee [cfr. R. KONERTZ - R. SCHÖNHOF, *Das technische Phäneomen "Künstliche Intelligenz" im allgemeinen Zivilrecht*, Baden-Baden, 2020, pp. 30 ss. e 135 (ove la qualificazione dell'AI come "*Oberbegriff*")].

Si tratta però anche di affrontare complessi problemi *tecnici* perché qualsiasi inquadramento concettuale di nuovi sviluppi della tecnologia, e a maggior ragione di quella algoritmica, impone di considerarne le specifiche, e per molti versi uniche, caratteristiche, al fine di minimizzare il divario tra l'ambito teorico di una possibile regolamentazione e l'effettività concreta della sua applicazione. Sotto questo profilo, il legislatore si trova sempre ad affrontare un dilemma di ordine «cronologico» perché, nell'inseguire le ragioni del mercato, rischia di intervenire o troppo "presto", paralizzando l'innovazione senza averne compreso le potenzialità, o troppo "tardi", lasciando carta bianca agli "innovatori" senza averne compreso la pericolosità [A. KERKEMEYER, *Herausforderungen des Blockchain-Netzwerks für das Kapitalmarktrecht*, in *ZGR*, 2020, p. 673].

Ma più di tutto sono i problemi *giuridici* ad attrarre l'attenzione degli operatori (e quindi anche a legittimare uno studio quale quello versato nel Quaderno qui prefato). L'affermazione dei sistemi di AI impone, infatti, una rinnovata comprensione di categorie del diritto che si pensavano ormai consolidate.

Ciò è vero, in primo luogo, per la delicata questione se sia necessario (o anche solo opportuno) ascrivere ai sistemi di AI una separata soggettività giuridica e, in caso

di risposta affermativa, se tale esito sia raggiungibile già in forza della disciplina esistente o non vi sia bisogno, piuttosto, di introdurre una nuova figura di personalità ("elettronica"?): ponendosi allora, in questo secondo caso, il tema di verificare se la personalità del sistema di AI vada concepita come "piena" (ossia equipollente a quella delle persone fisiche o giuridiche) oppure limitata ai singoli aspetti di volta in volta considerati rilevanti dall'ordinamento, senza bisogno di attribuire alla macchina la titolarità completa di diritti e obblighi [G. TEUBNER, *Digitale Rechtssubjekte?*, in *AcP* 218 (2018), pp. 155 ss.]. Si tratta, con ogni evidenza, di un problema nient'affatto marginale: si pensi alla possibilità di intestare al sistema algoritmico una autonoma capacità negoziale ai fini del perfezionamento di contratti secondo la disciplina della rappresentanza volontaria. Si pensi, soprattutto, alla possibilità di imputare all'algoritmo all'uopo personificato l'"intenzione" di porre in essere comportamenti dannosi e quindi di fungere da centro di imputazione di fattispecie (antiche o nuove) di responsabilità civile, amministrativa o penale.

Quest'ultimo è evidentemente un profilo di arduo inquadramento. Allo stato attuale delle conoscenze e anche in ragione delle delicate implicazioni di ordine etico che ne discenderebbero, appare a tutt'oggi difficile discorrere di un «libero arbitrio» o di una «volontà» dell'algoritmo; e altrettanto difficile appare sul piano del fatto sia *delimitarne* in concreto una eventuale "personalità", in ragione della circostanza che un algoritmo solitamente è costituito da catene o grappoli di altri algoritmi tra loro interconnessi [R. SEYFERT, *Algorithms as Regulatory Objects*, in *Information Communication and Society*, 2021, https://doi.org/10.1080/1369118X.2021.1874035, p. 6], sia dimostrare l'esistenza di un *nesso di causalità* tra il comportamento tenuto dall'algoritmo e il danno che ne sarebbe asseritamente derivato [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 s.]. Al fine di evitare un "vuoto" di tutela il legislatore potrebbe certamente far transitare quella responsabilità in capo alla figura umana più "vicina" al funzionamento della macchina: si tratti poi del produttore, del programmatore o dell'utilizzatore (secondo un approccio "umano-centrico" o "*human-in-the-loop-approach*": v. ancora A. AZZUTTI-W.G. RINGE-H. SIEGFRIED STIEHL, *Machine Learning*, cit., p. 128). Una soluzione, tuttavia, a sua volta non priva di inconvenienti, almeno in tutte le ipotesi in cui il sistema di AI abbia raggiunto un tale grado di autonomia da rendere imprevedibili i propri comportamenti [esponendo conseguentemente l'essere umano allo scenario di una responsabilità "quasi-oggettiva": v. T. BAUERMEISTER - T. GROBE, *Personen im Recht – über Rechtssubjekte und ihre Rechtsfähigkeit*, in *ZGR*, 2022, specie pp. 766 s.]. Il problema risiede, in particolare, nella "mancanza di interpretabilità" dei modelli algoritmici, i quali non vengono programmati per «spiegare le correlazioni che hanno scoperto» e che normalmente sfuggono alla capacità cognitiva degli esseri umani [R. SEYFERT, *Algorithms as Regulatory Objects*, cit., p. 14].

Vi sono poi gli *specifici* problemi giuridici sollevati dalla diffusione dell'intelligenza artificiale e che si prestano ad esser declinati (e risolti) in modo differente in ragione del singolo settore dell'ordinamento di volta in volta considerato.

Così, gli Studiosi di diritto societario si interrogano sul ruolo che gli algoritmi possono svolgere nel consentire agli amministratori di imprese organizzate in forma azionaria di formulare un processo decisionale consapevole e informato ai fini dell'operatività della *business judgment rule*. E pur escludendosi la possibilità di nominare un intero *Roboboard* o che i sistemi di AI si rendano destinatari di deleghe esecutive ai sensi dell'art. 2381 c.c., non si manca di sottolineare la notevole incidenza che il ricorso a quei sistemi può avere sia sulla conformazione degli obblighi degli amministratori (principalmente nella prospettiva del dovere di agire in modo informato, di curare e valutare l'adeguatezza degli assetti organizzativi, di motivare le decisioni di gestione), sia, e conseguentemente, sui termini di una loro responsabilità ai sensi dell'art. 2392 c.c. (cfr. G.D. MOSCO, *L'intelligenza artificiale nei consigli di amministrazione*, in *AGE*, n. 1, 2019, pp. 247 ss.; 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 ss.). Altrettanto percepito è però anche il rischio che l'utilizzo della tecnologia acuisca i conflitti di agenzia immanenti al governo societario in quanto i sistemi di intelligenza artificiale possono rendere più agevole per i manager che ne hanno il controllo diretto o indiretto attuare comportamenti opportunistici senza timore di essere adeguatamente vigilati (cfr. L. ENRIQUES - D.A. ZETZSCHE, *Corporate Technologies and the Tech Nirvana Fallacy*, *ECGI Law Working Paper*, March 2020).

Crescente attenzione viene inoltre riservata alle conseguenze dell'impiego di algoritmi "intelligenti" per il diritto antitrust. In questo caso è la presenza di programmi che coordinano i propri comportamenti in materia di fissazione dei prezzi (o l'utilizzo della medesima piattaforma algoritmica da parte di più imprese) a evocare il tema della collusione e quindi dell'intesa restrittiva della concorrenza [J. LÜBKE, *Preisabstimmung durch Algorithmen*, in *ZHR* 185 (2021), pp. 723 ss.]. Si tratta di uno scenario che non si può escludere, anche se esso sembra presupporre sistemi di AI particolarmente evoluti in quanto in grado di elaborare modalità sofisticate di interazione reciproca e di applicare conseguentemente prezzi alterati che massimizzino il profitto congiunto delle imprese utilizzatrici [U. SCHWALBE, *Algorithms, Machine Learning, and Collusion*, June 2018, in www.ssrn.com, p. 24].

Ma è con riguardo al funzionamento del mercato dei capitali che il diffuso impiego di nuove "entità" tecniche munite di intelligenza artificiale comporta le sfide più delicate. Qui si tratta, infatti, di articolare una disciplina che protegga l'integrità dei mercati e tuteli gli investitori senza ostacolare indebitamente lo sviluppo della finanza digitale. L'innovazione tecnologica può incrementare l'efficienza del mercato, aumentandone la liquidità e riducendo al tempo stesso i costi transattivi e i tempi di esecuzione degli ordini di acquisto e vendita. Ma l'innovazione può anche agevolare la consumazione di figure manipolative del mercato tali da minare gravemente la fiducia del pubblico, da disincentivare la partecipazione degli investitori più evoluti e da alterare irreparabilmente l'ordinato funzionamento del meccanismo di *price discovery*.

Il compito di chi intenda avvicinarsi a tali problemi non è certamente agevole.

Basti pensare, ad esempio, al rischio, da un lato, di una applicazione indiscriminata della disciplina degli abusi di mercato – ove si arresti l'analisi al piano dell'elemento *oggettivo* dell'illecito, attesa la capacità dei sistemi di AI di incidere in modo

significativo sul livello dei prezzi e allora anche di fissarli a un livello anomalo (come dimostrato dal dibattito antitrust appena ricordato) – e, dall'altro, di una generalizzata impunità per difetto dell'elemento *soggettivo* (in termini di dolo o comunque di consapevolezza della potenzialità dannosa della condotta), attesa la già menzionata difficoltà di "soggettivizzare" l'intelligenza artificiale e quindi anche di applicarle i consueti parametri di imputazione della responsabilità.

Si pensi, altresì, all'eventualità che le nuove tecnologie mettano in crisi paradigmi consolidati della regolamentazione europea degli abusi di mercato: primo fra tutti, quello dell'investitore "ragionevole" evocato dall'art. 7 *MAR* il quale dovrebbe assumere le proprie decisioni sulla base di notizie oggettive, attendibili e soprattutto idonee a segnalare un valore intrinseco («reale») del titolo diverso dal prezzo di mercato ma che, ove assuma la veste di *trader* algoritmico, si trova a effettuare scelte di acquisto o vendita che poco hanno a che fare con il *valore intrinseco* degli strumenti finanziari negoziati, con conseguente emersione di informazioni "privilegiate" (perché idonee a influire in modo sensibile sui prezzi degli strumenti finanziari), ma non *ragionevoli* (perché prive di correlazione con il valore fondamentale del titolo e con l'andamento del mercato) [v. 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 ss.; con riferimento alle cripto-attività, M. MAUGERI, *Cripto-attività e abusi di mercato*, in *Oss. dir. civ. e comm.*, Speciale/2022, pp. 413 ss., specie § 5].

Il Quaderno si propone, appunto, lo scopo di verificare se le fattispecie tradizionali in materia di abusi di mercato scolpite da MAR siano tuttora idonee a governare la complessità della negoziazione algoritmica o richiedano piuttosto di essere adattate all'unicità dell'agente AI, se non addirittura di essere integralmente ripensate nei loro archetipi concettuali fondativi. Al riguardo, diverse sono le alternative di *policy* astrattamente ipotizzabili. Una prima opzione attiene alla conformazione stessa della regolamentazione e alla possibilità di transitare da un approccio "casistico", come quello attuale, basato sulla tipizzazione delle modalità di abuso ("*rules-based approach*") a una impostazione articolata per principî generali ("*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, in www.ssrn.com, p. 4]. La scelta di predisporre in via normativa una lista predeterminata di condotte manipolative comporta infatti, inevitabilmente, l'esigenza di un costante aggiornamento alle condizioni indotte dall'operatività dei sistemi di AI: una "corsa" nella quale, tuttavia, la legge non riuscirebbe mai a raggiungere l'algoritmo, data la capacità di apprendimento di quest'ultimo (in una sorta di riedizione tecnologica del paradosso di Zenone). Ciò tanto più se si considera che l'essenza dei sistemi autonomi o "forti" di AI risiede nella *capacità* di individuare strategie di negoziazione ulteriori rispetto a quelle ragionevolmente attuabili da un operatore umano, con conseguente *incapacità* di quest'ultimo di seguire pienamente il processo decisionale dell'algoritmo [v., segnalando questo aspetto come "*black-box problem*", A. AZZUTTI - W.G. RINGE - H. SIEGFRIED STIEHL, *Machine Learning*, cit., pp. 118 s.].

Vi è poi il problema, già segnalato, della imputabilità della responsabilità conseguente al comportamento manipolativo dell'intelligenza artificiale. Qui l'alternativa

si muove tra una disciplina che guardi unicamente agli effetti *oggettivi* della negoziazione algoritmica ("*outcome-based approach*") contemplando una serie di esenzioni o di cause di giustificazione (ad es., adeguando alla realtà dei sistemi di AI il riferimento ai "legittimi motivi" contenuto nell'art. 12 di *MAR*); e una disciplina che ricolleghi la responsabilità del *soggetto* umano alla violazione di predefiniti obblighi. Aderendo a questa seconda linea di ragionamento si potrebbe immaginare l'obbligo del *designer* algoritmico di innestare nel programma regole di protezione ("*Schutznormen*") che vigilino sulla condotta del sistema e siano idonee, a una valutazione di ragionevolezza *ex ante*, a neutralizzarne "decisioni" contrarie agli interessi protetti dall'ordinamento; si potrebbe immaginare, inoltre, di statuire l'obbligo dell'impresa utilizzatrice di consentire all'Autorità di Vigilanza l'"accesso" all'algoritmo e di spiegarne le modalità di funzionamento (cfr., con riguardo al problema dei comportamenti algoritmici collusivi, v. J. LÜBKE, *Preisabstimmung*, cit., p. 731), se non addirittura l'obbligo dei partecipanti al mercato di servirsi di algoritmi il cui comportamento corrisponda alle aspettative di una "corretta" negoziazione di mercato (in questo senso e ragionando di un "*behaviouralist approach*", R. SADAF – O. MCCULLAGH – C. GREY – E. KING - B. SHEEHAN – M. CUNNEEN, *Algorithmic Trading,* cit., p. 18); e si potrebbe infine immaginare anche il passaggio da un sistema che reprime sul piano penale la condotta di esseri umani che creano algoritmi con l'intento di consumare un abuso di mercato a un sistema che sanzioni in futuro sul piano solo amministrativo la violazione del dovere di progettare/utilizzare algoritmi che *prevengano* l'abuso.

Quest'ultima soluzione influenzerebbe, certo, una rimeditazione dell'assetto domestico attuale imperniato sul "doppio binario" sanzionatorio (amministrativo e penale); un assetto il quale, tuttavia, da tempo assicura l'effettività della disciplina grazie alla efficace applicazione delle sanzioni amministrative, ma che, con il larghissimo, pressoché identico, perimetro associato alle fattispecie sanzionate penalmente, espone al rischio di produrre sovrapposizioni difficili da trattare tanto sul piano sistematico della costruzione dell'illecito manipolativo, quanto su quello pratico della sua repressione.

I Sistemi di AI e abusi di mercato

1 Lo sviluppo dell'AI e il quadro normativo in materia di abusi di mercato

La riflessione giuridica s'interroga di frequente sull'impatto delle trasformazioni tecnologiche e sociali nel quadro normativo[1], giungendo talvolta a conclusioni non univoche in merito alla tenuta di tale quadro e alla sua elasticità nel disciplinare fenomeni radicalmente nuovi quali – ad esempio – l'attitudine all'illecito di agenti non umani[2].

1 Risale al 1998 il magistrale confronto tra Natalino Irti e Giorgio Oppo sulla vitalità delle disposizioni del Codice civile in ambito contrattuale. Il primo (N. Irti, *Scambi senza accordo*, in *Riv. trim. dir. proc. civ.*, n. 2, 1998, pp. 347 ss.) ha sostenuto che l'impoverimento della lingua nel contratto e nelle contrattazioni a seguito dell'applicazione della tecnologia nella stipulazione di negozi giuridici, con il passaggio dall'*homo loquens* all'*homo videns*. Al contrario, il secondo (G. Oppo, *Disumanizzazione del contratto*, in *Riv. dir. civ.*, 1998, pp. 525 ss.) ha escluso nelle innovative manifestazioni del consenso e di conclusione del contratto, veicolate dalla tecnologia, la sussistenza di «scambi senza accordo»: seppure tradizionalmente il contratto e le relative negoziazioni siano state plasmate, nell'immaginario degli ideatori della disciplina civilistica, mediante lo scambio verbale di una proposta e di un'accettazione, «l'accordo non presuppone una o altra lingua ma solo l'espressione di voleri concordanti»; in altri termini, secondo quest'ultimo autore anche nelle moderne modalità di contrattazione è ravvisabile l'accordo poiché né la trattativa né il dialogo né l'espressione linguistica sono richieste dalla disciplina codicistica perché vi sia il contratto. Le più recente digitalizzazione delle negoziazioni ha portato a rivedere però alcune di queste ultime conclusioni. Si rinvia a G. Finocchiaro, *La conclusione del contratto telematico mediante i software agents: un falso problema giuridico?*, in *Contr. impr.*, n. 2, 2002, pp. 500 ss., in particolare p. 505, la quale, riportando l'ipotesi di un individuo che si rivolge ad un *software* con l'indicazione di comprare un determinato libro al prezzo più basso offerto sul mercato e comunque ad un prezzo non superiore all'importo di euro 15,00, affermava la riconducibilità della stipulazione all'individuo per la predeterminazione degli elementi del contratto. Recentemente la medesima A., *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ.*, n. 2, 2018, pp. 441 ss., giunge a conclusioni opposte per via dell'evoluzione della tecnologia che ha diffuso algoritmi in grado di apprendere in modo autonomo e di prendere decisioni senza che le relazioni causa-effetto siano necessariamente comprese dall'uomo. Sulla capacità delle disposizioni civilistiche in materia di responsabilità di adeguarsi, con innovazioni normative minime, nell'esperienza dell'Europa continentale, alle trasformazioni della società e alle tecnologie produttive si rinvia a U. Ruffolo, *Intelligenza artificiale, machine learning, responsabilità da algoritmo*, in *Giur. it.*, n. 1, 2019, pp. 1696-1697. Come si vedrà nel prosieguo, la questione dell'impatto dell'intelligenza artificiale costituisce oggetto di un dibattito recente anche nella dottrina penalistica che valuta la validità dell'applicazione dei tradizionali modelli di attribuzione della responsabilità penale in relazione ad eventi lesivi che derivano dall'agire di un sistema di AI ovvero dall'interazione uomo e AI. Oltre ai contributi infra citati, si rinvia *ex multis* a C. Piergallini, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato*, in *Riv. it. dir. proc. pen.*, n. 4, 2020, pp. 1743 ss.; I. Salvadori, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. proc. pen.*, n. 1, 2021, pp. 83 ss.; 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 ss.; M.B. Magro, *Biorobotica, robotica e diritto penale*, in D. Provolo – S. Riondato – F. Yenisey, *Genetics, robotics, law punishment*, Padova, 2014, pp. 499 ss. Più in generale, con riferimento alle implicazioni derivanti dalle innovazioni tecnologiche sulla ricostruzione della responsabilità penale, si segnala il contributo più risalente di 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 ss.

2 Sulle applicazioni di intelligenza artificiale in generale si rinvia a F. Basile, *Diritto penale e intelligenza artificiale*, in *Giur. it.*, Suppl. 2019, pp. 67 ss. Con particolare riguardo all'utilizzazione dell'intelligenza artificiale nell'attività di giustizia (e polizia) predittiva si rinvia a M. Luciani, *La decisione giudiziaria robotica*, in *Riv. AIC* (*rivistaaic.it*), n. 3, 2018,

La multiforme prassi delle imprese che adottano ormai capillarmente e su larga scala sistemi di intelligenza artificiale (cc.dd. sistemi di AI) fornisce al giurista ulteriore materia di riflessione, sia nell'ermeneutica del diritto vigente sia nell'elaborazione di regole nuove in grado di contemperare l'esigenza di prevenire tali illeciti con l'intento di non arrestare lo sviluppo tecnologico[3]. È vero, infatti, che alcune decisioni – incluse quelle idonee a causare eventi pregiudizievoli – possono ormai essere assunte sia dall'uomo sia dai sistemi di AI[4]. Ciò spiega l'interesse per una disciplina *ad hoc* dell'intelligenza artificiale da parte delle istituzioni nazionali[5] e delle istituzioni UE[6],

872 ss.; F. DONATI, *Intelligenza artificiale e giustizia*, in *Riv. AIC* (*rivistaaic.it*), n. 1, 2020, pp. 415 ss.; G. CANZIO, *Intelligenza artificiale e processo penale*, in *Cass. pen.*, n. 3, 2021, pp. 797 ss.; S. ARDUINI, *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 ss.; L. ALGERI, *Intelligenza artificiale e polizia predittiva*, in *Dir. pen. proc.*, n. 6, 2021, pp. 724 ss.; 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 ss. e, con riferimento anche alla decisione amministrativa automatizzata, *ex multis* 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 ss., e S. SASSI, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità, Analisi giur. econ.*, n. 1, 2019, pp. 109 ss.

3 *Amazon*, *Google*, *Facebook*, *Ibm*, *Microsoft* e *DeepMind* hanno elaborato nel 2016 sette regole per contenere l'evoluzione tecnologica e riparare i danni cagionati dall'intelligenza artificiale: «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». Si veda P. BOTTAZZINI, *Intelligenza artificiale. I sei big dettano le regole*, in *Pagina 99*, 8 ottobre 2016, pp. 20-21. Successivamente, a gennaio 2017, Elon Musk, Stephen Hawking e altri 2335 ricercatori ed esperti, sotto l'egida del neocostituito Istituto *Future of Life*, hanno approvato un manifesto di 23 principi, i cc.dd. "Principi di Asilomar", suddivisi in tre aree: Ricerca; Etica e valori; Problemi di scenario. Questi tentativi di normare l'intelligenza artificiale risale ad Asimov che ha elaborato le tre leggi della robotica, in *Circolo vizioso* del 1942, aventi il seguente tenore letterale: «1. Un robot non può recar danno a un essere umano né può permettere che, a causa del suo mancato intervento, un essere umano riceva danno. 2. Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non vadano in contrasto alla Prima Legge. 3. Un robot deve proteggere la propria esistenza, purché la salvaguardia di essa non contrasti con la Prima o con la Seconda Legge». Queste leggi sono state ritenute superate per la sopravvenienza di nuovi principi etici e morali da parte di S. CRISCI, *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm.*, n. 10, 2018, p. 1793. Sull'esigenza di individuazione di un punto di equilibrio nel bilanciamento dei diritti fondamentali con l'utilizzazione dell'intelligenza artificiale si veda 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 ss., spec. pp. 1936-1937.

4 Sulla difficoltà dei sistemi di AI di garantire il medesimo standard qualitativo di ragionamento della mente umana si veda E. BATTELLI, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e tutela della persona*, in *Dir. fam. pers.*, n. 3, 2022, p. 1099. Si veda tuttavia il caso del sistema di AI di conversazione Lamda (acronimo di *Language Model for Dialogue Applications*) che l'ingegnere di *Google* Black Lemoine ha dichiarato senziente, anche in contrasto con i vertici della piattaforma digitale di comunicazione e per questo sospeso dal suo lavoro. Si rinvia a M. SIDERI, *«L'intelligenza artificiale» sta diventando cosciente. In Google scoppia un caso*, in *Corriere della Sera*, 14 giugno 2022, p. 33.

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

6 L'utilizzazione dell'intelligenza artificiale porta, infatti, con sé numerosi vantaggi. Alcuni di questi sono indicati nel Libro bianco sull'intelligenza artificiale: per i cittadini una migliore assistenza sanitaria, un minor numero di guasti degli elettrodomestici, sistemi di trasporto più sicuri e più puliti e servizi pubblici migliori; per le imprese sarà possibile avvalersi di nuove generazioni di prodotti e servizi nei settori in cui l'Europa è particolarmente forte (macchinari, trasporti, cibersicurezza, agricoltura, economia verde e circolare, assistenza sanitaria e settori ad alto valore aggiunto come la moda e il turismo); per i servizi di interesse pubblico la riduzione dei costi di fornitura di servizi (trasporti, istruzione, energia e gestione dei rifiuti), migliorando la sostenibilità dei prodotti e dotando le forze dell'ordine di strumenti appropriati per garantire la sicurezza dei cittadini, con adeguate garanzie quanto al rispetto dei loro diritti e delle loro libertà.

che nei loro documenti ufficiali includono riferimenti fino a qualche tempo fa relegati alla letteratura di fantascienza, quali le leggi della robotica di Asimov[7].

Ad una concezione che non pone limiti al progresso e a forme d'ibridazione tra la macchina e la persona umana, se ne contrappone un'altra che auspica limitazioni e regole dettagliate facendo leva sul principio di precauzione[8].

Tra questi due orientamenti si pone l'approccio della Commissione europea, che nella proposta di Regolamento (UE) sull'intelligenza artificiale (legge sull'intelligenza artificiale) del 21 aprile 2021, COM(2021) 206 *final*, si prefigge di non inibire lo sviluppo delle applicazioni di intelligenza artificiale, pur distinguendo i sistemi di AI a seconda del rischio di compromissione per i diritti fondamentali dell'uomo (c.d. *risk-based approach*) e combinando diverse tecniche di protezione del rischio: il principio di precauzione per i sistemi di AI a rischio inaccettabile e il principio di prevenzione per i sistemi di AI a rischio alto[9].

A questa proposta di regolamentazione si affianca, più recentemente, la proposta di Direttiva (UE) relativa all'adeguamento all'intelligenza artificiale delle norme in materia di responsabilità extracontrattuale (direttiva sulla responsabilità da intelligenza artificiale) del 28 settembre 2022, COM(2022) 496 *final*. Queste regole di armonizzazione delineano una concezione antropocentrica dell'intelligenza artificiale nel tentativo di collegare gli effetti prodotti sulla realtà esterna dai sistemi di AI all'uomo e, in particolare, a fornitori e utenti[10].

7 Si fa riferimento al Considerando T della Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL), ove si precisa «che le leggi di Asimov devono essere considerate come rivolte ai progettisti, ai fabbricanti e agli utilizzatori di robot, compresi i robot con capacità di autonomia e di autoapprendimento integrate, dal momento che tali leggi non possono essere convertite in codice macchina».

8 T.E. Frosini, *L'orizzonte giuridico dell'intelligenza artificiale*, in *Dir. inf.*, n. 1, 2022, p. 12. Sull'applicazione allo sviluppo generato dall'intelligenza artificiale del principio di precauzione, giustificato originalmente per la protezione dell'ambiente e della salute, si rinvia a G. Proietti, *La responsabilità nell'intelligenza artificiale e nella robotica*, Milano, 2020, pp. 39 ss.

9 Sulla proposta di Regolamento (UE) sull'intelligenza artificiale (legge sull'intelligenza artificiale) del 21 aprile 2021, COM(2021) 206 *final*, si rinvia ai commenti di G. Finocchiaro, *La proposta di Regolamento sull'intelligenza artificiale: il modello basato sulla gestione del rischio*, in *Dir. inf.*, n. 2, 2022, pp. 303 ss.; G. Resta, *Cosa c'è di 'europeo' nella proposta di Regolamento UE sull'intelligenza artificiale*, in *ivi*, pp. 323 ss.; 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 ss.; F. Donati, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, in *Dir. Un. eur.*, nn. 3-4, 2021, pp. 453 ss.; G. Alpa, *Quale modello normativo europeo per l'intelligenza artificiale*, in *Contr. impr.*, n. 4, 2021, pp. 1003 ss.; G. Contaldi, *Intelligenza artificiale e dati personali*, in *Ord. int. dir. um.*, n. 5, 2021, pp. 1193 ss.; 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 ss.; G. Proietti, *Intelligenza artificiale: una prima analisi della proposta di regolamento europeo*, in *dirittobancario.it*, maggio 2021. Al testo iniziale ha fatto seguito l'orientamento generale del Consiglio dell'Unione europea sulla proposta del 6 dicembre 2022, costituente tuttora la base dei preparativi per i negoziati con il Parlamento europeo.

10 Si intende fare riferimento alla Proposta di Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale) del 28 settembre 2022, COM(2022) 496 *final*. In questa proposta è elaborato un principio generale in forza del quale la responsabilità per i danni cagionati dai sistemi di AI dovrebbe ricadere sull'uomo, non soltanto nelle ipotesi in cui non siano state date abbastanza informazioni agli utenti sul funzionamento del sistema di AI o in presenza di un difetto del sistema di AI, ma altresì qualora l'algoritmo sia così complesso da non consentire al programmatore di comprendere i motivi delle sue decisioni. In questo senso A. Longo, *Il robot che rompe paga. Stretta europea sui produttori*, in *la Repubblica*, 2 ottobre 2022, p. 28, e G. Ghidini, *Ma chi paga i danni. Se il robot combina guai?*, in *Corriere della Sera*, 13

Anche la Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)) e la Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI)) riconoscono la necessità di un quadro normativo orientato ad affermare sempre la responsabilità umana[11].

Con particolare riguardo al mercato finanziario, l'applicazione dei sistemi di AI ha trasformato la prestazione di alcuni servizi[12], quali la negoziazione algoritmica ad alta frequenza (c.d. *high frequency trading*), la consulenza finanziaria automatizzata (c.d. *robo-advice*) e la valutazione del merito creditizio (c.d. *credit scoring*)[13].

febbraio 2023, p. 6. In particolare, la proposta elabora una presunzione relativa di nesso di causalità tra la colpa del convenuto e l'*output* prodotto dal sistema di AI o la mancata produzione di *output* da parte di tale sistema anche qualora l'attore abbia unicamente dimostrato che il danno proviene dal sistema di AI. In dottrina si veda il commento di G. Proietti, *Sistemi di Intelligenza Artificiale e Responsabilità: la proposta di AI Liability Directive*, in *dirittobancario.it*, 6 ottobre 2022. In precedenza, vi sono state una serie di proposte: la Risoluzione del Parlamento UE del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica ha proposto l'attribuzione di una soggettività giuridica piena almeno per i robot più sofisticati in modo tale da consentire l'applicazione di meccanismi di riparazione per equivalente del danno cagionato dal funzionamento dei medesimi; il "Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia" della Commissione europea, COM (2020) 65 *final*, 16 febbraio 2020, ha sostenuto la necessità di adeguare la normativa in materia di sicurezza e responsabilità alle problematiche che i sistemi di AI sollevano; la "Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità" della Commissione europea, COM (2020) 64 *final*, 16 febbraio 2020, ha enunciato *expressis verbis* l'esigenza che il livello di protezione della vittima di sistemi di AI non sia inferiore a quello assicurato alla vittima di prodotti tradizionali, non compromettendo lo sviluppo dell'innovazione tecnologica; infine, la Risoluzione del Parlamento UE del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, (2020/2014(INL)), ha distinto gli effetti in base ai sistemi di AI, prevedendo una responsabilità oggettiva per i sistemi di AI ad alto rischio, con assicurazione obbligatoria, e una responsabilità per colpa presunta per i sistemi di AI a rischio limitato. Sul dibattito in ambito UE, con particolare riferimento alla posizione della Commissione, v. U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, in *Riv. dir. civ.*, n. 6, 2020, pp. 1246 ss., spec. pp. 1249 ss.; 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 ss. Sulla Risoluzione del Parlamento europeo del 20 ottobre 2020 si veda 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 ss.

11 Si veda il Considerando Z della Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, (2015/2103(INL)), e il Considerando J e il punto 13 della Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI)). Su quest'ultima risoluzione si rinvia a 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 ss., 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, spec. p. 12.

12 Sulle implicazioni della rivoluzione digitale nel settore finanziario in dottrina si rinvia a G. Alpa, *Fintech: un laboratorio per i giuristi*, in *Contr. impr.*, n. 2, 2019, pp. 377 ss., e nella dottrina straniera 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 ss., T.C.W. Lin, *Artificial intelligence, finance, and the law*, in *Fordham Law Rev.*, Vol. 88, Issue 2, pp. 531 ss. Sull'erogazione di servizi finanziari digitalizzati 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 ss.

13 Indica espressamente i servizi indicati quali campi di applicazione dell'AI nel settore finanziario 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. Più in generale si rinvia a 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 ss., e E. Mostacci, *L'intelligenza artificiale in ambito economico e finanziario*, in *DPCE online* (dpceonline.it), n. 1, 2022, pp. 361 ss. In un momento iniziale la proposta di Regolamento UE in materia

Come ha notato una parte della dottrina, l'adozione dell'intelligenza artificiale nel settore finanziario può assicurare benefici per gli investitori: ad esempio, può portare i soggetti abilitati a formulare raccomandazioni di investimento o valutazioni creditizie oggettivamente più affidabili. Non mancano altrettanti rischi: per la negoziazione algoritmica ad alta frequenza, episodi di repentina e alta volatilità delle quotazioni dei titoli nei mercati finanziari (i cc.dd. *flash crash*)[14]; per la consulenza finanziaria automatizzata, la tendenza di uniformità di comportamenti degli investitori, in luogo della valutazione appropriata e adeguata al profilo di ognuno (c.d. effetto *herding*)[15]; per la valutazione del merito creditizio, la possibile esclusione dall'accesso al credito di determinati gruppi sociali[16].

È in tale contesto che occorre valutare la tenuta dell'apparato normativo in materia di *market abus*e a fronte alla digitalizzazione della finanza e dell'operatività nei mercati di agenti non umani. L'esigenza di effettuare tale valutazione è particolarmente urgente con riferimento all'attività di *trading*, là dove l'utilizzo di sistemi di AI è già ampiamente diffuso, ma la dottrina più attenta non manca di rilevare che analoga esigenza si pone con riferimento anche al rapporto tra *MAR* e gestione delle informazioni privilegiate[17].

Sugli abusi di mercato l'ordinamento eurounitario e quello nazionale hanno predisposto un doppio binario sanzionatorio, sviluppatosi con una tendenziale sovrapposizione di illeciti penali e amministrativi, nell'intento di assicurare il corretto ed ordinato svolgimento delle transazioni[18]. Il divieto di *insider trading* salvaguarda la parità

di intelligenza artificiale, avanzata dalla Commissione europea nell'aprile 2021 ha classificato soltanto i sistemi di *credit scoring* quali i sistemi di AI "ad alto rischio" (All. III, punto 5, lett. b) in quanto insistono su servizi privati essenziali e possono perpetuare discriminazioni fondate su origini razziali o etniche, disabilità, età o orientamento sessuale. Il successivo testo di compromesso ha aggiunto nell'ambito del settore n. 5 di accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi, alla lett. b), i sistemi di AI destinati ad essere utilizzati a fini assicurativi, ovvero i sistemi per la determinazione dei premi, la sottoscrizione e la valutazione dei sinistri. Tuttavia, considerato il carattere flessibile della proposta, è presumibile ed auspicabile che il perimetro di applicazione dell'intelligenza artificiale ai servizi finanziari possa essere esteso a: a) *portfolio construction and rebalancing*, b) *roboadvice* e altre forme di AI nella consulenza, 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*.

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 ss.

15 Sul tema 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 ss.; 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 ss.; F. Sartori, *La consulenza finanziaria automatizzata: problematiche e prospettive*, in *Riv. trim. dir. econ.* (*fondazionecapriglione.luiss.it*), n. 3, 2018, pp. 253 ss.

16 Sui rischi attinenti all'applicazione di sistemi algoritmici di *credit scoring* si rinvia a 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 ss., in part. pp. 93-95. Per uno studio sull'esperienza maturata dagli intermediari italiani nell'adozione dei modelli di *credit scoring* si veda 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 Si veda F. Annunziata, *Artificial intelligence and market abuse legislation. A European perspective*, Edward Elgar, 2023 (dattiloscritto, in corso di pubblicazione, consultato per gentile concessione dell'Autore).

18 Il legislatore italiano, con la L. 18 aprile 2005, n. 62, in attuazione della Direttiva CE/6/2003 (*Market Abuse Directive*, c.d. *MAD*) ha introdotto un doppio binario cumulativo di illeciti penali (artt. 184 e 185 TUF) e di illeciti amministrativi (artt. 187-*bis* e 187-*ter* TUF).

di accesso alle informazioni sensibili e contrasta lo sfruttamento illegittimo di informazioni privilegiate[19]; il divieto di manipolazione del mercato protegge l'andamento degli scambi dalla diffusione di informazioni false, da comportamenti simulati o altri artifici da parte di coloro che sono in grado di influire sul processo di formazione dei prezzi degli strumenti finanziari. Le fattispecie incriminatrici (artt. 184 e 185 TUF) dal canto loro intendono prevenire e reprimere le condotte abusive più gravi, unicamente a carattere doloso, laddove le fattispecie d'illecito amministrativo (artt. 187-*bis* e 187-*ter* TUF) contemplano anche le condotte abusive meno gravi, anche a titolo di colpa, che trovano la propria risposta sanzionatoria in misure pecuniarie ed interdittive[20].

La disciplina penale sull'illecito di abuso di informazioni privilegiate, che è sanzionato con pene detentive e pecuniarie, riguarda anzitutto gli "*insider* primari", ovvero chiunque, essendo in possesso delle stesse in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio, o per il fatto di essere coinvolto in attività criminali:

«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;

19 La normativa ruota intorno a due principali obblighi: uno di *disclosure* in quanto impone alle società quotate di comunicare immediatamente al mercato tutte le informazioni privilegiate di cui vengono a conoscenza e che le riguardano; un divieto di operare e anche di rivelare in modo selettivo ad alcuni soggetti queste informazioni privilegiate o dare consigli di investimento. In base all'art. 7 del Regolamento (UE) *MAR*, l'informazione è privilegiata quando ricorrono quattro elementi: a) l'informazione riguarda uno o più emittenti (c.d. corporate information) o uno o più strumenti finanziari (c.d. *market information*), b) l'informazione non è pubblica, ovvero un'informazione non disponibile alla generalità degli investitori sul mercato, c) l'informazione ha carattere "preciso", d) l'informazione è *price sensitivity*, ossia è un'informazione che, se resa pubblica, "potrebbe avere un effetto significativo sui prezzi di tali strumenti finanziari". In particolare, l'informazione ha carattere preciso se i) "fa riferimento a una serie di circostanze esistenti o che si può ragionevolmente ritenere che vengano a prodursi o a un evento che si è verificato o del quale si può ragionevolmente ritenere che si verificherà" e se ii) "è sufficientemente specifica da permettere di trarre conclusioni sul possibile effetto di detto complesso di circostanze o di detto evento sui prezzi degli strumenti finanziari". Inoltre, nel caso di un "processo prolungato che è inteso a concretizzare, o che determina, una particolare circostanza o un particolare evento, tale futura circostanza o futuro evento, nonché le tappe intermedie di detto processo che sono collegate alla concretizzazione o alla determinazione della circostanza o dell'evento futuri, possono essere considerati come informazioni aventi carattere preciso". E ancora, è chiarito nello stesso articolo che una "tappa intermedia in un processo prolungato" può costituire, a sua volta, un'informazione privilegiata. Riguardo alla *price sensitivity*, per "informazione che, se comunicata al pubblico, avrebbe probabilmente un effetto significativo sui prezzi degli strumenti finanziari (...) s'intende un'informazione che un investitore ragionevole probabilmente utilizzerebbe come uno degli elementi su cui basare le proprie decisioni di investimento". L'accertamento della consumazione dell'abuso di informazione privilegiata è di difficile individuazione ed è necessario il ricorso a presunzioni che consentano di risalire al fatto ignoto (*factum probandum*) desumendolo da fatti noti gravi, precisi e concordanti (indizi o fonti della presunzione) alla stregua di canoni di ragionevole probabilità e secondo regole di esperienza. Sull'evoluzione della nozione di informazione privilegiata, sia in ambito normativo sia in quello giurisprudenziale, si veda S. SEMINARA, *L'informazione privilegiata*, in M. CERA – G. PRESTI (a cura di), *Il testo unico finanziario*, cit., pp. 2124 ss.

20 La fattispecie di manipolazione del mercato può essere realizzata mediante più condotte differenti: le condotte di c.d. "manipolazione informativa" per la diffusione di notizie false e le condotte di c.d. "manipolazione operativa" tramite il conferimento di ordini o l'esecuzione di operazioni secondo una varietà di strategie, alcuni delle quali esemplificativamente indicate. Si tratta di comportamenti che possono alterano la trasparenza e la correttezza delle negoziazioni in ambito finanziario. L'eventuale realizzazione di due o più delle condotte darà sempre luogo a una sola sanzione penalmente rilevante e non a un concorso di illeciti.

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)».

L'illecito è esteso anche ai cosiddetti "*insider* secondari" cioè a coloro che entrano in possesso di informazioni privilegiate per altre circostanze sapendo, o comunque dovendo sapere, che si tratta di informazioni privilegiate.

La disciplina penale sulla manipolazione del mercato prevede per chiunque diffonda notizie false o ponga in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, sanzioni detentive e pecuniarie (art. 185 TUF).

La Direttiva 89/592/CEE del 13 novembre 1989 (*Coordinating Regulations on insider trading*) aveva previsto unicamente il divieto di *insider trading*. Soltanto con la Direttiva CE/6/2003 (*Market Abuse Directive*, c.d. *MAD I*) è stata inclusa, nell'ambito delle fattispecie di *market abuse*, quella di manipolazione del mercato, imponendo agli Stati membri l'obbligo di adottare le sanzioni amministrative e lasciando libertà ai legislatori nazionali quanto all'introduzione delle sanzioni penali per entrambe le fattispecie. Successivamente, il legislatore eurounitario ha adottato due nuovi strumenti normativi (il Regolamento (UE) 596/2014, *Market Abuse Regulation*, c.d. *MAR*, e la Direttiva 2014/57/UE, *Criminal Sanctions Market Abuse Directive*, c.d. *CSMAD*, o *Market Abuse Directive 2*, c.d. *MAD II*). Con il Regolamento (UE) *MAR*, che si applica dal 2 luglio 2016, è stato perseguito l'obiettivo di massima e immediata armonizzazione delle fattispecie in analisi, è stato esteso l'ambito di applicazione e sono stati definiti nel dettaglio i limiti edittali e non delle sanzioni amministrative; con la Direttiva *MAD II* è stato previsto l'obbligo (e non più la facoltà) degli Stati membri UE di introdurre sanzioni penali.

Gli illeciti amministrativi sono stati poi riqualificati dalla giurisprudenza della Corte EDU con la nota sentenza *Grande Stevens*. I giudici di Strasburgo, infatti, hanno ritenuto che le fattispecie amministrative di abuso di informazioni privilegiate (art. 187-*bis* TUF) e di manipolazione del mercato (art. 187-*ter* TUF) dovessero essere considerate sostanzialmente penali a causa del livello di severità delle sanzioni previste (pecuniarie, interdittive e ablatorie)[21], in coerenza con i criteri stabiliti dalla medesima

21 Corte EDU, 4 marzo 2014, ric. n. 18640/2010, *Grande Stevens ed altri c. Italia*). Su questa decisione si vedano *ex multis* i commenti di 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 ss.; P. Montalenti, *Abusi di mercato e procedimento Consob: il caso Grande Stevens e la Sentenza CEDU*, in *Giur. comm.*, n. 3, 2015, pp. 478 ss.; A. Genovese, *Il controllo del giudice sulla regolazione finanziaria*, in *Banca borsa tit. cred.*, n. 1, 2017, pp. 49 ss.; 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 ss.

giurisprudenza con la sentenza *Engel*[22].

Un siffatto carattere è stato condiviso successivamente dalla Corte di giustizia UE[23] e dalla Corte costituzionale, quest'ultima pronunciandosi recentemente sulla retroattività *in mitius* delle sanzioni amministrative[24] e sul diritto al silenzio (c.d. *nemo tenetur se detegere*)[25] nei procedimenti di natura formalmente amministrativa in materia di abusi di mercato[26].

22 Corte EDU, 8 giugno 1976, ric. n. 5100/71, *Engel e altri c. Paesi Bassi*, ha definito tre criteri per la qualificazione sostanzialmente penale delle sanzioni amministrative: la qualificazione giuridica dell'illecito nel diritto nazionale; la natura dell'illecito e la finalità repressiva della sanzione; la natura punitiva e il grado di severità della sanzione; il collegamento con una violazione penale. Dopo questa sentenza, la Corte EDU, 28 novembre 1999, *Escobet c. Belgio*, ha sostenuto che «in ogni caso la nozione di pena contenuta nell'art. 7 della Convenzione come quella di accusa in materia penale che figura nell'art. 6 hanno portata autonoma [...] la Corte non è vincolata dalle qualificazioni del diritto interno, che hanno valore relativo». Sui criteri sviluppati dalla vicenda *Engel* si è espressa in senso sostanzialmente conforme alla Corte EDU la Corte di giustizia UE, sentenze del 5 giugno 2012, *Bonda*, C-489/10, EU:C:2012:319, punto 37, e del 26 febbraio 2013, *Åkerberg Fransson*, C-617/10, EU:C:2013:105, punto 35.

23 Rispettivamente con riferimento alla fattispecie di manipolazione del mercato, prevista dall'art. 187-*ter* TUF, e alla fattispecie di abuso di informazione privilegiata, prevista dall'art. 187-*bis* TUF, la Corte di giustizia UE, sentenza del 20 marzo 2018, *Garlsson Real Estate SA c. Consob*, C-537/16, EU:C:2018:193, punto 33, e sentenza del 20 marzo 2018, *Di Puma c. Consob*, C-596/16 e C-597/16, EU:C:2018:192, punto 35, qualifica le sanzioni sostanzialmente penali sulla base della natura dell'illecito e della gravità della sanzione.

24 Corte cost., sentenza 21 marzo 2019, n. 63, sulla quale si rinvia al commento di E. Bindi – A. Pisaneschi, *La retroattività* in mitius *delle sanzioni amministrative Consob*, in *Giur. comm.*, n. 5, 2019, pp. 1015 ss.

25 Corte cost., ordinanza 10 maggio 2019, n. 117, sulla quale si rinvia ai commenti di A. Logli, *Poteri istruttori della Consob e* nemo tenetur se detegere, in *Giur. comm.*, n. 2, 2020, pp. 230 ss.; 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 ss. In generale sul tema si rinvia a 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 ss.

26 Prima di queste decisioni la natura sostanzialmente penale del procedimento e delle sanzioni in materia di abusi di mercato era stata affermata dalla Corte costituzionale, sentenze 12 dicembre n. 223 e 12 aprile 2017 n. 68. Fuori da questo ambito, la giurisprudenza della Corte di Cassazione (Cass., Sez. II, 26 settembre 2019, n. 24081 e n. 24082; Cass., Sez. II, 6 agosto 2019, n. 21017; Cass., Sez. II, 5 aprile 2017 n. 8855; Cass., Sez. I, 2 marzo 2016, n. 4114; Cass., Sez. I, 30 giugno 2016, n. 13433) e delle Corti d'Appello non riconoscono la natura sostanzialmente penale delle sanzioni amministrative di Consob, sulla base della circostanza che la sentenza *Grande Stevens* riguardava unicamente gli abusi di mercato, seppure la stessa Corte costituzionale (sentenza 21 marzo 2019, n. 63) abbia espressamente rilevato che «è da respingere l'idea che l'interprete non possa applicare la CEDU, se non con riferimento ai casi che siano già stati oggetto di puntuali pronunce da parte della Corte di Strasburgo». Analogamente la giurisprudenza della Corte di Cassazione (Cass. civ., Sez. II, 3 gennaio 2019, n. 4 e Cass. civ., Sez. II, 28 settembre 2016, n. 19219; Cass. civ, Sez. II, 18 aprile 2018, n. 9517; Cass. civ., Sez. II, 11 gennaio 2017, n. 463; Cass. civ., Sez. II, 4 agosto 2016, n. 16313; Cass. civ., Sez. II, 10 marzo 2016, n. 4725; Cass. civ., Sez. II, 14 dicembre 2015, n. 25141; Cass. civ, Sez. II; 3 dicembre 2013, n. 27038; Cass. civ., Sez. Un., 30 settembre 2009, n. 20935 e 20939; Cass. civ., Sez. II, 24 febbraio 2016, n. 3656) si è pronunciata con riguardo a tutti gli illeciti e i procedimenti di competenza di Banca d'Italia. Il Consiglio di Stato, rimasto competente per le sanzioni amministrative comminate dall'IVASS, ha invece qualificato tali sanzioni sostanzialmente penali in ragione del loro carattere afflittivo sulla base dei criteri Engel (Cons. Stato, Sez. VI, 28 marzo 2019, nn. 2042 e 2043). Questa diversa ricostruzione è la conseguenza del riconoscimento della competenza in capo a differenti organi giurisdizionali per i provvedimenti sanzionatori adottati dalle autorità indipendenti a seguito degli interventi della Corte costituzionale, sentenze 20 giugno 2012, n. 162, e 4 aprile 2012, n. 94, che hanno riattribuito al giudice ordinario, ovvero alla Corte d'Appello, la giurisdizione sulle sanzioni di Banca d'Italia e Consob per un difetto di delega nel codice del processo amministrativo che aveva trasferito tutte le sanzioni delle autorità di regolazione dei mercati alla giurisdizione esclusiva del giudice amministrativo. Si rinvia per una ricostruzione della giurisprudenza sulla qualificazione delle sanzioni di Banca d'Italia e Consob a E. Bindi – P. Luccarelli – A. Pisaneschi, *Le sanzioni della Banca d'Italia e della Consob*, in *Giur. comm.*, n. 3, 2021, pp. 553 ss., spec. pp. 555-559, e 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 ss., spec. pp. 83-86. In dottrina si esprime a favore di un'estensione dell'ambito della materia sostanzialmente penale per le sanzioni irrogate dalla Consob e da Banca d'Italia oltre il perimetro degli abusi di mercati 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, spec. p. 95.

A causa di questa riqualificazione sono state sollevate una serie di questioni sulla presunta violazione dell'art. 6 CEDU, riguardante il diritto ad un processo equo, dell'art. 4 del Protocollo 7 CEDU, concernente la violazione del principio del *ne bis in idem*, dell'art. 7 CEDU che consacra il principio del *favor rei* e della retroattività della *lex mitior*, nonché degli artt. 47 e 48 della Carta dei diritti fondamentali UE per la violazione del diritto al silenzio[27].

La già citata sentenza *Grande Stevens*, pur evidenziando la violazione del principio del giusto processo nel procedimento sanzionatorio Consob in materia di *market abuse*[28], ha rilevato però che le garanzie previste dall'art. 6 CEDU sono comunque salvaguardate dalla previsione del giudizio di opposizione davanti alla Corte d'Appello, per motivi anche di merito, e dal giudizio di legittimità dinnanzi alla Corte di Cassazione, per soli motivi di legittimità, contro i medesimi provvedimenti sanzionatori dell'autorità di vigilanza. Secondo la Corte EDU, infatti, lo Stato è libero di scegliere dove collocare le garanzie dell'equo processo, nella fase amministrativa o nella fase giurisdizionale, in quanto trattasi di decisione rimessa all'apprezzamento delle autorità nazionali[29].

Sulla presunta violazione del *ne bis in idem* (o *double jeopardy*), i giudici di Strasburgo, con un brusco *revirement*, nella decisione *A/B c. Norvegia*, hanno ammesso la compatibilità convenzionale di una duplice risposta sanzionatoria sostanzialmente penale e di una pluralità di procedimenti riguardanti il medesimo fatto qualora vi sia una «connessione sostanziale e temporale sufficientemente stretta», ravvisabile in presenza di alcuni determinati criteri[30].

27 Su tutte queste questioni si veda per tutti 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 ss.

28 La predetta violazione si riferiva al previgente Regolamento sul procedimento sanzionatorio Consob 19 dicembre 2013, n. 18750, nella misura in cui il procedimento non garantiva il rispetto di un contraddittorio adeguato, non prevedeva un'udienza pubblica e non assicurava l'imparzialità dell'organo giudicante. In particolare, il procedimento, così come era articolato, era in contrasto con il principio di parità delle armi di accusa e difesa in quanto non consentiva all'interessato un'interlocuzione sulla Relazione conclusiva prima della determinazione finale della Commissione.

29 Dopo la sentenza Grande Stevens della Corte EDU il Consiglio di Stato (sentenze 26 marzo 2016, n. 1595 e n. 1596) ha ravvisato l'incompatibilità del procedimento sanzionatorio Consob con il principio del contraddittorio sancito dall'art. 195 TUF poiché la Relazione conclusiva dell'Ufficio Sanzioni Amministrative «non è oggetto di comunicazione (o di altre forme di conoscenza) e rispetto ad esso non vi è alcuna possibilità di controdeduzione». Tuttavia, queste pronunce non hanno ravvisato alcun contrasto con la CEDU ma unicamente i principi del contraddittorio "rinforzato" sanciti dall'art. 187-septies TUF. Oltre a queste pronunce della giustizia amministrativa, anche decisione della giustizia ordinaria hanno pronunciato la legittimità del procedimento sanzionatorio della Consob (Corte d'Appello di Roma, decreto 30 maggio 2014; Corte d'Appello di Roma, sentenza 1° luglio 2014; Corte d'Appello di Bologna, sentenza 3 marzo 2015, n. 199). La Consob ha comunque modificato il Regolamento sul Procedimento Sanzionatorio, con delibera n. 19521 del 24 febbraio 2016, introducendo il diritto dei destinatari della lettera di contestazione degli addebiti, che abbiano presentato deduzioni scritte o abbiano partecipato all'audizione, di ricevere la relazione finale e di presentare le proprie controdeduzioni rispetto alle conclusioni raggiunte dall'ufficio entro trenta dalla ricezione della stessa.

30 Corte EDU, sentenza 15 novembre 2016, ric. nn. 24130/11 e 29758/11, *A. e B. c. Norvegia*, ha elaborato alcuni criteri per individuare una siffatta connessione dal punto di vista sostanziale e temporale. Con riferimento ai primi la connessione sussiste *«– 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*

La legittimità del doppio binario sanzionatorio, penale e amministrativo, è stata ribadita altresì dalla giurisprudenza eurounitaria in quanto è stata riconosciuta agli Stati membri UE «libertà di scelta delle sanzioni applicabili che possono assumere la forma di sanzioni amministrative, di sanzioni penali o di una combinazione di entrambe»[31] purché la duplicazione sanzionatoria complessivamente irrogata rispetti il principio di proporzionalità[32]. In tale senso depone altresì il disposto dell'art. 187-*terdecies* TUF che, in applicazione di detto principio, stabilisce che l'autorità, giudiziaria o amministrativa, che si pronuncia per seconda sullo stesso fatto, debba tenere conto, al momento dell'irrogazione delle sanzioni di proprio competenza, delle misure già irrogate. Questo controllo di proporzionalità può condurre, come affermato dalla giurisprudenza di legittimità, a disapplicare, totalmente o parzialmente, la sanzione che debba essere applicata per ultima qualora la prima sia commisurata al disvalore del fatto o comunque a modulare la seconda tenendo conto della prima[33].

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». Con riguardo alla connessione temporale «*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*». Per alcuni commenti sulla sentenza si rinvia a F. VIGANÒ, *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, 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 ss.

31 Corte di giustizia UE, sentenza 20 marzo 2018, C-524/15, *Menci*, par. 47; Corte di giustizia UE, sentenza 20 marzo 2018, C-537/16, *Garlsson Real Estate SA e altri*, punto 49; Corte di giustizia UE, sentenza 20 marzo 2018, C-596/16 e C-597/16, *Di Puma c. Consob*, punto 26. Su queste tre decisioni si rinvia a F. CONSULICH, *Il prisma del* ne bis in idem *nelle mani del Giudice eurounitario*, in *Dir. pen. proc.*, n. 7, 2018, pp. 949 ss.

32 Corte di giustizia UE, sentenza 20 marzo 2018, C-537/16, *Garlsson Real Estate SA e altri*, punto 60, aveva manifestato perplessità sull'efficacia del principio di proporzionalità, considerato il tenore previgente dell'art. 187-*terdecies* TUF che sembrava fare riferimento soltanto al cumulo di pene pecuniarie e non anche al cumulo di una sanzione amministrativa pecuniaria di natura penale e di una pena della reclusione.

33 Corte di Cassazione penale, Sez. V, sentenza 15 aprile 2019, n. 3999. Si veda 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. Si è avuta applicazione dell'art. 187-*terdecies* TUF da parte della Corte d'Appello di Milano, Sez. II, sentenza 15 gennaio 2019 (dep. 15 aprile 2019), n. 284, sulla quale si rinvia al commento di C. PAGELLA, *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. Un siffatto scrutinio di proporzionalità della complessiva risposta sanzionatoria, tuttavia, potrebbe non essere sufficiente dopo la sentenza della Corte EDU, 6 giugno 2019, ric. n. 47342/14, *Nodet c. Francia*, che – pur esplicitamente estendendo i criteri di *A/B c. Norvegia* agli abusi di mercato – aderisce ad una interpretazione restrittiva dei criteri, che riguarderebbe non solo il piano sanzionatorio ma il diritto a non essere sottoposto a due procedimenti per il medesimo fatto, con conseguente valutazione di tutti i parametri della c.d. «*close connection*» per escludere la violazione del *ne bis in idem*. Sulla sentenza si veda la nota di 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. Sul doppio binario sanzionatorio è intervenuta da ultimo la Corte costituzionale, sentenza 16 giugno 2022, n. 149, in materia di violazione dei diritti d'autore. La Corte ha reputato fondata la questione di illegittimità costituzionale dell'art. 649 c.p.p. nella parte in cui non prevede che il giudice pronunci il proscioglimento o il non luogo a procedere nei confronti di un imputato per un delitto in materia di diritto d'autore che, in relazione allo stesso fatto, sia già stato sottoposto a un procedimento sanzionatorio, ormai concluso. In questa circostanza i giudici hanno altresì rivolto un monito al legislatore per superare la disarmonia e rimeditare complessivamente i sistemi di doppio binario sanzionatorio ancora vigenti. Si veda il commento di 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.

Questo processo di estensione delle garanzie convenzionali ha riguardato il principio del *favor rei* e della retroattività della *lex mitior*[34]. Sulle sanzioni amministrative in materia di abusi di mercato tali principi sono stati consacrati dalla Corte costituzionale, con la sentenza n. 63 del 2019, che ha dichiarato incostituzionale l'art. 6, comma 2, del d.lgs. n. 72 del 2015 nella parte in cui escludeva l'applicazione retroattiva della legge successiva più favorevole. In tale circostanza, i giudici costituzionali hanno affermato l'applicazione dei principi elaborati in materia penale qualora il fatto non sia più considerato illecito o sia mutato l'apprezzamento della gravità di esso da parte dell'ordinamento, salvo che vi siano ragioni di tutela di interessi di rango costituzionale tali da resistere al medesimo vaglio di ragionevolezza[35].

L'ultimo approdo concerne l'applicazione del diritto di non cooperare alla propria incriminazione (c.d. *nemo tenetur se detegere*) e del diritto al silenzio da parte dell'incolpato nei procedimenti amministrativi in materia di *market abuse* davanti alla Consob. La questione è stata oggetto di un dialogo giurisprudenziale tra Corte costituzionale[36] e Corte di giustizia UE[37], a seguito di un incidente di costituzionalità sollevato dalla Corte di Cassazione[38]. In particolare, i giudici di Lussemburgo, partendo dalla considerazione che il diritto al silenzio è garantito dagli artt. 47 e 48 della Carta dei diritti fondamentali UE, escludono che una persona possa essere sanzionata in siffatte circostanze. Condividendo questo assunto iniziale – e tenuto conto della natura punitiva delle sanzioni amministrative in materia di abusi di mercato – la Corte costituzionale ha dichiarato l'illegittimità dell'art. 187-*quinquesdecies* TUF, nella parte in cui sanziona chi si sia rifiutato di rispondere alle domande di Banca d'Italia e Consob nell'esercizio del diritto al silenzio. Questo principio, tuttavia, non viene considerato assoluto in quanto la decisione precisa che «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

34 Il fondamento del principio di retroattività *in mitius* ha ricevuto un fondamento costituzionale nell'art. 3 Cost.: il principio di eguaglianza «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 vigora della norma che ha disposto l'abolitio criminis o la modifica mitigatrice» (Corte costituzionale, sentenza 27 luglio 2011, n. 236). Invero, tale principio è entrato a fare parte dell'ordinamento nazionale con la pronuncia della Corte EDU (sentenza 17 settembre 2009, ric. n. 10249/03, *Scoppola c. Italia*) che, per il tramite della norma di apertura all'ordinamento convenzionale dell'art. 117 Cost., ha ricevuto un nuovo fondamento con l'interposizione dell'art. 7 CEDU, salvo disconoscere la sua natura assoluta qualora il legislatore individui deroghe o limitazioni sorrette da una valida giustificazione.

35 Corte cost., sentenza 21 marzo 2019, n. 63. Sul punto si rinvia ai commenti di 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 ss., 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 ss.

36 Corte cost., ordinanza 10 maggio 2019, n. 117. Su questa ordinanza si rinvia al commento di 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 ss.

37 Corte di giustizia UE, sentenza del 2 febbraio 2021, *DB c. Consob*, C-481/19, EU:C:2021:84. Si veda il commento di 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 ss.

38 Corte di Cassazione civile, Sez. II, ordinanza 16 febbraio 2018, n. 3831, con nota di 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.

stessa. Né il diritto al silenzio potrebbe legittimare l'omessa consegna di dati, documenti, registrazioni preesistenti alla richiesta della CONSOB»[39].

Il quadro normativo in materia, a seguito degli interventi eurounitari del Regolamento (UE) *MAR* e della Direttiva (UE) *MAD II*, è quindi articolato sulla possibilità di configurazione di un doppio binario sanzionatorio di illeciti penali e illeciti amministrativi, in quanto lascia agli Stati membri la facoltà di punire le violazioni di *market abuse*, oltre che con sanzioni penali per le condotte ritenute più gravi, anche con sanzioni amministrative. Ciò non solo delinea discipline nazionali non armonizzate ma, com'è stato notato, possibili difficoltà di coordinamento tra i procedimenti dell'autorità di vigilanza e i processi dell'autorità giurisdizionale e il rischio di violazione del principio eurounitario (art. 50 Carta dei diritti fondamentali UE) e convenzionale (art. 7 CEDU) del *ne bis in idem*. Su quest'ultima questione la legislazione europea incarica gli Stati membri di garantire che l'irrogazione di sanzioni penali per i reati ai sensi della Direttiva (UE) *MAD II* e di sanzioni amministrative ai sensi del Regolamento (UE) MAR non violino il divieto del doppio processo per l'*idem factum* (considerando n. 23 della Direttiva *MAD II*), questione poi che è stata amplificata dalla natura sostanzialmente penale delle sanzioni amministrative e dalla relativa estensione dei principi del processo equo al procedimento[40].

2 La distinzione tra AI "deboli" e AI "forti"

Nel quadro normativo così sinteticamente delineato, hanno da tempo fatto il proprio ingresso, da protagonisti, i sistemi di intelligenza artificiale, ponendo plurimi interrogativi a regolatori e interpreti del diritto dei mercati finanziari.

Per un corretto approccio metodologico al tema, occorre procedere con una identificazione del fenomeno.

I sistemi di AI si distinguono in base alla loro differente capacità d'interazione con l'uomo[41]. Rispetto ai sistemi primordiali di AI (cc.dd. sistemi di AI "deboli"), i cui

39 Corte cost., sentenza 30 aprile 2021, n. 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 ss., 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 ss.

40 Su alcune proposte di soluzione, a legislazione vigente e *de iure condendo*, v. C. DEODATO, *op. cit.*, pp. 28 ss.

41 N. ABRIANI – G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale*, Bologna, 2021, pp. 21 ss., distinguono i sistemi di intelligenza artificiale sulla base di due differenti approcci. Secondo un primo approccio i differenti sistemi di intelligenza artificiale sono suddivisi in ragione dei differenti modelli statistico-matematici di elaborazione delle informazioni e di apprendimento automatico (*machine learning*, *supervised learning*, *reinforcement learning*, *unsupervised learning* e *deep learning*). Secondo un altro approccio, i sistemi di intelligenza artificiale sono identificati sulla base della loro capacità di interazione con l'intelligenza umana, per cui sono distinti sistemi di intelligenza assistita, sistemi di intelligenza aumentata, sistemi di intelligenza amplificata e sistemi di intelligenza autonoma. La proposta di regolamento UE definisce «sistema di intelligenza artificiale» (sistema di AI): «un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono». Nell'Allegato I sono indicati i seguenti approcci: a) approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (deep learning); b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti; c) approcci statistici,

outputs dipendono dalle istruzioni prestabilite da produttori, programmatori o utenti, i sistemi di AI più evoluti (cc.dd. sistemi di AI "forti") sono dotati di capacità di autoapprendimento e producono, quindi, *outputs* autonomi e imprevedibili rispetto agli *inputs* iniziali di produttore, programmatore o utente[42]. Dal momento che l'*iter* logico-decisionale seguito da questo secondo tipo di AI non è di per sé trasparente e immediatamente decifrabile, si è solito anche designarlo come "*black box*"[43].

Per i sistemi di AI "forti" diviene centrale, pertanto, la questione del controllo umano sul loro funzionamento e sul risultato dell'elaborazione dei dati immessi nel sistema.

La proposta di Regolamento (UE) sull'intelligenza artificiale definisce il c.d. *duty of human oversight* (art. 14)[44] ma non copre tutta la catena di produzione dell'*output*: l'art. 14, infatti, riguarda unicamente il momento della raccolta dei dati e non è esteso alla loro successiva elaborazione, proprio a cagione della difficoltà di comprendere appieno il funzionamento e i meccanismi che governano gli algoritmi di autoapprendimento[45].

stima bayesiana, metodi di ricerca e ottimizzazione. Sulla distinzione tra "*augmented intelligence*" e "*artificial intelligence*" v., da ultimo, F. ANNUNZIATA, *Artificial intelligence and market abuse legislation. A European perspective*, cit., pp. 133-141.

42 La distinzione tra sistemi di AI forti e sistemi di AI deboli è ormai diffusa sia nella dottrina civilistica sia in quella penalistica ma si veda per una prima esemplificazione a P. SPERA, voce *Intelligenza artificiale*, in G. ZACCARI – P. PERRI (a cura di), *Dizionario Legal Tech*, Milano, 2020, pp. 535 ss., e a F. MAGGINO – G. CICERCHIA, *Algoritmi, etica e diritto*, in *Dir. inf.*, n. 6, 2019, p. 1165, ma anche più diffusamente si veda anche G. PASCERI, *Intelligenza artificiale, algoritmo e* machine learning, Milano, 2021, pp. 18- 24.

43 Questa espressione è stata coniata da F. PASQUALE, *The black-box society: The secret algorithms that control money and information*, Cambridge-London, 2015. In senso critico si rinvia a 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 ss.

44 L'art. 14 della proposta di Regolamento (UE) sull'intelligenza artificiale disciplina la sorveglianza umana, stabilendo che «1. (i) sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui il sistema di IA è in uso. 2. La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare quando tali rischi persistono nonostante l'applicazione di altri requisiti di cui al presente capo. 3. La sorveglianza umana è garantita mediante almeno una delle seguenti misure: a) misure individuate e integrate nel sistema di IA ad alto rischio dal fornitore prima della sua immissione sul mercato o messa in servizio, ove tecnicamente possibile; b) misure individuate dal fornitore prima dell'immissione sul mercato o della messa in servizio del sistema di IA ad alto rischio, adatte ad essere attuate dall'utente. 4. Le misure di cui al paragrafo 3 consentono le seguenti azioni, a seconda delle circostanze, alle persone alle quali è affidata la sorveglianza umana: a) comprendere appieno le capacità e i limiti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, in modo che i segnali di anomalie, disfunzioni e prestazioni inattese possano essere individuati e affrontati quanto prima; b) restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio ("distorsione dell'automazione"), in particolare per i sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche; c) essere in grado di interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto in particolare delle caratteristiche del sistema e degli strumenti e dei metodi di interpretazione disponibili; d) essere in grado di decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio; e) essere in grado di intervenire sul funzionamento del sistema di IA ad alto rischio o di interrompere il sistema mediante un pulsante di "arresto" o una procedura analoga. 5. Per i sistemi di IA ad alto rischio di cui all'allegato III, punto 1, lettera a), le misure di cui al paragrafo 3 sono tali da garantire che, inoltre, l'utente non compia azioni o adotti decisioni sulla base dell'identificazione risultante dal sistema, a meno che essa non sia stata verificata e confermata da almeno due persone fisiche.

45 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.

La medesima proposta di Regolamento, inoltre, non prevede meccanismi di tutela che consentano alle vittime di *outputs* "errati" di ripristinare le posizioni giuridiche lese[46]. È vero, d'altronde, che la proposta di Regolamento stabilisce una serie di obblighi di trasparenza che potrebbero attenuare l'opacità dei processi di produzione degli *outputs* degli algoritmi[47], ma resta pur sempre evidente la difficoltà, anche sul piano normativo, di utilizzare per i sistemi di AI forti i consolidati principi generali di imputabilità, quali la causalità e la colpevolezza.

Sul piano pratico, l'autonomia dei sistemi di AI forti[48] complica notevolmente l'individuazione di un nesso causale tra la condotta, commissiva o omissiva, di un agente umano e l'evento produttivo di illecito, a causa della opacità degli algoritmi che guidano il funzionamento dei sistemi di AI e degli ostacoli ad una loro *disclosure* effettiva e generalizzata. E anche qualora si riesca a conoscere il procedimento che ha portato ad un determinato *output* e ad escludere qualsiasi disegno operativo da parte di un agente umano, l'illecito quale conseguenza unica del funzionamento del sistema di AI potrebbe essere qualificato come fattore causale sopravvenuto interruttivo del nesso causale (art. 41, comma 2, c.p.)[49]. Sul piano teoretico, l'imprevedibilità dei sistemi di AI forti rende difficoltosa l'imputazione della responsabilità del danno a produttori, programmatori o utenti, financo a titolo colposo[50].

46 Si veda *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.

47 In particolare, la trasparenza costituisce uno dei valori fondamentali promossi dall'UE per lo sviluppo, la diffusione e l'uso dei sistemi di AI. Dall'inizio del processo politico per la regolamentazione dell'AI, tutti i documenti ufficiali delle istituzioni dell'Unione europea hanno promosso la trasparenza quale principio guida nella disciplina dell'utilizzazione dei sistemi di AI. La proposta sottopone i sistemi di AI a rischio alto e limitato rispettivamente a regole in tema di trasparenza generalizzata e selettiva. Con riferimento ai sistemi a rischio alto prevede che i fornitori debbano garantire un livello "adeguato" di trasparenza ma non è precisato cosa debba intendersi per "adeguato" (art. 13) e debbano predisporre una disciplina relativa alla *governance* e alla gestione dei dati per i sistemi di AI che usano banche dati di informazione, con l'elencazione delle pratiche da seguire per l'addestramento, la convalida e la prova dei set di dati (art. 10, par. 2) e l'indicazione di criteri di pertinenza, rappresentatività, completezza e correttezza dei dati (art. 10, par. 3). È stabilito altresì che i sistemi di AI debbano contenere le informazioni tecniche prima che siano immessi nel mercato: le informazioni devono essere indicate in modo tale che il sistema sia conforme al regolamento (art. 11) e consenta la registrazione automatica di tutti gli eventi una volta entrato in funzione (art. 12). Allo stesso tempo, questi sistemi devono essere previamente approvati e registrati da parte dell'autorità di vigilanza prima dell'immissione sul mercato e devono essere progettati e sviluppati in modo tale da garantire la supervisione e il monitoraggio umano durante la sua utilizzazione (art. 14). I fornitori devono registrare i sistemi di AI in una banca dati prima di immetterli sul mercato (art. 60). Le informazioni elaborate nella banca dati relativamente al sistema di AI (fornitore, scopo del sistema, tipo e data di scadenza del certificato di conformità, indicazione degli Stati in cui è stato immesso sul mercato, messo in servizio o reso disponibile). La predisposizione di tutti questi meccanismi potrebbe facilitare l'accertamento probatorio del collegamento causale tra il comportamento dell'agente artificiale e l'uomo che normalmente incontra numerosi ostacoli a causa della difficoltà di decifrare la scatola nera e i codici crittografici. Si veda in questo senso U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, cit., p. 1247.

48 B. Panattoni, *op. cit.*, p. 323, ritiene preferibile fare riferimento al concetto di comportamento emergente piuttosto che di autonomia, per evitare di riconoscere ai sistemi di AI un'autonomia decisionale assimilabile all'intenzionalità. In senso analogo A. Amidei, *Intelligenza artificiale e product liability: sviluppi del diritto dell'Unione Europea*, in *Giur. it.*, n. 7, 2019, p. 1717.

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

50 Imprevedibilità non solo soggettiva ma anche oggettiva secondo 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 ss. Nella dottrina straniera su questo fenomeno di agenti artificiali "irreducible", ovvero non riconducibili all'uomo, si rinvia a

Questa prospettiva dischiude scenari insoluti di irresponsabilità, con relativo pregiudizio anche di interessi di natura pubblicistica, specialmente in ambito penalistico. Il diritto civile, infatti, conosce modelli imputativi della responsabilità più flessibili e quindi consente di collegare l'evento lesivo verificatosi in concreto mediante l'adattamento di forme di imputazione di carattere oggettivo[51]; il diritto penale, viceversa, non prevede analoghi criteri di imputazione oggettiva, sicché è elevato il rischio che si venga a creare un'area di illeciti non punibili[52] (c.d. "*responsibility gap*"[53]).

R. ABBOTT – A. SARCH, *Punishing Artificial Intelligence: Legal Fiction or Science Fiction*, in *UC Davis Law Rev.*, Vol. 53, 2019, pp. 323 ss., spec. pp. 330 ss., che individuano le caratteristiche (*unpredictably*, *unexplainably*, *autonomously*) e i motivi (*enforcement problems*, *practical irreducibility*, *legal irreducibility*) per i quali un reato commesso da un sistema di AI non possa essere attribuito ad un uomo.

51 In materia di responsabilità civile derivante dai danni prodotti dai sistemi di AI si rinvia a C. LEANZA, *Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel Terzo Millennio*, in *Resp. civ. prev.*, n. 3, 2021, pp. 1011, spec. pp. 1021-1024, il quale ritiene applicabile la disciplina da prodotto difettoso di derivazione eurounitaria (direttiva 85/374/CEE) in caso di sistema di AI debole che presenti un difetto, con attribuzione della responsabilità al produttore del sistema indipendentemente dalla sussistenza dell'elemento soggettivo del dolo o della colpa. Detta disciplina non sembra applicabile nel caso di sistemi di AI forti, ossia autonomi e capaci di assumere decisioni indipendenti rispetto alla programmazione originaria, per i quali è stata elaborata la nozione del c.d. «rischio da sviluppo» che consentirebbe l'applicazione del regime della responsabilità oggettiva previsto dall'art. 2050 c.c. in materia di danno cagionato da attività pericolosa, incentivando produttori e programmatori a destinare risorse idonee per minimizzarne la pericolosità. Si veda altresì U. RUFFOLO, *Intelligenza artificiale,* machine learning*, responsabilità da algoritmo*, cit., p. 1700, per il quale è possibile individuare l'applicazione di un'altra fattispecie di responsabilità oggettiva (art. 2051 c.c., danno cagionato da cose in custodia) a carico di colui che comunica ulteriori dati e "allena" il sistema di AI, oltre a quella similare dell'art. 2052 c.c. che disciplina il danno cagionato da animali, anche qualora siano smarriti o fuggiti. Di più difficile adeguamento è l'applicazione della disciplina consumeristica in materia di responsabilità da prodotti difettosi, che recepisce la direttiva 85/374/CEE, per i sistemi di AI forti qualora il danno sia stato cagionato da un comportamento né prevedibile né evitabile. Al riguardo, appare dirimente l'art. 120, comma 2, cod. cons. che esclude infatti la responsabilità del produttore quando il difetto non esisteva al momento in cui il prodotto è stato messo in circolazione. Evidenziano questa questione 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 ss., spec. pp. 1719 ss. Quest'ultimo propone in queste ipotesi la configurazione di una responsabilità oggettiva a carico del produttore del sistema di AI, ritenendo che la previsione o meno del difetto possa costituire unicamente elemento per la valutazione della sussistenza dell'elemento psicologico della colpa. Suggerisce altresì di estendere l'imputazione della responsabilità al programmatore in quanto ideatore dell'algoritmo che guida e compone il sistema di AI, con conseguente riduzione della responsabilità del produttore. Da ultimo, rileva che un ruolo decisivo nel funzionamento è svolta anche dal *trainee* che fornisce i dati perché il sistema di AI possa formare il proprio processo di apprendimento e di evoluzione. Quest'attività è però difficilmente riconducibile nella nozione di "prodotto" ma più esattamente di prestazione di servizi, con l'effetto di precludere l'applicazione della normativa di origine UE e la facoltà da parte del danneggiato di rivolgersi a quest'ultimo soggetto per ottenere un risarcimento dei danni. A queste posizioni si aggiunge quella di G. FINOCCHIARO, *Intelligenza artificiale e responsabilità*, in *Contr. impr.*, n. 2, 2020, p. 731, che propone la costruzione di «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». In senso conforme ID., *Intelligenza artificiale e protezione dei dati personali*, in *Giur. it.*, n. 7, 2019, p. 1676.

52 Sul punto B. PANATTONI, *op. cit.*, p. 325, che sottolinea due criticità derivanti dall'eventuale attribuzione di personalità giuridica agli agenti artificiali. In primo luogo, questa prospettiva condurrebbe ad un «crescente "antropomorfismo"» nei confronti degli agenti artificiali; in secondo luogo, alimenta il rischio di una deresponsabilizzazione degli operatori. In senso conforme C. PIERGALLINI, *Intelligenza artificiale: da 'mezzo' a 'autore' del reato?*, cit., p. 1753.

53 In questo senso A. MATTHIAS, *The responsibility gap: Ascribing responsibility for the actions of learning automata*, in *Ethics Inf. Tech.*, n. 6, 2004, pp. 175 ss.

3 *Machina delinquere non potest?*

I sistemi di AI – siano essi deboli o forti – possono essere coinvolti nella commissione di un reato, quali strumenti della sua commissione o quali autori della condotta materiale: basti pensare alle *self driving cars*, alla chirurgia robotica e alle *fake-news* tramite *chatbot*[54].

Nei fatti, la circolazione in via sperimentale di *driving cars* semiautonome[55] ha già comportato incidenti stradali[56] dovuti al malfunzionamento degli algoritmi che pilotano tali autovetture[57]. Situazioni analoghe si sono verificate in ambito sanitario, ove i sistemi di AI sono già ampiamente utilizzati, sia nella diagnosi sia nella chirurgia, per velocizzare decisioni e operazioni di precisione[58].

54 Sulla capacità dell'intelligenza artificiale di concepire e sviluppare il fatto tipico concernente "nuovi reati" si vedano le considerazioni di M. Papa, Future crimes*: intelligenza artificiale e rinnovamento del diritto penale*, in *disCrimen* (*discrimen.it*). 4 marzo 2020, pp. 9 ss.

55 Si rinvia per alcune riflessioni in ambito civile a A. Davola – R. Pardolesi, *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?*, in *Danno resp.*, n. 5, 2017, pp. 616 ss.; U. Ruffolo – E. Al Mureden, Autonomous vehicles *e responsabilità nel nostro sistema ed in quello statunitense*, in *Giur. it.*, n. 7, 2019, pp. 1704 ss.; 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 ss. (Parte II); e in ambito penale a A. Cappellini, *Profili penalistici delle* self-driving cars, in *Dir. pen. cont.* (*archiviodpc.dirittopenaleuomo.org*), n. 2, 2019, pp. 325 ss.

56 È il caso dell'episodio raccontato da R. Barlaam, *Incidente mortale, Uber sospende test su guida autonoma*, in *Il Sole 24 ore*, 20 marzo 2018, p. 34. Si tratta cronologicamente del terzo sinistro, avvenuto a Tempe in Arizona (USA) il 18 marzo 2018, nel quale ha perso la vita non il conducente ma un pedone. Il primo incidente risale al 20 gennaio 2016 ad Handan (Cina) provocando la morte del conducente; il secondo a Williston in Arizona (USA) il 7 maggio 2016, quando una vettura Tesla modello S si è infilata sotto ad un camion bianco, non riuscendo a distinguerlo dal cielo luminoso, provocando la distruzione dell'automobile e la morte del conducente. Un ultimo incidente è avvenuto a Mountain View in California (USA) cagionando la morte del conducente.

57 Secondo una parte della dottrina la circolazione delle *self driving cars* evoca scenari utopici (e forse distopici), i quali sono prefigurati da 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, e solleva altresì questioni di natura puramente etica, incisivamente descritti con l'espressione del c.d. "*trolley problem*", da parte di Y. Hu, *Robot Criminals*, in *Univ. Mich. Journal of Law Reform*, Vol. 52, n. 2, 2019, p. 496, con riferimento alle *self driving cars*, interrogandosi sulla seguente questione: «*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?*». Verosimilmente però queste situazioni accomunano sia le *self driving cars* sia l'uomo in quanto la concitazione della guida non sembra consentire di esprimere sempre la decisione "giusta" (o meno censurabile moralmente) sia da parte del conducente più esperto sia da parte della autonomous car più addestrata possibile. In tale senso 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.

58 Si veda U. Ruffolo, *L'intelligenza artificiale in sanità: dispositivi medici, responsabilità e "potenziamento"*, in *Giur. it.*, n. 2, 2021, pp. 502 ss., spec. pp. 502, 507, secondo il quale uno dei primi settori nei quali l'attività umana sarà presto soppiantata dai sistemi di AI è quello della radiologia, ormai più precisa dell'uomo nell'esaminare una grande quantità di informazioni e nell'elaborare una diagnosi, non necessariamente corretta in quanto l'algoritmo (oltre che opaco, poco trasparente e quindi non immediatamente verificabile), sviluppa outputs basati su mere correlazioni statistiche e non per inferenza logica. L'A. comunque ipotizza una responsabilità a carico del programmatore del sistema per non avere previsto meccanismi interni volti ad inibire ogni evoluzione comportante eventi lesivi. Sulle applicazioni e sull'individuazione di alcuni limiti dell'intelligenza artificiale in ambito sanitario si rinvia a G. Pasceri, *Intelligenza artificiale, algoritmo e* machine learning, cit., pp. 45-50, e 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 octuber 2019, Vol. 366, Issue 6464, pp. 447 ss., ove si riporta il caso dell'utilizzazione di un algoritmo (sistema *Optum* della *United Health Group*) per individuare i pazienti con esigenze sanitarie complesse che produce effetti discriminatori sulla base del colore della pelle con conseguente sovrastima dei costi della parte di popolazione pregiudicata.

Altri recenti casi hanno dimostrato la pericolosità degli assistenti vocali basati sull'AI[59]: questi meccanismi (cc.dd. *social bot*), infatti, talvolta acquisiscono informazioni *on line* e selezionano le risposte agli utenti sulla base di criteri di natura computazionale, ripetendo eventualmente errori e pregiudizi diffusi nello spazio sociale[60].

Come detto, il differente grado di autonomia del sistema di AI ha riflessi sul tema dell'imputazione della responsabilità. Mentre per i sistemi di AI deboli possono essere adattate le regole giuridiche in vigore con imputazione della responsabilità all'uomo, per i sistemi di AI forti risulta più difficile imputare e poi distribuire la responsabilità in capo al produttore, al programmatore o all'utente.

3.1 I sistemi di AI istruiti all'illecito

È pacifico che il reato è imputabile direttamente all'uomo quando l'intelligenza artificiale è utilizzata come strumento per la sua consumazione mediante una serie di istruzioni[61] da colui che, impartendole, l'abbia determinato a commettere materialmente l'illecito[62]: si pensi alle truffe finanziarie di c.d. *phishing* di *mail* o di messaggi telefonici, effettuati mediante *software agent* che riproducono in maniera massiva tentativi di estorcere ai clienti *password* di accesso alle pagine personali, incluse quelle dell'*internet banking*.

Si può aggiungere che, in presenza di un *input* umano alla commissione di un illecito, il compimento di un evento diverso (ma pur sempre illecito) da quello ideato per una deviazione imprevedibile dell'agente artificiale non recide il collegamento causale e l'imputazione all'uomo ma si risolve, tutt'al più, in una mera *aberratio causae* che non fa venire meno l'imputabilità dell'evento all'agente umano[63]. Ugualmente,

59 Si può ricordare il caso dell'applicazione di *Amazon*, *Alexa*, che, in risposta alla richiesta di una *challenge*, ha invitato una bambina di dieci anni a inserire un caricabatterie del telefono a metà in una presa di corrente e toccare i poli opposti con una moneta. Dopo l'incidente Amazon ha aggiornato il *software* per evitare la ripetizione di analoghe sfide pericolose. Si veda *Amazon nei guai, la sfida di Alexa alla bimba. «Inserisci una moneta nella presa elettrica»*, in *il Giornale*, 29 dicembre 2021, p. 15. Un altro caso riguarda la *chatbot TAY* (*Thinking About You*) che, dopo solo un giorno dalla sua attivazione, è stata bloccata per avere diffuso sulle piattaforme digitali di comunicazione messaggi razzisti, sessisti e xenofobi, amplificando gli effetti delle informazioni che l'applicazione aveva acquisito sulla rete. Su questo episodio L. BENFATTO, *Microsoft blocca il* software Tay*: era diventato razzista e xenofobo*, in *Il Sole 24 ore Tecnologia*, 25 marzo 2016.

60 In questo senso l'articolo *L'intelligence artificielle reproduit nos préjugés*, in *Le Monde*, 18 aprile 2017, pp. 1, 28, ma anche in dottrina A. CARCATERRA, *Macchine autonome e decisione robotica*, in A. CARLEO (a cura di), *Decisione robotica*, Bologna, 2019, pp. 38 ss., il quale ricorda che tale effetto è stato definito dai *data scientist* come '*GIGO*', ovvero "*garbage in garbage out*".

61 Si rinvia a F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo* (*dirittopenaleuomo.org*), n. 10, 2019, in part. pp. 24 ss., il quale cita quali casi esemplificativi di utilizzazione dei sistemi di intelligenza artificiale per la commissione di reati il c.d. bagarinaggio *on line* e le condotte di manipolazione abusiva del mercato.

62 Si veda A. CAPPELLINI, *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale*, in *disCrimen* (*discrimen.it*), 27 marzo 2019, pp. 7-8.

63 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, con riguardo alle negoziazioni algoritmiche in ambito finanziario, ha rilevato in situazioni analoghe un difetto del dolo in quanto non vi è una completa e perfetta sovrapposizione delle modalità concrete di manifestazione del fatto compiuto dall'algoritmo.

qualora la deviazione imprevedibile dell'algoritmo non conduca alla commissione di un illecito non potrà escludersi una imputazione all'uomo del tentativo[64].

Algoritmi istruiti a delinquere potrebbero essere utilizzati anche in ambito finanziario da parte di *traders* che sfruttano il vantaggio competitivo della velocità di computazione, rispetto alle strategie di *trading* basate su sole cognizioni umane che, per quanto sofisticate, non potranno mai colmare il *gap* tecnologico e, quindi, informativo di coloro che si servono di sistemi di AI[65].

3.2 I sistemi di AI autori dell'illecito

La consumazione del reato può non provenire da un proposito umano ma essere conseguenza di comportamenti autonomi ed imprevedibili dell'agente artificiale (il riferimento è ovviamente ai sistemi di AI forti) quando non sono stati predisposti meccanismi inibitori che identifichino soglie di comportamento non valicabili[66].

64 A. CAPPELLINI, Machina delinquere non potest*? Brevi appunti su intelligenza artificiale e responsabilità penale*, cit., p. 8.

65 Si rinvia a G. RUTA, *I.A. nei reati economici e finanziari*, cit. pp. 67-70, che fornisce una casistica di tre casi nella giurisdizione inglese e americana. Oltre al caso *Coscia* su cui infra, ricorda il caso *Da Vinci Invest Limited* e *Paul Axel Walter*, i quali costituiscono – secondo l'Autore – una rappresentazione esemplificativa di realizzazione di fattispecie di *market abuse* mediante l'interazione di uomo e macchina, consistente nell'adozione del meccanismo massivo di ordini, tipico dell'*high frequency trading*.

66 Non rientrano in questo ambito gli illeciti causati da un errore di fabbricazione, programmazione, addestramento o sorveglianza o, più specificatamente, da un deficit informativo o da un inadeguato addestramento. Su questa distinzione da C. PIERGALLINI, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato*, cit., p. 1752, che distingue i «difetti di costruzione», i «difetti di progettazione», i «difetti di informazione» e i «difetti da rischio di sviluppo». A ciascuno di questi difetti corrisponde un preciso rischio ma, salvo quello da sviluppo su cui infra, come puntualizza B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, cit., p. 334, non si tratta di un rischio insito nell'autonomo funzionamento dei sistemi di AI ma «di un rischio creato, attualizzato e gestito da quei soggetti che programmano, commercializzano o impiegano il sistema intelligente». Sulla necessità di un *dataset* informato si veda C. DA ROLD, *Quando gli algoritmi sbagliano spesso sono solo disinformati*, in *Il Sole 24 ore*, 18 settembre 2022, p. 14. In queste situazioni non dovrebbero condurre a ripensare le categorie giuridiche vigenti ma piuttosto a promuovere un certo adattamento di quelle esistenti per i nuovi "prodotti" dotati di una maggiore libertà di azione rispetto al passato. In particolare, nelle fattispecie descritte l'evento del sistema di AI potrebbe essere ascrivibile a titolo colposo a produttore, programmatore, *trainer* o utente. Ovviamente, la giustificazione del rimprovero dovrebbe essere diversamente declinata: presumibilmente in caso di algoritmi male informati o male addestrati, come qualora vi sia stato un difetto di produzione o di programmazione, potrebbe essere stato violato un obbligo di perizia; in caso di sistemi di AI non controllati potrebbe essere stato violato un obbligo di sorveglianza e, quindi, di diligenza. Si tratta di ipotesi nelle quali sarebbe possibile ricostruire il rimprovero in termini di mancato impedimento colposo dell'evento da parte dell'operatore (i.e. produttore, programmatore, trainer o utente), previa definizione di un criterio di perizia o diligenza esigibile, commisurata al rischio secondo una normazione settoriale. Così 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, secondo il quale l'attribuzione del fatto illecito potrebbe trovare una giustificazione nella disposizione dell'art. 40, comma 2, c.p. Assumeranno, di conseguenza, maggiore rilevanza gli addebiti di natura omissiva in quanto l'agente umano sarà coinvolto solo indirettamente nel processo decisionale. Il tutto determinerà un maggiore coinvolgimento e una responsabilizzazione degli agenti umani in tutte le fasi di vita del sistema di AI, come già prefigura la proposta di Regolamento (UE) sull'intelligenza artificiale. Con riferimento ai sistemi di AI ad alto rischio, il Capo II del Titolo III della proposta di Regolamento (UE) sull'intelligenza artificiale stabilisce che, prima di essere immessi sul mercato, devono osservare le seguenti condizioni: istituire e realizzare un sistema di gestione dei rischi; predisporre una governance e gestione dei dati per i sistemi di AI che prevedono l'uso di dati; redigere la documentazione tecnica prima dell'immissione sul mercato o della messa in servizio; progettare e sviluppare i sistemi mediante registrazione automatica degli eventi durante il loro funzionamento; progettare e sviluppare i sistemi in modo da assicurare adeguata trasparenza, consentendo agli utenti di interpretare gli output e di ricevere istruzioni per l'uso; garantire la supervisione e il monitoraggio durante l'utilizzazione in modo tale da prevenire e ridurre rischi per salute, sicurezza e diritti fondamentali; garantire accuratezza, robustezza e cybersicurezza dei sistemi in modo da evitare errori, guasti o

Una parte della dottrina ha proposto di attribuire (o riconoscere) uno status giuridico a questi sistemi di AI, onde poterne configurare una responsabilità per gli illeciti da loro materialmente commessi[67], in uno con l'individuazione degli elementi (*actus reus* e *mens rea*)[68] e delle ragioni[69] di tale imputabilità.

Financo i più risalenti interventi delle istituzioni UE (finora limitati a fonti di *soft law*), come la Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), avevano implicitamente prospettato l'istituzione di una soggettività giuridica piena per i sistemi di AI forti, con la specifica finalità di consentire la creazione di un centro di imputazione di responsabilità dei danni cagionati dai medesimi[70], ma

incongruenze. Si tratta di obblighi a carico del fornitore del sistema di AI, ai quali si sommano i seguenti: istituire un sistema di gestione della qualità che garantisca la conformità al Regolamento; sottoporre il sistema alla procedura di valutazione di conformità, prevista dall' art. 43 prima dell'immissione sul mercato o messa in servizio; redigere una dichiarazione di conformità se il sistema è conforme e apporre la marcatura CE; conservare i log generati automaticamente; registrare il sistema nella banca dati UE prima dell'immissione sul mercato. Altrettanti obblighi sono previsti per gli utenti: utilizzare e monitorare il sistema conformemente alle istruzioni per l'uso elaborate dal fornitore; organizzare risorse e attività per attuare le misure di sorveglianza umana indicate dal fornitore; informare il fornitore o il distributore qualora abbiano individuato un incidente grave o un malfunzionamento e interrompere l'uso del sistema; assicurare il rispetto degli obblighi normativi esistenti se rilevanti (ad esempio, direttiva *CRD4* per gli enti creditizi, Regolamento *GDPR* in caso di informazioni fornite *ex* art. 13).

67 In questo senso G. Teubner, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi* (trad. it. a cura di 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, i quali postulano il riconoscimento di una capacità giuridica parziale, ovvero la capacità di essere rappresentante, in quanto assumono decisioni autonome e per ciò stesso possono causare conseguenze in punto di responsabilità. A favore del riconoscimento di una personalità giuridica elettronica nella letteratura italiana U. Ruffolo, *La "personalità elettronica"*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, pp. 213 ss., e nella letteratura di *common law* L.B. Solum, *Legal Personood for Artificial Intelligences*, in *North Carolina L. Rev.*, Vol. 70, n. 4, 1994, pp. 1231 ss.

68 Con riferimento a questo modello di responsabilità si veda G. Hallevy, *The Basic Models of Criminal Liability of AI Systems and Outer Circles*, (June 11, 2019), su SSRN: https://ssrn.com/abstract=3402527 or http://dx.doi.org/10.2139/ssrn.3402527, il quale stabilisce un'analogia tra la capacità dei sistemi di AI e la capacità delle persone incapaci (*i.e.* minori di età), alla quale non può essere imputata la commissione di illeciti penali. In queste ipotesi, pur potendo essere integrato l'elemento materiale del reato (*actus reus*) da parte di un sistema di AI, manca comunque l'elemento soggettivo (*mens rea*) per l'attribuzione della responsabilità all'intelligenza artificiale che viene qualificata come «*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*». Nello stesso senso del medesimo A., *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 ss. In altre due ipotesi l'A. prefigura la possibilità di individuare una responsabilità del sistema di AI: nella prima individua una responsabilità solidale di uomo e AI qualora al programmatore o all'utilizzatore sia imputabile un addebito colposo; nella seconda una responsabilità esclusiva dell'AI qualora sia reciso il collegamento con il programmatore o l'utilizzatore. Per alcune obiezioni a questo orientamento si veda R. Borsari, *Intelligenza artificiale e responsabilità penale: prime considerazioni*, in *Rivista di diritto dei media* (*medialaws.eu*), n. 3, 2019, pp. 267-268.

69 Y. Hu, *Robot Criminals*, cit., *passim*, individua un triplice ordine di ragioni per considerare i sistemi di AI responsabili penalmente: in primo luogo, l'algoritmo alla base del sistema di AI sia dotato di algoritmi in grado di assumere decisioni moralmente rilevanti; in secondo luogo, l'algoritmo sia capace di comunicare le sue decisioni agli uomini; infine, l'algoritmo sia autorizzato ad agire senza la supervisione umana.

70 Si veda il § 59, lett. f), della Risoluzione del Parlamento UE del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, cit., ove tra le soluzioni giuridiche possibili da adottare nel futuro, si valuta «l'istituzione di uno status giuridico specifico per i robot nel lungo termine, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi».

lasciando irrisolta una doppia questione: (i) la difficoltà di muovere un giudizio di rimproverabilità nei confronti delle "macchine"[71], (ii) la definizione delle modalità di riparazione e punizione dei pregiudizi causati dai comportamenti degli agenti artificiali[72]. Ed invero, la prospettiva di considerare l'AI un autonomo centro d'imputazione giuridica è stata criticata ampiamente, non soltanto dalla migliore dottrina[73], ma anche dalle stesse istituzioni dell'UE. Il Comitato economico e sociale europeo, nel parere su «L'intelligenza artificiale — Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società», (2017/C 288/01), del 22 settembre 2016, ha dichiarato che attribuire personalità giuridica ai robot «comporterebbe un rischio inaccettabile di azzardo morale» in quanto eliminerebbe la funzione di prevenzione propria del regime della responsabilità[74]. Il Gruppo di esperti sull'intelligenza artificiale istituito dalla Commissione europea nel giugno 2018, nel *Report on Liability for Artificial Intelligence and other emerging digital technologies*, ha ribadito che «*there is currently no need to give a 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*

71 Su questo punto si rinvia alle notazioni critiche di M.B. Magro, *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, cit., pp. 9-10, ove si sottolinea la difficoltà di individuare il requisito della colpevolezza in quanto l'AI non è in grado di percepire e comprendere l'antigiuridicità della condotta. Nel medesimo senso 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 ss.; 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. Nella letteratura anglosassone si veda 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 ss., spec. p. 181, che esclude l'applicazione della responsabilità penale in quanto gli agenti artificiali non sono dotati di capacità morale.

72 Come sostiene infatti U. Ruffolo, *Intelligenza artificiale*, machine learning*, responsabilità da algoritmo*, cit., pp. 1702-1703, perché l'AI sia responsabile e abbia risorse patrimoniali per riparare un danno non è necessario attribuire ad essa personalità giuridica.

73 In dottrina si ritiene che l'evoluzione tecnologica non abbia raggiunto uno stadio tale da accordare uno status giuridico ai sistemi di AI. In questo senso E. Palmerini, *Soggettività e agenti artificiali: una soluzione in cerca di un problema*, in *Oss. dir. civ. comm.*, n. 2, 2020, pp. 445 ss. In senso sostanzialmente conforme G. Bevivino, *Situazioni giuridiche "soggettive" e forme di tutela delle intelligenze artificiali*, in *Nuova giur. civ. comm.*, n. 4, 2022, pp. 899 ss., spec. p. 907, ma non esclude che in futuro vi sia l'esigenza di regolamentare forme di responsabilità diretta qualora i sistemi di AI raggiungano meccanismi di funzionamento del tutto sovrapponibili a quelli dell'uomo. Contrario alla creazione di sistemi di AI si veda 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, il quale ritiene che nelle pieghe dell'ordinamento possa rinvenirsi un divieto di creare sistemi di AI che abbiano anche capacità umana. Il dato normativo viene individuato nell'art. 13 della Legge n. 40 del 2004, che prevede un divieto generale di produrre ibridi e chimere, ritenuto dall'A. in grado di comprendere anche "robot umanizzati". Se si vuole estendere l'analisi poi sul piano della responsabilità civile si veda in senso critico U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, cit., pp. 1250-1251, secondo il quale la prospettiva di una soggettività giuridica, collegata alla creazione di un patrimonio o di un fondo assicurativo, costituirebbe soltanto un espediente per imputare la responsabilità a una pluralità di imprenditori e utenti. Si veda altresì E. Bocchini, *Contro la "soggettivizzazione" dell'intelligenza artificiale*, in *Il Nuovo Dir. So*c., n. 2, 2023, pp. 195 ss.

74 Parere del Comitato economico e sociale europeo su «*L'intelligenza artificiale — Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società*», (2017/C 288/01), 22 settembre 2016. In questi termini L. Coppini, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Pol. dir.*, n. 4, 2018, p. 730.

a new category of legal person»[75]. Anche il Parlamento europeo, in una successiva Risoluzione del 20 ottobre 2020, ha reputato non necessario conferire personalità giuridica ai sistemi di AI poiché in tutte le attività vi è comunque un apporto umano[76]. A ciò si aggiunge che una sanzione penale nei confronti dei sistemi di AI non sarebbe in grado di svolgere alcuna delle funzioni riconosciute alla pena, ovvero quella retributiva, rieducativa e preventiva. In primo luogo, la sanzione non potrebbe svolgere alcuna funzione retributiva in quanto ai sistemi di AI non è possibile muovere alcun rimprovero: l'intelligenza artificiale è sprovvista del libero arbitrio[77]. In secondo luogo, la finalità rieducativa non potrebbe essere perseguita: l'ipotetica previsione della distruzione o della disattivazione del sistema di AI finirebbe per ricadere sempre sul proprietario o sull'utente[78], senza contare che entrambe queste "pene" potrebbero essere comunque scongiurate da una riprogrammazione della "macchina"[79]. Infine, la sanzione non sarebbe idonea a comunicare il disvalore sociale del comportamento antigiuridico agli altri sistemi di AI in quanto insensibili ai precetti penali perché artificiali e, come tali, correggibili mediante una mera riprogrammazione[80].

Un altro orientamento dottrinale, all'opposto, suggerisce di imputare l'illecito pur sempre all'uomo, marginalizzando la dimensione soggettiva della colpa ed estendendo i confini della prevedibilità e della evitabilità dell'evento sino a configurare un modello di responsabilità quasi "oggettivo", ricostruito sulla base di una prevedibilità astratta, coincidente con l'assunzione di un rischio, pur in mancanza della violazione di regole di condotta di uno qualsiasi degli operatori coinvolti nel processo di produzione e programmazione, ovvero solo per avere volutamente messo in funzione un sistema di AI dal comportamento imprevedibile[81]. Non vi è dubbio che quest'ultima ricostruzione contrasta col consolidato principio di imputazione personale della

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

76 Si veda il § 7 della Risoluzione del Parlamento UE del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, cit.

77 In questo senso 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. Sulla capacità degli algoritmi di condizionare le decisioni dell'uomo si veda M. Abriani, *Gli algoritmi minacciano il libero arbitrio?*, in *MichePost*, 16 maggio 2020, mentre sulla necessità di una predisposizione etica degli algoritmi si vedano A. Celotto, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi giur. econ.*, n. 1, 2019, p. 59, e 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.

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

79 Si veda V.C. Talamo, *Sistemi di intelligenza artificiale: quali scenari in sede di accertamento della responsabilità penale?*, in *ilPenalista*, 3 luglio 2020, pp. 5-6, che esclude la possibilità di configurare una responsabilità penale degli agenti artificiale non soltanto per la mancanza del requisito della colpevolezza ma altresì per l'impossibilità di alcuna funzione rieducativa e risocializzante della pena. Possibilista sul raggiungimento delle funzioni della pena F. Basile, *Diritto penale e intelligenza artificiale*, cit., pp. 73-74, limitatamente a quella retributiva e special-preventiva, mentre manifesta perplessità di un effetto general-preventivo nei confronti delle "entità" artificiali.

80 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.

81 M.B. Magro, *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, cit., pp. 19-20.

responsabilità penale; vero è d'altronde che essa ha il pregio di incentivare un atteggiamento di cautela da parte di produttori, programmatori e utilizzatori, forse a discapito dell'illimitata evoluzione tecnologica dell'AI.

Vi è infine un terzo scenario, non meno problematico dei due precedenti: l'accettazione di un rischio "normale" nell'utilizzazione dei sistemi di AI equiparabile al rischio ambientale oppure al caso fortuito e alla forza maggiore (artt. 45-46 c.p.), come tale imponderabile ma distribuito e condiviso su tutta la collettività[82]. A ben vedere, si tratta della consapevole accettazione dell'accennato *responsibility gap*, nell'ottica di una valutazione comparativa di benefici e costi che considera prioritario lo sviluppo tecnologico e recessive le esigenze di tutela dell'individuo ma fatti salvi alcuni limitati divieti per le ipotesi di rischio del tutto inaccettabile[83].

4 *Trading*, abusi di mercato e AI: uno sguardo d'insieme

I sistemi di AI consentono di acquisire e processare una gran mole di informazioni e di elaborare nuove strategie di mercato in pochi millesimi di secondo. Ciò è dovuto a due caratteristiche principali del funzionamento di alcuni degli algoritmi di negoziazione algoritmica: l'arbitraggio statistico e l'arbitraggio di latenza. L'analisi economica ha evidenziato come gli arbitraggi siano centrali per il funzionamento dei mercati: essi consentono, da un lato, guadagni a rischio (quasi) nullo per gli operatori che li sanno implementare e, di converso, offrono benefici per la collettività degli investitori, che si può giovare, così, di prezzi che rimangono coerenti con l'insieme delle informazioni pubblicamente disponibili.

Tutte le modalità di *trading* algoritmico, compresa la negoziazione algoritmica (c.d. *algorithmic trading*) e la negoziazione algoritmica ad alta frequenza (c.d. *high frequency trading*), dischiudono nuove vulnerabilità e scenari inediti di consumazione degli illeciti di abuso di mercato[84]. Il pericolo diffuso acquisisce un'evidente consistenza se si ha riguardo ai beni che l'ordinamento intende salvaguardare con la predisposizione di un organico apparato normativo sanzionatorio, che dovrebbe necessariamente essere aggiornato con misure proporzionate a queste forme di negoziazione.

82 Prospetta questo scenario in ambito penale M.B. Magro, *Robot, cyborg e intelligenze artificiali*, in A. Cadoppi – S. Canestrari – A. Manna – M. Papa, *Cybercrime*, Torino, 2019, pp. 1180 ss., spec. p. 1211, ma apre le porte a ipotesi di responsabilità civile di natura oggettiva qualora non vi fosse alcuna colpa di operatore, programmatore o venditore.

83 In questo senso la proposta di Regolamento (UE) sull'intelligenza artificiale già individua alcune pratiche inaccettabili di intelligenza artificiale. In particolare, l'art. 5, par. 1, della proposta di Regolamento (UE) sull'intelligenza artificiale vieta le seguenti pratiche di intelligenza artificiale: i sistemi di AI che utilizzano tecniche subliminali (lett. a); i sistemi di AI che sfruttano la vulnerabilità di alcuni soggetti (lett. b); i sistemi di AI utilizzati per valutare l'affidabilità delle persone (lett. c); i sistemi di AI di identificazione biometrica in tempo reale in spazi aperti al pubblico (lett. d). L'art. 71 della proposta di Regolamento (UE) stabilisce per l'inosservanza del divieto di pratiche illecite la sanzioni amministrative pecuniaria fino ad euro 30.000.000 o, se l'autore del reato è una società, fino al 6% del fatturato mondiale totale annuo dell'esercizio precedente. Le medesime sanzioni sono previste anche per la violazione delle regole in tema di dati e governance dei dati dei sistemi di AI ad alto rischio.

84 In questo senso 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 ss., spec. pp. 265 e 271.

Le molteplici teorie che giustificano l'introduzione di divieti di abuso di mercato sono accomunate dalla finalità di assicurare il corretto ed ordinato funzionamento degli scambi inerenti a strumenti finanziari. Mediante la proibizione di abusi di informazioni privilegiate (o *insider trading*), infatti, l'ordinamento giuridico intende evitare che il rischio che la controparte esegua un contratto sulla base di informazioni non pubbliche disincentivi i *market maker* dal ridurre, nella loro competizione reciproca il *bid ask spread*, ovvero i costi di transazione per la generalità degli investitori[85], e dissuada gli investitori istituzionali dal prendere posizioni contrarie ai *trend* in atto che

85 Nell'analisi economica tradizionale i *market maker* assumono un ruolo cruciale per il funzionamento dei mercati in quanto sono gli intermediari che offrono liquidità agli altri partecipanti al mercato grazie alle proposte di acquisto (*bid*) e di vendita (*ask*) che espongono in via continuativa su un dato strumento finanziario. Tipicamente, i profitti attesi dei *market maker* crescono al crescere della frequenza degli scambi, che quindi consente a ciascuno di ridurre la differenza tra la migliore proposta offerta in acquisto e la migliore proposta offerta in vendita. La competizione tra *market maker* su un medesimo strumento finanziario porta, a parità di altre condizioni, ad una riduzione della migliore proposta in acquisto offerta nel complesso da tutti i *market maker* (*bid-ask spread*). Ciò va a vantaggio degli altri partecipanti al mercato che, invece, vedono il *bid-ask spread* come il costo di transazione che devono sostenere per effettuare i loro investimenti. Pertanto, l'analisi economica presta molta attenzione alle scelte di *policy* e alle regole di funzionamento dei mercati che favoriscono la riduzione del *bid-ask spread* da parte dei *market maker*. In particolare, è esaminato il ruolo svolto dai *market maker* nel processo di formazione dei prezzi ovvero nel processo di *price discovery*, che consente ai prezzi di incorporare e riflettere le informazioni che i partecipanti al mercato forniscono implicitamente a tutti gli altri partecipanti al mercato con i loro ordini di acquisto e di vendita. Alla domanda se sia bene introdurre un divieto di *insider trading* gli economisti hanno fornito risposte contrastanti sulla base di diverse teorie. La più importante teoria che è contraria all'introduzione del divieto fa leva sull'efficienza informativa dei mercati, ovvero sulla misura in cui i prezzi sono in grado di rappresentare il valore sottostante del bene cioè il suo valore intrinseco o fondamentale. In particolare, la classica ripartizione proposta dal premio Nobel Eugene Fama è tra efficienza informativa debole, semi-forte e forte a seconda che i prezzi riescano ad incorporare ed esprimere le informazioni che sarebbe in alternativa possibile ricavare dalla conoscenza, rispettivamente, dei prezzi passati, di tutte le informazioni già pubblicate e di tutte le informazioni non pubblicate (cioè private). È quindi evidente che se in un mercato è proibito agli *insider* di operare, in quanto dispongono per definizione di informazioni private, allora in tale mercato i prezzi non potrebbero mai raggiungere una efficienza forte, ma, al più, semi-forte. Si aggiunge che l'efficienza informativa dei mercati è a sua volta funzionale all'efficienza allocativa delle risorse. Quanto più, infatti, i prezzi riescono ad esprimere i valori fondamentali degli strumenti finanziari e tanto più facile sarà per la "mano invisibile" teorizzata da Adam Smith di portare fisiologicamente le risorse di una economia verso gli investimenti che più sono meritevoli delle stesse. Di contro, varie teorie sulla microstruttura dei mercati hanno dimostrato come i *market maker* sono significativamente danneggiati dall'eventuale presenza di insider sul mercato. Se infatti il *market maker* offre liquidità ad un insider che è a conoscenza di una informazione privilegiata che sta per essere pubblicata, allora il *market maker* che non riesca a chiudere prima della pubblicazione dell'informazione la posizione che ha aperto per offrire liquidità all'insider subirà, al momento della pubblicazione, una perdita pari alla differenza tra il nuovo prezzo di mercato e quello al quale aveva offerto liquidità all'*insider*. Essendo consapevoli di tale rischio, allora i *market maker* allargano il *bid-ask spread*, cioè impongono agli altri partecipanti al mercato un più alto costo di transazione, in modo da compensare le perdite derivanti da tale possibile evenienza sfavorevole. Peraltro, poiché i *market maker* non riescono a riconoscere gli strumenti finanziari e i periodi in cui gli insider possono presentarsi come controparti, allora essi allargano i via sistematica il *bid-ask spread*. A cascata, occorre anche tenere presente che più ampi *bid-ask spread* allontanano dal mercato quei partecipanti che, al margine, non riescono a sostenere tale costo di transazione e questo, a sua volta, riduce la frequenza degli scambi e quindi sia i profitti attesi dai *market maker* sia l'efficienza informativa dei prezzi, che non possono più incorporare le informazioni che tali partecipanti apportano con i loro ordini sul mercato. Sull'efficienza informativa dei mercati: 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. Sui principali modelli che esaminano l'influenza dell'operatività degli *insider* sul processo di formazione dei prezzi si vedano: 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. Su altre teorie favorevoli o contrarie all'introduzione di un divieto di *insider trading*: 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. Sulle evidenze empiriche: U. Bhattacharya – D. Hazem, *The world price of*

non risultino coerenti con l'insieme delle informazioni pubblicamente disponibili[86].

È questo un approccio che si oppone alla visione di una parte della dottrina secondo la quale l'indiscriminato utilizzo di informazioni privilegiate consentirebbe ai prezzi che si formano nei mercati di convergere più rapidamente verso i *fundamentals*. Il rallentamento del processo di *price discovery* introdotto dal divieto di abuso è quindi accompagnato nei vari ordinamenti dall'introduzione di obblighi informativi per gli emittenti. Emblematicamente, nella UE gli obblighi per gli emittenti partono proprio dal momento in cui le informazioni assumono natura privilegiata, cioè dal momento in cui sono pronte per essere sfruttate con profitto dagli *insiders* (art. 17, par. 1, Regolamento (UE) *MAR*).

Mediante il divieto di manipolazione del mercato, d'altronde, l'ordinamento giuridico intende parimenti scongiurare che informazioni false o fuorvianti non solo rallentino il processo di convergenza verso i *fundamentals* ma addirittura lo impediscano[87]. È, pertanto, sanzionata la diffusione di informazioni false da parte di quanti abbiano capacità con le proprie affermazioni o omissioni di influire sui prezzi di mercato. E poiché questi ultimi non sono soltanto il risultato dell'interazione tra domanda e offerta ma costituiscono, a loro volta, informazioni – lette, esaminate e valutate dalle varie tipologie di operatori – è parimenti sanzionato il conferimento di ordini o l'esecuzione di operazioni che alterino il processo di formazione dei prezzi e li allontani dai *fundamentals*, creando quindi prezzi artificiali, ovvero un quadro informativo distorto.

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.

86 Se, infatti, gli *insider* spostano in anticipo I prezzi dal loro valore coerente con l'insieme delle informazioni pubblicamente disponibili, come rilevabile dagli studi prodotti da agenzie di *rating* e analisti finanziari, allora gli investitori istituzionali (fondi pensione, fondi speculativi, ecc.) potrebbero essere indotti a prendere importanti posizioni che puntino sul riallineamento dei prezzi correnti verso quelli coerenti con l'insieme delle informazioni pubblicamente disponibili. Quando tuttavia l'informazione privilegiata è resa pubblica, tali investitori rimangono sorpresi e subiscono perdite che altrimenti non avrebbero subito. Anticipando, tale scenario avverso, gli investitori istituzionali non sarebbero incentivati a domandare agli analisti finanziari ricerche sofisticate sul valore dei prezzi coerente con l'insieme delle informazioni pubblicamente disponibili. A cascata, la riduzione della domanda porta a una minore produzione di ricerche e quindi ad una maggiore erraticità dei prezzi, che quindi risulterebbero meno efficienti: 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.

87 Il pericolo immanente alle negoziazioni ad alta frequenza è stato condiviso dal legislatore UE. Il Considerando 38 del Regolamento (UE) n. 596/2014 (c.d. *MAR*, acronimo di *Market Abuse Regulation*), precisa, infatti, che «per rispecchiare il fatto che la negoziazione di strumenti finanziari è sempre più automatizzata, è auspicabile che la definizione di manipolazione del mercato fornisca esempi di strategie abusive specifiche che possono essere effettuate con qualsiasi strumento disponibile di negoziazione, incluse le negoziazioni algoritmiche e quelle ad alta frequenza. Gli esempi forniti non sono da considerare esaustivi e non tendono a suggerire che le stesse strategie attuate con altri mezzi non siano abusive». Per una descrizione delle pratiche più diffuse di abusivisimo a seguito della diffusione dell'high frequency trading si rinvia a V. Caivano – S. Ciccarelli – G. Di Stefano – M. Fratini – G. Gasparri – M. Giliberti – N. Linciano – I. Tarola, *Il Trading ad alta frequenza*, in *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.

In effetti, con l'utilizzazione dei sistemi di AI nella negoziazione finanziaria l'attività di vigilanza è stata resa più complessa per la difficoltà non soltanto di individuare il *software*[88], che ha determinato una certa dinamica di mercato, ma anche di valutare l'operato del medesimo in termini di individuazione delle relative motivazioni sottostanti e, quindi, di liceità o illiceità e attribuire le conseguenti responsabilità[89]. Ciò accade in quanto le soluzioni veicolate dall'intelligenza artificiale favoriscono l'ideazione di nuove condotte incidenti sull'incontro tra domanda ed offerta e sul valore degli strumenti finanziari.

L'intelligenza artificiale, applicata alle transazioni finanziarie, ha quindi una portata "*disruptive*"[90], *à la* Schumpeter, ed è oggetto di questo studio capire in quale misura le attuali fattispecie di *insider trading* e di manipolazione siano in grado di contenere le nuove e differenti declinazioni abusive del fenomeno[91]. Il rischio di un ritardo è, come spesso succede, legato alla difficoltà dell'ordine "giuridico" del mercato[92] di rimanere progressivamente allineato all'evoluzione "economica" di quest'ultimo, con la predisposizione di più innovative regole "proibitive", "attributive" e "conformative" in ossequio ai principi costituzionali in materia economica[93], senza le quali aumentano i rischi di stabilità e di integrità dei mercati finanziari[94].

Invero, la diffusione di sistemi di AI è avvertita con maggiore evidenza nel *trading* piuttosto che nella formazione e circolazione delle informazioni privilegiate.

Innanzitutto, in dottrina, come nella letteratura economico-finanziaria, è dibattuto l'effetto dei *traders* algoritmici sulle grandezze che esprimono la qualità del

88 Sull'opportunità di utilizzare meccanismi di intelligenza artificiale per individuare la diffusione al mercato delle informazioni privilegiate da parte degli emittenti quotati v. 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 ss., spec. p. 2033, che individua nella nuova disposizione di diritto comune dell'art. 2086 c.c. il proprio radicamento, ove si utilizza una formulazione ampia ed elastica di «assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa».

89 In questo senso F. Di Ciommo, Smart contract *e (non-) diritto. Il caso dei mercati finanziari*, in *Nuovo diritto civile*, n. 1, 2019, pp. 283-284.

90 In linea generale sugli effetti dell'intelligenza artificiale sulla regolamentazione giuridica si v. 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 ss.

91 Per una descrizione delle nuove modalità commissive di manipolazioni di mercato mediante algoritmi (in particolare *algorithmic trading* e *high frequency trading*) v. infra. In dottrina delinea i principali schemi manipolativi di *spoofing*, *pinging* e *mass-information* T.C.W. Lin, *The new market manipulation*, in *Emory Law Journal*, Vol. 66, Issue 6, pp. 1252 ss.

92 Su questa espressione si rinvia a N. Irti, *L'ordine giuridico del mercato*, Roma-Bari, 2003, *passim*, spec. pp. 51-54, che analizza la funzione conformatrice del diritto mediante norme "proibitive", ovvero le norme che stabiliscono divieti, norme "attributive", ovvero le norme che conferiscono posizioni a soggetti ed a beni, e norme "conformative", ovvero le norme che disciplinano i negozi dando una propria fisionomia al mercato.

93 Un discorso analogo è stato già fatto da 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 ss., a causa dei risvolti sulla razionalità giuridica del mercato derivanti dalla pandemia e dalle scelte di investimento riconducibili al fenomeno della c.d. "*gamification*".

94 In tale senso 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*.

mercato[95]. Non vi è dubbio che ciascuna operazione algoritmica costituisca un'informazione al pari di ogni altra transazione di mercato; ma si dibatte in dottrina se esse favoriscano o meno una migliore comprensione degli scambi complessivamente considerati[96]. Dal dibattito, sembra, in breve, che l'effetto sia positivo sulla liquidità e sull'efficienza informativa e rimanga dubbio, invece, sulla volatilità e sulla resilienza nelle fasi di *stress* o *crash*[97].

Nella UE, i primi tentativi di regolamentazione, sul lato della prevenzione, riguardano quegli algoritmi che sfruttano la velocità di latenza per limitare la commissione di condotte abusive. In particolare, l'art. 17 della Direttiva 2014/65/UE (*Markets in financial instruments directive*, c.d. *MiFID II*) stabilisce che le imprese di investimento esercitino «controlli dei sistemi e del rischio efficaci e idonei» e «impediscano l'invio di ordini erronei o comunque un funzionamento dei sistemi tale da creare un mercato disordinato o contribuirvi»; l'art. 48 della *MiFID II* prevede l'introduzione nei mercati dei cc.dd. *circuit breakers*, meccanismi presso le sedi di negoziazione per arrestare temporaneamente o vincolare le negoziazioni se si verificano all'improvviso movimenti di prezzo inattesi[98]. Inoltre, sul lato della repressione, sono state ulteriormente definite le pratiche di manipolazione con l'intento di assicurare una più incisiva tutela alla formazione dei prezzi degli strumenti finanziari (v. Cap. II, par. 2).

L'applicazione dei sistemi di AI alle negoziazioni determina in via tendenziale la rottura del collegamento tra operazione finanziaria e persona fisica[99], acuita dalla velocità di esecuzione degli ordini che rendono impraticabile una correzione sugli algoritmi utilizzati[100]. Ma anche una volta individuato il nesso causale tra *input* umano e *output* algoritmico gli illeciti di abuso di mercato richiedono, sul piano della responsabilità penale, quale elemento soggettivo indefettibile una componente intenzionale ravvisabile unicamente quando l'algoritmo sia usato come strumento per la commissione del reato[101]. È il caso di quanto accaduto negli Stati Uniti d'America, là dove

95 Su questa disputa M. Bertani, Trading *algoritmico ad alta frequenza e tutela dello* slow trader, cit., pp. 274-275, il quale aggiunge che, dall'utilizzazione di questi meccanismi che sfruttano il vantaggio di latenza, venga depauperata anche la capacità del mercato di informare gli operatori sul grado di liquidità di uno strumento finanziario a causa della presumibile riduzione dell'effetto in tempi infinitesimali.

96 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, per i quali l'imperscrutabilità dei meccanismi di funzionamento dei sistemi di AI rende incomprensibile il come e il perché di una singola operazione algoritmica.

97 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.

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

99 Si rinvia a F. Consulich, *Il nastro di Mobius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, cit., pp. 195 ss., spec. pp. 207, 218, e M. Palmisano, *L'abuso di mercato nell'era delle nuove tecnologie*, in *Dir. pen. cont.*, n. 2, 2019, pp. 129 ss., spec. p. 133.

100 Secondo G. Strampelli, *L'informazione societaria a quindici anni dal T.U.F.: profili evolutivi e problemi*, cit., pp. 1002-1004, il *gap* informativo tra *traders* algoritmici e gli altri *traders* non può tantomeno essere colmato dalla normativa in materia di *mandatory disclosure* in quanto le condotte operative dei primi sono effetto non dell'abuso di informazioni privilegiata ma del vantaggio tecnologico garantiti dalle infrastrutture utilizzate.

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

Michael Coscia è stato condannato con l'accusa di avere programmato un algoritmo per eseguire un'operazione di «*pump and dump*», consistente nell'inviare simultaneamente ordini piccoli e grandi di acquisto e di vendita per creare illusione della domanda e manipolare la rappresentazione degli scambi in capo agli altri operatori[102].

Qualora non sia possibile individuare una componente soggettiva dolosa in capo al programmatore o all'utilizzatore dell'algoritmo di negoziazione, ciò potrebbe comportare la delimitazione di un'area impunita di illeciti in ambito penale[103]. In tali casi, l'ordine giuridico del mercato sarebbe salvaguardato unicamente dalla responsabilità amministrativa, purché sia comunque possibile muovere un rimprovero colposo alla persona fisica per difetti di fabbricazione e di progettazione o per omessa vigilanza[104].

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

103 Ritengono si assista al «*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

104 A questo riguardo 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 ss., propone alle autorità di regolamentazione del settore di richiedere agli utenti di sistemi di IA di fornire un *feedback* significativo per rilevare potenziali manipolazioni e per creare registrazioni probatorie nel caso in cui vi siano comportamenti di manipolazione dell'agente artificiale.

L'adeguatezza della fattispecie normativa II di abusi di mercato

1 Abuso di informazioni privilegiate e AI

Per quanto sopra espresso sono ormai evidenti i motivi per cui gli ordinamenti hanno risposto ai rischi di abusi di mercato ponendo una pluralità di argini che incidono sia sui soggetti che gestiscono i mercati e le relative piattaforme di negoziazione sia sugli operatori che accedono direttamente agli stessi, in primo luogo gli intermediari, ma anche gli emittenti strumenti finanziari, gli investitori professionali o meno, e financo i soggetti il cui comportamento incide comunque sulla formazione dei prezzi: si pensi ai *media* in ambito economico-finanziario, alle istituzioni che diffondono statistiche, agli analisti che producono ricerche, agli accademici che intervengono sulla stampa e a coloro che, in qualche modo, si porgono sui *social* come "esperti" in materia di investimenti. Infine, diverse disposizioni riguardano gli stessi regolatori.

Se infatti l'obiettivo è tutelare la fiducia nel buon funzionamento del mercato finanziario ovvero la credibilità dello stesso[105], non è soltanto l'azione repressiva degli abusi a poter ridurre significativamente i rischi sopra illustrati[106].

Ogni fattispecie punitiva fa perno sulla delimitazione dell'ambito di applicazione, sulla definizione delle informazioni (privilegiate) che possono essere oggetto di

105 S. SEMINARA, *Il diritto penale del mercato mobiliare*, Torino, 2022, pp. 8 ss.

106 L'art. 16, par. 1, del Regolamento (UE) *MAR* richiede alle società di gestione dei mercati di istituire e mantenere dispositivi, sistemi e procedure volti a prevenire e individuare abusi di mercato. I riferimenti impliciti sono molti, quali, ad esempio, *circuit breakers* che bloccano automaticamente le negoziazioni in caso di variazioni eccessive dei prezzi, la chiusura random delle fasi di negoziazione ad asta, ecc. Inoltre, tali società, al pari degli intermediari e di chiunque operi in modo professionale sui mercati, devono segnalare all'autorità nazionale competente le eventuali operazioni sospette ("STOR") che individuano con appositi sistemi e procedure. Gli artt. 17, 18 e 19 del Regolamento (UE) *MAR* prevedono obblighi per gli emittenti con riguardo alla pubblicazione di informazioni privilegiate, procedure per la gestione della riservatezza, comunicazione al pubblico delle operazioni effettuate dai manager sugli strumenti finanziari emessi. L'art. 20, par. 1, del Regolamento (UE) *MAR* richiede agli analisti finanziari di adeguarsi ad una serie di misure che assicurano la correttezza delle loro valutazioni e di rendere pubblici i conflitti di interessi. L'art. 20, par. 2, del Regolamento *MAR* indica alle istituzioni che diffondono al pubblico statistiche o previsioni che possono avere un impatto significativo sui mercati di pubblicarle in modo corretto e trasparente, quindi non selettivo. L'art. 21 del Regolamento (UE) *MAR* si rivolge anche ai giornalisti e ai media esplicitando che le loro condotte sono valutate, rispetto a ipotesi di manipolazione informativa del mercato o di comunicazione illecita di informazioni privilegiate o di diffusione di raccomandazioni di investimento, tenendo conto delle norme della professione. Diverse norme si applicano anche alle autorità nazionali competenti, specie nel caso, disciplinato dall'art. 13 del Regolamento (UE) *MAR*, in cui intendano autorizzare a livello nazionale una prassi di mercato che possa valere come difesa rispetto ad una manipolazione di tipo informativo.

abuso, sulle condotte poste in essere da soggetti che, naturalmente, sono assai variegati per tipologia e qualità[107].

A tale ultimo riguardo, nel corso dei decenni di sviluppo e applicazione della disciplina sono andate sfumando alcune differenze relative alla qualità dei soggetti: se persone fisiche o giuridiche, se in possesso dell'informazione a motivo dello svolgimento di un'occupazione, una professione, una funzione (*insiders* primari) o, invece, a motivo di altro ancora (*insiders* secondari), se investitori professionali o *retail*, se soggetti vigilati o meno, se società emittenti o persone fisiche. Come sopra illustrato, è invece oggetto di recente analisi, anche di questa ricerca, se norme specifiche debbano essere previste per i sistemi di AI.

1.1 *Criminal insider* e AI

Uno degli scenari più preoccupanti nel contrasto agli abusi di mercato riguarda il caso in cui organizzazioni terroristiche o criminali intervengano sui mercati finanziari sfruttando, eventualmente anche con modalità sofisticate, informazioni attinenti ad attività criminali in corso di preparazione e, tra l'altro, capaci di incidere sui prezzi degli strumenti finanziari. All'indomani degli efferati attentati alle torri gemelle di New York dell'11 settembre 2001, stante le repentine e persistenti riduzioni dei prezzi di molti strumenti finanziari potenzialmente sfruttabili dalle stesse organizzazioni terroristiche che avevano sferrato l'attacco, il Consiglio dell'Unione europea e il Parlamento UE intervennero sulla proposta iniziale della Commissione europea riguardante la *MAD I* (Direttiva 2003/6/CE del 28 gennaio 2003), per estendere esplicitamente il divieto di abuso non soltanto ai *manager* delle società quotate, ma anche alle organizzazioni criminali. La Direttiva *MAD I* (art. 2, par. 2, lett. d) ha infatti ampliato il perimetro degli *insiders* primari a chi possieda informazioni privilegiate "in virtù delle proprie attività criminali". Il Regolamento (UE) *MAR* ha confermato l'impostazione indicando tra gli *insiders* primari chi possieda informazioni privilegiate "per il fatto che è coinvolto in attività criminali"[108].

107 Si rinvia per una descrizione dettagliata dell'evoluzione normativa delle differenti fattispecie di abusi di mercato a F. D'Alessandro, *Market Abuse*, in M. Cera – G. Presti (a cura di), *Il testo unico finanziario*, Vol. II, Bologna, 2020, pp. 2166 ss., e a 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 ss.

108 In particolare, si vedano i Considerando nn. 14 e 17 della *MAD I* che espressamente riconoscevano che «(l)a presente direttiva dà riscontro alle preoccupazioni espresse dagli Stati membri in seguito agli attacchi terroristici dell'11 settembre 2001 per quanto riguarda la lotta al finanziamento delle attività terroristiche» e precisavano che dovrebbe tenersi conto «dei casi in cui la fonte dell'informazione privilegiata non è legata a una professione o a una funzione, ma allo svolgimento di attività criminali». A seguito dell'estensione del perimetro del divieto di utilizzazione di informazione privilegiata a chiunque possiede tali informazioni «in virtù delle proprie attività criminali», il legislatore italiano ampliò il divieto nei confronti di chiunque fosse in possesso di informazioni privilegiate «a motivo della preparazione o esecuzione di attività delittuose» (art. 184, comma 2, TUF). Per un approfondimento si rinvia a M.I. Steinberg, *The Sec and the Securities Industry Respond to September 11*, in *International Lawyer*, Vol. 36, n. 1, 2002, pp. 131 ss. Successivamente con la *MAD II*, l'art. 3, par. 3, lett. d), ha esteso il divieto a chiunque possieda l'informazione privilegiata «in ragione del suo coinvolgimento in attività delittuose». In tale modo, la qualifica di *insider* criminale ed il possesso dell'informazione privilegiata non derivano più unicamente dal compimento di un'attività delittuosa ma, altresì, dall'ipotesi in cui l'*insider* concorra nel reato commesso da altri.

Il dato letterale mostra che la persona ricade tra gli *insiders* primari anche se l'informazione di cui entra in possesso non è quella oggetto della propria attività criminale, come sarebbe stato nel menzionato caso di terrorismo, ma quella prodotta da altri soggetti, eventualmente dall'emittente stesso. Per esempio, chi ruba un documento in cui è riportato un evento societario importante che è prossimo alla pubblicazione assume lo *status* di soggetto attivo del reato sebbene egli non abbia preso parte alla formazione di quell'accadimento o comunque non ne sia stato informato "nell'esercizio di un'occupazione, una professione o una funzione".

La sostanziale equiparazione operata già dalla Direttiva *MAD I* (e, in Italia, più recentemente, sul versante penale dalla L. 23 dicembre 2021, n. 238, che ha novellato l'art. 184 del D.Lgs. n. 58/1998, c.d. TUF) tra *insider* primario e *insider* secondario fa sì che tale distinzione soggettiva rilevi soltanto nella definizione della pena, che, a parità di altre condizioni, dovrebbe essere più elevata per i primari, data la funzione o attività che svolgono[109]. L'*insider* criminale che non dovesse rientrare nella figura dell'*insider* primario è ben probabile che riceva una pena comunque molto elevata, dato il forte disvalore della sua condotta.

I sistemi di AI potrebbero costituire strumenti istruiti a delinquere nell'ambito di più ampi disegni criminosi attuati dagli stessi o da altri sistemi che agiscono in vario modo sotto il controllo del medesimo soggetto o di più soggetti collusi.

Si pensi, ad esempio, ad attacchi *cyber* che mettano in difficoltà i più importanti operatori, intermediari o investitori istituzionali, che magari costringano gli stessi a procedere a ingenti vendite di strumenti finanziari per evitare che l'attacco produca problemi ulteriori (ad esempio di stabilità prudenziale) o, addirittura, che creino difficoltà alla piattaforma di contrattazione, per cui sia *ex ante* prevedibile un impatto sui prezzi o un blocco delle negoziazioni. Tali informazioni potrebbero facilmente assumere natura privilegiata ed essere opportunamente sfruttate da un sistema di AI grazie ad ordini immessi sul mercato calibrati a ridosso dell'attacco prima che l'attacco venga reso pubblico dagli stessi soggetti coinvolti o dai *media*.

In simili situazioni rientreremmo nella sopra illustrata casistica dei sistemi di AI istruiti a delinquere (v. sopra par. 3). Ma lo stesso è a dirsi, a maggior ragione, qualora l'informazione privilegiata sia parte dell'attività programmata dal medesimo sistema di AI. Casi ormai classici sono rappresentanti dall'acquisizione delle credenziali di clienti di un intermediario che consenta ai sistemi di AI di movimentare tali conti a beneficio di altri o, ancora, di inserire ordini di acquisto o vendita che creino bolle nei prezzi di

109 La Direttiva 89/592/CEE (MAD I), che ha introdotto nel diritto comunitario una disciplina sull'abuso di informazioni privilegiate, qualificava nell'art. 4 l'*insider* secondario come colui "*che consapevolmente sia in possesso di un'informazione privilegiata, l'origine diretta o indiretta della quale potrebbe essere soltanto*" un *insider* primario. Con la Direttiva 2003/6/CE, e successivamente anche con il Regolamento (UE) n. 596/2014 (MAR) e la Direttiva 2014/57/UE (MAD II), la seconda condizione è caduta, per cui l'*insider* secondario è semplicemente colui "*che sappia o che avrebbe potuto sapere trattarsi di informazioni privilegiate*", superando così il legame tra l'*insider* secondario e l'*insider* primario. Come è stato evidenziato: "*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).

predeterminati strumenti finanziari favorendo poi facili guadagni su conti di individui collusi.

Una ulteriore strategia di abuso di sistemi di AI potrebbe consistere nel compimento di piccole, ma ripetute violazioni, di guisa che le vittime difficilmente riescano a rendersi conto di essere state adescate o truffate; tale strategia appare tanto più insidiosa quanto più l'algoritmo sia "intelligente" (*recte*: astuto) e riesca a dosare illeciti in maniera tale da rendere irriconoscibile il progetto criminale complessivo.

1.2 *Insider* di sé stesso e AI

Largamente dibattuta nella dottrina e nella giurisprudenza l'ipotesi in cui il soggetto abusa di un'informazione attinente ad un evento dallo stesso progettato/ideato.

Nel contesto dell'informazione privilegiata relativa alle offerte pubbliche di acquisto, è stato a lungo esaminata la vicenda Cremonini, attinente a operazioni effettuate dal soggetto che controllava la società quotata prima di lanciare un'OPA che avrebbe portato al *delisting* della stessa.

Ad avviso della Consob, se le operazioni di acquisto sul mercato da parte del soggetto che controlla l'emittente sono state effettuate quando lo stesso ha già deciso di lanciare un'OPA per il *delisting*, e non lo ha ancora comunicato al pubblico, allora esse hanno violato la disciplina di settore, indipendentemente dalla circostanza che l'informazione era stata ideata dallo stesso soggetto che ha effettuato le operazioni[110].

Di diverso avviso una parte della dottrina, secondo la quale l'illiceità della condotta richiede una "necessaria alterità nei confronti dell'informazione" poiché, anche semanticamente, "un determinato nucleo di conoscenze potrà essere qualificato "informazione" solo ove sottenda il suddetto passaggio trasmissivo di due sfere di conoscenze"[111].

In giurisprudenza, viceversa, ha prevalso l'orientamento secondo cui l'*insider* di sé stesso è punibile sia sul lato penale sia su quello amministrativo[112].

110 Delibera Consob n. 17777 dell'11 maggio 2011. La delibera Consob è stata oggetto di opposizione, *ex* art. 187-*septies* TUF, dinanzi alla Corte di Appello di Bologna che l'ha poi rigettata; decisione poi convalidata anche dalla Corte di cassazione civile, Sez. II, 13 aprile 2017, n. 24310, in *Banca borsa tit. cred.*, n. 6, 2018, pp. 962 ss., con nota di A. BARTALENA, *O.p.a. per* delisting e insider trading*: brevi riflessioni sull'*insider *di sé stesso*, in *ivi*, pp. 2617 ss., 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 ss.; S. LOMBARDO, *L'*insider *di se stesso alla luce della decisione della Corte di Cassazione (civile)*, in *Giur. comm.*, n. 4, 2018, pp. 666 ss.

111 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 ss.; A.F. TRIPODI, *Informazioni privilegiate e statuto penale del mercato finanziario*, Padova, 2012.

112 Si veda Corte di Cassazione penale, Sez. V, 15 aprile 2021, n. 31507, nella quale i giudici della Suprema Corte affermano la rilevanza penale dell'*insider* di sé stesso. In particolare, la Corte delinea una nuova interpretazione del concetto di «informazione» quale «insieme di dati descrittivi della realtà», che non indica necessariamente una componente "dinamica" di raccolta e trasmissione delle informazioni ma altresì una componente "statica", ovvero «il dato di conoscenza, ancorché quest'ultimo sia rappresentativo di una realtà prodotta dal medesimo soggetto obbligato». Sulla base di queste considerazioni la Corte ha giudicato infondato il motivo di ricorso e chiarisce che l'art. 184, comma 1, TUF non

Come evidenziato[113], nel contesto delle OPA obbligatorie, d'altronde, le esigenze regolamentari che spingono per una legittimità degli acquisti preventivi dell'offerente trovano comunque un limite difficilmente valicabile quando la definizione dell'informazione privilegiata (decisione relativa al lancio dell'OPA) precede tali acquisti.

Il sistema di AI che sfrutti, con operazioni sul mercato, l'informazione attinente ad un evento da esso stesso progettato commetterebbe certamente un illecito[114].

Un esempio concreto di informazione privilegiata che un operatore artificiale è in grado di ideare o progettare consiste nei sistemi di AI che prevedono, in un primo momento, l'acquisizione di informazioni elementari su ordini "curando" pendenti (ottenute magari dallo stesso intermediario che gestisce il sistema di AI nei suoi rapporti, informatizzati o meno, con la clientela *retail* o istituzionale) e, in un secondo momento, la definizione di una ottimale strategia di minimizzazione dinamica del *price impact* dei medesimi ordini[115]. Ebbene, in tale contesto il sistema di AI potrebbe essere "esteso" con la decisione di eseguire altri ordini per conti proprietari dell'intermediario in grado di sfruttare l'impatto che la predefinita strategia di minimizzazione dinamica genererebbe sul mercato. Si è in sostanza nell'ambito di una sorta di schema di *front running*.

Analoghi esempi potrebbero riguardare le raccomandazioni di investimento generate dai *robo-advisor*, laddove il sistema di AI dovesse sfruttare tali informazioni anticipando i probabili ordini della clientela che riceve tali raccomandazioni, eventualmente in appositi documenti (c.d. studi o ricerche, su specifici settori industriali o titoli o a commento delle notizie diffuse dai *media* o dei *trend* dei prezzi).

Più complesso è il tema dell'accertamento dell'*insider* di sé stesso connesso ad un sistema di AI. Laddove, infatti, tale accertamento è sempre possibile se ad operare siano sistemi di AI deboli[116], in quanto il percorso logico-decisionale che li porta a

richiede la necessaria alterità tra creatore e utilizzatore dell'informazione, stabilendo che la disposizione *de qua* «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». Su questa pronuncia si rinvia a 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. In senso contrario a questa decisione si veda la precedente decisione Corte di Cassazione civile, Sez. II; 12 maggio 2020, n. 8782, e il relativo commento di C. PASSI, *Esiste il* Self-insider*, ma va scagionato! Riflessioni intorno alla sua qualificazione giuridica*, in *Soc.*, n. 4, 2021, pp. 455 ss. La decisione della Suprema Corte giunge all'esito di un *iter* giudiziario nel quale si erano pronunciati prima il Tribunale di Milano, Sez. III, 5 febbraio 2016, n. 12149, e poi la Corte d'Appello di Milano, Sez. II, 15 gennaio 2019, n. 284, ritenendo rilevante in sede penale la condotta dell'*insider* di se stesso. Si veda 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 ss.

113 M. MAUGERI, *Offerta pubblica di acquisto e informazioni privilegiate*, in *Riv. dir. comm.*, n. 2, 2018, pp. 267 ss.

114 M. VENTORUZZO, *Qualche nota su cosiddetto "insider di sé stesso" alla luce del Regolamento UE sugli abusi di mercato*, cit.

115 Come noto, tali sistemi di AI sono utilizzati sia dagli intermediari sia dagli investitori istituzionali.

116 Come illustrato nella Sez. II par. 1, i sistemi di AI si distinguono in base alla loro differente capacità d'interazione con l'uomo. Mentre i sistemi di AI deboli producono *outputs* che dipendono dalle istruzioni prestabilite da produttori,

immettere un ordine nel mercato è, per definizione, trasparente; viceversa, per i sistemi di AI forti tale accertamento è reso difficoltoso dall'opacità (*black box*) di tale percorso logico-decisionale.

1.3 *Tipping*, *tuyautage* e AI

Oltre alla conclusione di operazioni, le altre principali modalità di sfruttamento dell'informazione privilegiata tipicamente proibite dagli ordinamenti riguardano la comunicazione a terzi senza "giustificato motivo" dell'informazione (c.d. *tipping*) e la raccomandazione a terzi (c.d. *tuyautage*[117]), sulla base dell'informazione privilegiata, di operare in una modalità conveniente. Ai destinatari della comunicazione illecita e della raccomandazione sono posti analoghi divieti. Tali divieti sono necessari per evitare facili elusioni del divieto di *insider trading*, ma trovano anche una loro autonoma ragion d'essere rispetto all'obiettivo di salvaguardare l'integrità dei mercati. Se non fossero vietate l'ulteriore comunicazione o raccomandazione, si potrebbe arrivare a situazioni teoriche paradossali in cui l'insieme dei soggetti a conoscenza dell'informazione privilegiata sia più ampio di quello dei soggetti che non ne sono a conoscenza[118].

Anche per le fattispecie di *tipping* e *tuyautage* è d'uopo individuare quali siano le informazioni privilegiate di cui un sistema di AI potrebbe eventualmente abusare. Valgono al riguardo le analisi sopra esposte, in merito al caso del sistema che tenga in considerazione informazioni attinenti all'attacco *cyber*, agli ordini pendenti della clientela o alle raccomandazioni d'investimento alla clientela.

Con riferimento a queste ultime, si potrebbe esaminare il caso in cui le raccomandazioni di investimento riguardino proprio quell'insieme di informazioni che porta il sistema di AI ad effettuare le operazioni di *trading* per le quali è stato programmato e che grazie alle notevoli capacità di immagazzinamento ed elaborazione dei dati possono risultare profittevoli. Ad esempio, la miriade di micro-informazioni sui movimenti che avvengono nella profondità dei *book* di negoziazione di strumenti finanziari negoziati in più sedi di negoziazione o di strumenti finanziari collegati o correlati agli stessi; siamo naturalmente nel campo dei *big data*. Ad esempio, le informazioni rilevate dai satelliti sulla dimensione del traffico su autostrada, che consentono di prevedere con maggiore accuratezza i ricavi delle società autostradali; siamo nel campo degli *alternative data* e della *mosaic theory*[119]. Ad esempio, ancora, l'immediata rilevazione delle informazioni lanciate dalle agenzie di stampa.

programmatori o utenti, i più evoluti sistemi di AI forti, dotati di capacità di auto-apprendimento, producono *outputs* autonomi e imprevedibili rispetto agli *inputs* iniziali di produttore, programmatore o utente.

117 Talora pure definiti, rispettivamente, *illegal disclosure* e *tipping*.

118 Per una ricostruzione delle condotte di *tipping* e *tuyautage* si veda V. Calandra Buonaura, *Sub art. 184*, in *Commentario breve al Testo Unico della Finanza*, Padova, 2020, pp. 1228 ss., spec. pp. 1236-1241.

119 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*».

Appare pacifico che tali informazioni che i sistemi di AI utilizzano per elaborare le proprie strategie di speculazione, investimento, *trading* o arbitraggio e che se rese pubbliche dal sistema potrebbero essere qualificate come privilegiate (si pensi per esempio al caso in cui la strategia operativa venga rappresentata in un apposito studio diffuso dall'intermediario alla propria clientela), oltre a poter essere utilizzate dal sistema di AI in qualità di *insider* di sé stesso, possano essere oggetto di lecita comunicazione a terzi o raccomandazione ad operare in una certa direzione. È questo il caso del *robo-advising*[120].

In generale, finché le informazioni elementari sulle quali tali strategie si basano sono pubbliche non può certamente ipotizzarsi un abuso.

Ciò nondimeno, si pone la questione se alcuni tipi di informazione, ad esempio quelle contenute nelle rilevazioni fotografiche elaborate da satelliti orbitali, possano essere considerate pubbliche, stante l'importante investimento necessario per acquisirle. Con specifico riferimento al campo finanziario, lo stesso potrebbe dirsi per gli ingenti investimenti che servono per la rielaborazione delle informazioni relative ai *book* di negoziazione o la raccolta di informazioni disaggregate.

Considerato che tali investimenti non sono alla portata di qualsiasi investitore, al punto che la difficoltà di accedere a tali informazioni ha portato a un dibattito sui rischi per la competitività del mercato[121], si potrebbe valutare se questa difficoltà infici anche quella *ratio* della disciplina che giustifica l'introduzione del divieto di abuso con l'egalitarismo, almeno potenziale, degli investitori che partecipano agli scambi.

Al riguardo, si deve però tenere presente che sono comunque davvero molti i soggetti che investono in queste tecnologie (e, naturalmente, ancora di più quelli che hanno la possibilità di farlo) e che l'*expertise* si muove facilmente, coinvolgendo peraltro in modo imprescindibile l'accademia, che porta con sé una spinta alla divulgazione delle tecnologie e degli *outputs*[122]. Si rileva altresì che un incentivo alla divulgazione è insito presso i *data provider*: si pensi a quelle funzioni offerte da *Bloomberg* o *Refinitiv Eikon* alla rispettiva vasta clientela, professionale e non, che consentono di conoscere in tempo reale l'andamento di variabili che la letteratura accademica ha qualificato come "informative" perché, ad esempio, esprimono il *sentiment* del mercato, quali il numero di volte che il nome di un titolo ricorre su *Google* o su *Twitter*[123].

120 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.

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

122 Il tema sembra del tutto analogo a quello dell'accesso limitato a ricerche o studi diffusi a pagamento dagli analisti finanziari e che poi detti *media provider* ribaltano alla rispettiva vastissima clientela nelle loro linee essenziali (*target price*, raccomandazioni, previsione dei risultati aziendali annuali). È proprio opera dei menzionati *media provider* la definizione del c.d. *consensus* degli analisti, cioè la statistica di sintesi delle stime prodotte dagli analisti.

123 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*

In conclusione, sembra valere ancora in questo nuovo ambito quella osservazione fatta rilevare in passato con riferimento all'accesso alle informazioni diffuse dai quotidiani: sebbene questo accesso richieda il pagamento di un prezzo non indifferente per molti investitori, ciò non mette in discussione la solidità della *ratio* della disciplina.

Se allora le informazioni privilegiate rilevate (più che create) dal sistema di AI possono essere rappresentate in forma di studio, ricerca o raccomandazione d'investimento e diffuse dall'intermediario che gestisce il sistema di AI alla relativa clientela, appare pacifico che la comunicazione di tali informazioni o le raccomandazioni operative basate sulle stesse siano considerate lecite.

Rimane ferma l'opportunità che, in conformità alla disciplina generale, prevista anche dal Regolamento (UE) *MAR,* tali studi, ricerche o raccomandazioni di investimento siano diffusi alla clientela con modalità e tempistiche *fair* che evitino abusi. Il Regolamento (UE) *MAR* richiede, ad esempio, che tali studi indichino la data e l'orario di prima diffusione alla clientela[124]. Pertanto, chi li dovesse ricevere prima di tale istante dovrebbe astenersi dall'utilizzarli con operazioni sul mercato, trattandosi ancora di informazioni privilegiate, o dal comunicarli a terzi e chi li riceve tempo dopo tale istante sa che l'informazione è stata verosimilmente già oggetto di operazioni da parte di altri clienti.

2 Manipolazione del mercato e AI

Le criticità nell'impiego dell'intelligenza artificiale sono oggi tra le questioni più dibattute e non soltanto nel mercato finanziario[125]. Con particolare riguardo alle criticità dell'AI nella sfera delle operazioni finanziarie, i rischi per l'integrità dei mercati derivanti dal comportamento dei sistemi di AI sono avvertiti in misura maggiore nel *trading* piuttosto che nella formazione e circolazione delle informazioni privilegiate. Essi sono stati oggetto di numerosi approfondimenti ed interventi regolamentari con

Than Words: Quantifying Language to Measure Firms' Fundamentals, in *The Journal of Finance*, Vol. 63, 2008, pp. 1437-1467.

124 Si vedano gli artt. 7 e 8 del Regolamento Delegato (UE) 2016/958. In particolare, l'art. 7 stabilisce che «(l)a persona che produce raccomandazioni che diffonde una sua raccomandazione vi include la data e l'ora della prima diffusione».

125 In una lettera pubblicata sul sito del *Future of Life Institute* il 22 marzo 2023 (https://futureoflife.org/open-letter/pause-giant-ai-experiments/), firmata tra gli altri da Elon Musk, Yuval Noah Harari, Steve Wozniak e Andrew Yang, si evidenziano i rischi che l'intelligenza artificiale può comportare per la società e l'umanità. Gli estensori si chiedono se sia il caso che sistemi di AI divengano competitivi come l'uomo, con il pericolo per quest'ultimo di perdere il controllo della nostra civiltà, e chiudono la lettera con l'auspicio di arrivare preparati all'autunno dell'intelligenza artificiale dopo una lunga estate di sviluppo dell'AI. Questa lettera è stata oggetto di attenzione da parte dei media; si veda *ex multis* M. GAGGI, *Perché l'intelligenza artificiale spaventa i re della tecnologia*, in *Corriere della Sera*, 30 marzo 2023, pp. 1-22. A questo appello si è unito, più di recente, il monito di Geoffrey Hinton, padre della tecnologia da cui è nata *ChatGPT*, che ha definito «spaventose» le conseguenze dell'utilizzazione dell'intelligenza artificiale in quanto questa tecnologia sarebbe capace di imparare separatamente e poi condividere la conoscenza istantaneamente a tutti gli altri sistemi. Si veda P. PISA, *Il 'Nobel' dell'informativa lascia Google. "L'intelligenza artificiale è pericolosa"*, in *La Repubblica*, 3 maggio 2023, p. 14.

riguardo all'operatività ad alta frequenza (*HFT*) posta in essere, principalmente, da soggetti membri dei mercati sui quali operano[126].

L'operatività di un sistema di AI debole non è in ultima analisi che una evoluzione molto sofisticata degli elementari ordini condizionati, quali gli *iceberg orders* o gli *stop-loss orders*, che al presentarsi di certi livelli di prezzo immettono nel mercato un certo quantitativo in acquisto o in vendita. Questi tipi di ordini comparvero all'indomani dell'introduzione dei sistemi di negoziazione telematici, negli anni Novanta del secolo scorso, presentando diversi profili di criticità poi comunque largamente superati.

L'assetto regolamentare che ne è derivato per gestire l'operatività *HFT* sembra oggi piuttosto adeguato ad affrontarne i rischi[127]. Del resto, alcuni casi di abuso sono già stati sanzionati in diverse giurisdizioni, anche della UE[128].

Naturalmente, rimangono importanti dubbi sul comportamento del singolo sistema di AI debole o sul comportamento congiunto di più sistemi di AI, specie in condizioni di elevata incertezza sui mercati o in situazioni di *market disruption*, collegati ai cc.dd. *flash crash*.

Per valutare le criticità associate all'utilizzo congiunto di più sistemi di AI si consideri preliminarmente che non è inusuale riscontrare operatività acefala da parte di intermediari, tipicamente quando operano nei mercati con più *desk* (anche antropici) sul medesimo strumento finanziario ma ciascuno perseguendo finalità diverse: un *desk* opera come *market maker*, uno per fare *delta hedging*[129] per il portafoglio proprietario, un altro per sfruttare *trend* nell'andamento dei prezzi di breve o brevissima durata (c.d. *trading* direzionale). In tali casi, potrebbero emergere sospetti di manipolazione se una delle due gambe con cui si muove un *desk* (quella in acquisto o quella in vendita) incrocia o interseca successivamente una gamba di un altro *desk*, dando luogo, nel primo

126 Sull'evoluzione del quadro normativo in materia di manipolazione del mercato si veda E. AMATI, *Abusi di mercato e sistema penale*, Torino, 2012, pp. 171 ss., e più di recente, con riferimento all'illecito amministrativo, ID., *L'illecito amministrativo di manipolazione del mercato e le persistenti criticità del doppio binario sanzionatorio*, in *Giur. comm.*, n. 2, 2021, pp. 263 ss., e, con riferimento all'illecito penale, a F. CONSULICH, *Manipolazione dei mercati e diritto eurounitario*, in *Soc.*, n. 2, 2016, pp. 203 ss.

127 Sulle prospettive di una rivisitazione della disciplina UE si veda ESMA "*MIFID II Review Report*", 28 settembre 2021, ESMA70-156-4572.

128 La casistica include (tra parentesi l'anno in cui è occorsa la manipolazione): negli Stati Uniti *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* (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).

129 Il *delta hedging* consiste nelle operazioni di acquisto e/o vendita che sono effettuate giornalmente sul sottostante di strumenti finanziari derivati per coprire il rischio delle variazioni dei prezzi del sottostante sulle posizioni precedentemente assunte su tali strumenti finanziari derivati (J. HULL, *Opzioni futures e altri derivati*, Pearson, 2022).

caso, ad operazioni apparentemente fittizie (*matched orders*)[130] e, nel secondo caso, a tipiche figure manipolative (ad esempio, *trash & cash*)[131].

Ebbene, quando i *desk* sono gestiti da individui o da sistemi di AI deboli il sospetto di manipolazione potrebbe essere alla fine escluso guardando il *track record* della precedente operatività sui medesimi conti, riscontrando le condizioni esterne che hanno motivato gli ordini, chiedendo spiegazioni ai *traders* o all'unità di *compliance* dell'intermediario, ecc.

Inoltre, in via preventiva la società di gestione del mercato potrebbe contrastare i rischi associati a tali eventuali operazioni sospette (*matched orders*)[132] cancellando automaticamente i contratti incrociati che produce il conto proprio di uno stesso intermediario, sia pure per *desk* diversi.

Per valutare le criticità associate all'utilizzo di un singolo sistema di AI debole, d'altronde, si consideri che è già prassi ordinaria di numerosi importanti investitori istituzionali quella di inserire i propri ingenti ordini secondo tempistiche determinate

130 Nell'Allegato II del Regolamento Delegato (UE) 2016/522 della Commissione che integra MAR (c.d. Livello 2) è individuata tra le prassi (manipolative) quella di "*effettuare operazioni a seguito dell'inserimento di ordini di acquistare e vendere che sono negoziati contemporaneamente o quasi contemporaneamente in quantità simili e a un prezzo simile da uno stesso soggetto o da soggetti diversi ma in collusione tra loro — prassi generalmente nota come «improper matched orders». Questa prassi può essere illustrata anche dai seguenti indicatori aggiuntivi di manipolazioni del mercato: i) operazioni o ordini di compravendita che hanno o è probabile che abbiano l'effetto di fissare un prezzo di mercato quando la liquidità o lo spessore del book di negoziazione (order book) non è sufficiente per fissare un prezzo durante la sessione; ii) gli indicatori di cui alla presente sezione, paragrafo 1, lettera a), punto i)* [ovvero: *insolita concentrazione di operazioni e/o ordini di compravendita, in termini generali o da parte di una sola persona che utilizza uno o più conti o da parte di un numero limitato di persone*;], *e paragrafo 3, lettera a), punti i) e ii)* [ovvero: "*aderire ad accordi per la vendita o l'acquisto di uno strumento finanziario, un contratto a pronti su merci collegato o un prodotto oggetto d'asta sulla base di quote di emissioni senza variazioni degli interessi beneficiari o del rischio di mercato o con il trasferimento dell'interesse beneficiario o del rischio di mercato tra soggetti che agiscono di concerto o in collusione tra loro — prassi generalmente nota come «wash trades». Questa prassi può essere illustrata anche dai seguenti indicatori aggiuntivi di manipolazioni del mercato: i) ripetizione insolita di un'operazione tra un numero limitato di soggetti durante un determinato periodo di tempo; ii) operazioni o ordini di compravendita che modificano o è probabile che modifichino la valutazione di una posizione senza diminuirne/aumentarne le dimensioni*"]. Esempi di manipolazione tramite "*improper atched orders*" sono stati sanzionati dalla Consob con riferimento, tra l'altro, a incroci di ordini da parte di un *asset manager* che curava l'operatività di due fondi favorendo la *performance* di un fondo a scapito di quella dell'altro, sul quale percepiva minori commissioni. Nel dettaglio, l'*asset manager* inseriva prima un ordine di importanti dimensioni per conto del fondo che intendeva favorire ad un prezzo che era molto distante dal *bid-ask spread* (e quindi non influiva sul processo di formazione dei prezzi) e successivamente un ordine di dimensioni ancora più importanti per conto dell'altro fondo ad un prezzo tale da incrociare sia tutti gli ordini a prezzi più convenienti del primo, così "scalando" il book di negoziazione fino ad arrivare a sia quello del fondo che intendeva favorire. Tale operatività "puliva" il *book* con una serie di contratti generando una importante variazione istantanea del prezzo corrente, per poi tipicamente rimbalzare dopo pochi istanti grazie all'operatività degli arbitraggisti che riconoscevano un prezzo non coerente con l'insieme delle informazioni pubblicamente disponibili. Per un'analisi C. Milia, *Essays in Market Manipulation and Insider Trading*", PhD Thesis, Bocconi University, 2008.

131 Nel citato Allegato II del Regolamento Delegato (UE) 2016/522 della Commissione che integra MAR è individuata tra le prassi (manipolative) quella di "*assumere una posizione short (corta) in uno strumento finanziario, (...) e poi effettuare ulteriori attività di vendita (...) allo scopo di abbassarne il prezzo attirando altri venditori. Quando il prezzo è sceso, la posizione detenuta viene chiusa - prassi generalmente nota come «trash and cash»*". In sostanza si tratta della prassi inversa a quella del «*pump and dump*», cioè della "bolla manipolativa" dei prezzi.

132 Borsa Italiana S.p.A. prevede, come misura preventiva, la possibilità per gli intermediari membri di cancellare automaticamente gli ordini immessi dai conti proprietà, c.d. *Self-Trade Prevention* ("*Guide to the Euronext Trading System*", Version 1.2, March 2023).

dall'AI, ad esempio per minimizzare l'impatto dell'operatività sui prezzi (il *price impact*[133]). Gli ordini che tali investitori immettono sui mercati per gestire i relativi imponenti portafogli sono spesso molto elevati rispetto alla liquidità dei mercati e, quindi, la loro esecuzione richiede tempo in modo tale da non generare un impatto sfavorevole sui prezzi. Se infatti l'investitore intende assumere una posizione su uno strumento finanziario azionario, quanto più i suoi ordini di acquisto generano aumenti dei prezzi e tanto maggiore sarà il prezzo di carico della posizione che intende assumere e, quindi, tanto minore sarà il profitto che potrà eventualmente conseguire quando il previsto rialzo dei prezzi dovesse realizzarsi. È quindi solitamente preferibile inserire gli ordini sul mercato in modo gentile, diradato nel tempo, "curando"[134], come indicavano verbalmente gli investitori istituzionali italiani agli intermediari incaricati di eseguire tali ingenti ordini.

Se, per un verso, la minimizzazione del *price impact* dovrebbe, altresì, ridurre i rischi di generare un impatto significativo sul processo di formazione dei prezzi[135], è, per altro verso, anche vero che il sovrastante fine di minimizzare i costi potrebbe non essere soggetto ad ulteriori condizioni. In uno scenario in cui l'investitore istituzionale intenda ridurre la propria posizione su uno strumento finanziario, allora l'algoritmo che dovesse pure prevedere una prossima riduzione dei prezzi dello strumento finanziario troverebbe conveniente accelerare l'immissione di ordini in vendita sullo stesso strumento in modo da ridurre le perdite attese derivanti dal previsto peggioramento delle condizioni di prezzo. L'immediatezza e la violenza dell'esecuzione con frequenti e ingenti ordini aggressivi di vendita sarebbero, dunque, pienamente coerenti con il suddetto obiettivo di ridurre il *price impact* degli ordini.

Si rammenta che il sistema di AI debole che innescò il noto *flash crash* del 6 maggio 2010 era utilizzato da un investitore istituzionale che intendeva coprire le proprie elevatissime posizioni su singoli strumenti finanziari azionari tramite la rapida e progressiva vendita di *futures* sull'indice azionario. Quell'algoritmo inseriva ogni minuto ordini in vendita senza limite di prezzo alla condizione che fossero pari al 9% dei quantitativi complessivi scambiati sul mercato nel minuto precedente, così progressivamente accentuando il *trend* decrescente dei prezzi[136].

I dubbi e le criticità sollevati dai sopra descritti modelli di operatività assumono una nuova dimensione ove si consideri l'ipotesi che tali condotte siano effettuate avvalendosi di sistemi di AI forti[137], cioè quelli basati sulle reti neurali artificiali, sul

133 *Ex pluribus*, si veda Bouchaud, Jean-Philippe. "Price impact." arXiv preprint arXiv:0903.2428 (2009).

134 L'ordine "curando" è un ordine nel quale il cliente si affida all'esperienza dell'intermediario per la scelta delle migliori possibilità offerte dal mercato. Gli ordini non recano alcuna condizione riguardo al prezzo e devono essere assolti dall'intermediario nei tempi e nei modi più opportuni per il committente.

135 Sulle applicazioni di AI alle attività di *trading* v. ESMA "*Artificial Inteligence in EU Security Markets*", ESMA-164-6247, 3 February 2023.

136 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.

137 Nei citati principi di Asilomar i sistemi di AI forti sono qualificati ora "advanced AI system" (principio n. 9) ora "(h)ighly autonomous AI systems" (principio n. 10). I principi di Asilomar sono consultabili sulla pagina internet del Future of Life Institute (https://futureoflife.org/open-letter/ai-principles/).

deep reinforcement learning, dove l'algoritmo è in grado da solo di riconoscere nuove opportunità di profitto senza che lo stesso o i suoi programmatori o i suoi gestori siano capaci di spiegare il percorso logico che ha portato proprio a quelle scelte operative osservate[138].

Infatti, quando le gambe sono mosse da un sistema di AI forte si perde la possibilità, per l'intermediario, per la società di gestione del mercato – e financo per le Autorità di vigilanza – di riconoscere *ex post* l'origine della strategia di *trading* perseguita: *market making*, *delta hedging*, *trading* direzionale[139], ecc. In altri termini, si potrebbe rappresentare quello che ha fatto l'AI forte, si potrebbe dire perché dovrebbe averlo fatto ma non si potrebbe dire perché lo ha fatto.

In aggiunta, si pensi anche al caso, realistico, in cui il sistema di AI, per quanto forte sul piano del *deep learning* e dell'elaborazione autonoma di strategie operative, al pari di un qualsiasi sistema di AI debole difetti, tuttavia, di autocoscienza, cioè non sia in grado di riconoscere che alcuni degli ordini che egli stesso vede presenti nel *book* di negoziazione siano stati, in realtà, immessi dallo stesso sistema; come se lo stesso fosse una specie di piovra senza testa.

In una recente analisi prodotta dall'autorità olandese *AFM* emerge come più intermediari non si avvalgono di sistemi di AI forti per la preoccupazione di non saper gestire il rischio di turbative degli scambi, anche derivante dall'incapacità di saper eventualmente fornire spiegazioni alle Autorità[140].

Ciò nondimeno, evidenze sull'utilizzo di sistemi di AI forti esistono.

Non che la loro adozione porti necessariamente a comportamenti che costituiscano, di per sé, una manipolazione del mercato. Ma se lo stesso investitore istituzionale, magari tramite il medesimo conto e lo stesso sistema di AI forte, immettesse ordini di segno opposto al seguire del *trend* innescato dai suddetti ordini di vendita, allora rientreremmo pienamente in uno schema manipolativo *trash & cash* e nessuno sarebbe probabilmente in condizione di fornire una spiegazione alternativa a questa. Il sistema di AI forte, infatti, lasciato all'autoapprendimento e non "allenato" ad evitare schemi manipolativi quali il *trash & cash*, troverebbe coerente con l'obiettivo di minimizzare il costo per l'investitore derivante dall'inserimento di ordini ingenti di vendita quello di far seguire a questi anche ordini di acquisto capaci di mediare con profitto il prezzo di carico degli ordini di vendita.

138 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. Per rispondere alle esigenze di trasparenza ed aprire la "*black box*", sono in corso numerose analisi da parte della comunità scientifica nel ramo della c.d. *Explainable AI* (ovvero, XAI): P. Bracke – A. Datta – C. Jung – S. Sen, *Machine Learning exlainability in finance: an application to default risk analusis*, 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.

139 Il *trading* direzionale consiste nell'operatività volta a prendere una direzione di acquisto o di vendita di strumenti finanziari sulla base di previsioni sul prossimo andamento dei prezzi di mercato.

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

È quindi opportuno chiedersi se i sistemi di AI forti possano essere ammessi al *trading* e a quali condizioni.

Nell'ipotesi in cui si ritenga, come oggi, che i sistemi di AI possano operare sui mercati, risulta altresì doveroso chiedersi se le fattispecie previste dagli ordinamenti siano adeguate a fronteggiare comportamenti manipolativi o che, comunque, mettano a rischio eccessivo l'integrità dei mercati.

2.1 L'approccio regolamentare europeo

Per fronteggiare la complessità degli schemi di abuso e i rischi che le fattispecie colgano involontariamente condotte speculative in vero lecite o, ancora, la difficoltà per le Autorità di distinguere le violazioni dalle condotte conformi, la Direttiva 2003/6/CE introdusse un approccio molto ricco e articolato che contrastava con quello olistico in vigore in Italia dal 1991 e che ancora, con alcune modifiche, sopravvive nell'art. 185 TUF sia pure "limitatamente" al regime penale.

Mentre quest'ultima norma oggi sanziona "(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", il Regolamento (UE) *MAR* – che deriva da quella direttiva e permea la corrispondente Direttiva 2014/17/UE che individua le condotte sanzionabili penalmente – si basa su un approccio articolato su quattro pilastri: le fattispecie, suddivise in quattro tipologie (nell'art. 12, par. 1), gli esempi (nell'art. 12, par. 2) e gli "indicatori" delle stesse (nell'art. 12, par. 3, e nell'Allegato I) nonché le ulteriore "prassi" manipolative (che potremmo definire esempi o strategie manipolative) che specificano tali indicatori (all'art. 4 e nell'Allegato II del Regolamento delegato (UE) 2016/522); inoltre, l'art. 15 indica il divieto di manipolazione, l'art. 5 prevede alcune esenzioni per l'acquisto di azioni proprie e la stabilizzazione se effettuati secondo certe stringenti condizioni, e l'art. 13 stabilisce una disciplina per le prassi di mercato eventualmente ammesse dalle Autorità di vigilanza nazionali[141].

La ricchezza di questo approccio illustra bene come le difficoltà insite nella definizione dell'illecito siano altrimenti considerate a rischio di interpretazioni soggettive: una pluralità di fattispecie, accompagnate da esempi e indicatori spesso (ma non necessariamente) caratterizzanti lo schema manipolativo, dovrebbe infatti ridurre tale rischio, che, secondo alcuni[142], è talmente importante da rendere preferibile non introdurre alcun divieto di manipolazione e non offrire alcuna protezione al bene del "regolare funzionamento del mercato", cioè del processo di formazione dei prezzi e, quindi, dell'efficienza informativa e dell'efficienza allocativa delle risorse[143].

141 Ad oggi è stata ammessa solo una prassi, relativa ai contratti di liquidità ed articolata in modalità diverse dalle autorità di Francia, Spagna, Italia e Portogallo. Sempre sui contratti di liquidità una prassi di mercato è stata istituita in via generale nel Regolamento (UE) 2019/2155 per tutte le PMI con azioni negoziate nei relativi mercati di crescita.

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

143 A differenza di quanto in precedenza illustrato con riguardo all'abuso di informazioni privilegiate, l'analisi economica è sostanzialmente concorde nel ritenere che la manipolazione rechi un danno al mercato. Condotte che artificiosamente allontanano i prezzi di mercato dai valori fondamentali, o, comunque, da quelli che il mercato in un dato mo-

Al di là del differente approccio eurounitario rispetto a quello nazionale, come ancora oggi espresso sul lato penale dall'art. 185 TUF, sembra si possa concordare con quanti concludano che "nonostante la diversità di formulazione, gli ambiti degli art. 185 e 187-*ter* (che rinvia al regolamento eurounitario, ndr) tendano a coincidere"[144]. Del resto, a valle di una severa procedura di infrazione avviata dalla Commissione europea, la normativa nazionale è stata infine ritenuta coerente con la citata Direttiva 2014/17/UE che individua le condotte sanzionabili penalmente, che, a sua volta, nell'art. 5 richiama perfettamente, con gli aggiustamenti dovuti al carattere penale delle fattispecie, il ricco *wording* previsto dall'art. 12 del Regolamento (UE) *MAR* per le fattispecie sanzionate in via amministrativa.

mento ritiene tali, alterano il processo di formazione dei prezzi, forniscono falsi segnali agli altri partecipanti al mercato, riducono l'efficienza informativa dei prezzi e, in ultima analisi, l'efficienza allocativa delle risorse (v. L. Loss, *Fundamentals of Securities Regulation*, Boston MA, 1988). Inoltre, tipicamente ai guadagni del manipolatore corrispondono almeno pari perdite per gli altri partecipanti al mercato. Non si tratta necessariamente di un gioco a somma zero, potendo i falsi segnali trasmessi dal manipolatore generare ulteriori perdite per quanti vengono ingannati da tali falsi segnali. Inoltre, gli scandali associati alla manipolazione, sia di tipo informativo che operativo, conducono sistematicamente ad una perdita di fiducia nel funzionamento dei mercati e quindi ad un allontanamento di molti investitori dai mercati, o quanto meno dai segmenti in cui gli scandali si verificano. Si pensi al mercato dei *corporate bond* dopo gli scandali Parmalat e Cirio o al mercato dei mutui *subprime* dopo la crisi finanziaria del 2007. Tuttavia, diversi economisti hanno rappresentato come l'introduzione di un divieto di manipolazione del mercato possa risultare eccessivamente costoso per via del rischio che le autorità commettano errori valutativi nel qualificare una condotta come manipolativa, sia con riguardo a quella informativa che a quella operativa (C.F. Camerer, *Can Asset Markets Be Manipulated? A field Experiment with Racetrack Betting*, in *Journal of Political Economy*, 1988). Tantopiù se si considera come non sia tecnicamente agevole riuscire a manipolare i mercati. Infatti, rispetto alla prima, è stato rappresentato come chi diffonda informazioni false o fuorvianti non possa ripetere la condotta più volte senza danneggiare la propria reputazione, e quindi non ci sia spazio nel lungo periodo per la manipolazione. Rispetto alla seconda, è stato evidenziato come l'elasticità dei prezzi (v. J.S. Mill, *Principles of Political Economy*, London: Longmans, Green and Co., 1921), l'elevata liquidità dei mercati, le sempre più sofisticate misure di microstruttura degli stessi (si pensi ai *circuit breakers* o alla chiusura *random* dell'asta elettronica) e l'importante trasparenza degli scambi (si pensi anche agli obblighi di comunicazione delle vendite allo scoperto) non consentano di alterare significativamente i prezzi per un periodo prolungato (v. E. Avgouleas, *The Mechanics and Regulation of Market Abuse*, Oxford University Press, 2005). Altri studi hanno di contro dimostrato come, con riferimento alla manipolazione informativa, qualora l'informazione falsa non sia verificabile *ex post* o se il soggetto che la diffonde possa apparire aver agito in buona fede (come, ad esempio, nel caso degli analisti finanziari che producono molte ricerche ogni mese), allora sussisterebbero importanti spazi per la manipolazione anche nel lungo periodo (v. R. Benabou – G. Laroque, *Using Privileged Information to Manipulate Markets : Insiders, Gurus and Credibility*, in *Quarterly Journal of Economics*, 1992). Con riferimento alla manipolazione operativa è oggi di comune evidenza come l'elasticità dei prezzi dipenda dalle molte condizioni di quantità e di tempo che caratterizzano gli ordini che li generano, mentre la liquidità, la microstruttura e la trasparenza, pur limitando gli spazi delle possibili manipolazioni, non sono in grado di eliminarle del tutto. Se, quindi, sul lato empirico, alla fine del secolo scorso la manipolazione del mercato sembrava confinata alla inadeguata struttura dei mercati dei secoli precedenti, con le spettacolari bolle dei prezzi dei tulipani (v. P.M. Garber, *Famous First Bubbles*, The MIT Press, 2000), con i giochi settecenteschi degli *stock jobbers* (v. F. Annunziata, *Un Robinson Crusoe alla borsa di Londra*, La Vita Felice, 2019) o nei primi decenni del secolo scorso con i *corner* sui mercati dei derivati sulle merci (F. Allen – L. Litov – J. Mei, *Large Investors, Price Manipulation, and Limits to Arbitrage: An Anatomy of Market Corners*, in *Review of Finance*, 2006) e gli *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), e, più recentemente, con i *pump & dump schemes*, ma soltanto in mercati minori quali gli *OTC bulletin pink sheet* (v. R.K. Aggarwal – G. Wu, *Stock Market Manipulations*, in *Journal of Business*, 2006, Vol. 79, n. 4, pp. 1915 ss.), i più vicini scandali del nuovo millennio relativi alle IPO durante la *tech-bubble*, alla manipolazione dei *benchmark* e del Libor, alla manipolazione del *fixing* dei mercati a pronti delle valute (v. P. Hillion – M. Suominen, *The Manipulation of Closing Price*s, in *Journal of Financial Markets*, 2004, p. 7), all'operatività ad alta frequenza durante i *flash crash* e agli interrogativi connessi al caso *Gamestop* (v. US SEC, *Staff Report on Equity and Options Market Structure Conditions in Early 2021*, 14 October 2021) hanno progressivamente ribaltato quell'orientamento ottimistico, portando anche la Commissione UE ha proporre la *MAD II*, prima direttiva attinente all'armonizzazione di sanzioni penali. Peraltro, la frammentazione degli scambi su più sedi di negoziazione ha ampliato il novero delle correlazioni e delle interconnessioni degli scambi, apprendo nuovi o ulteriori spazi per strategie di manipolazione *cross-markets* e *cross-product*.

144 S. Seminara, *Il diritto penale del mercato mobiliare*, cit., p. 121.

Nel prosieguo, si farà quindi riferimento alle definizioni del Regolamento (UE) *MAR*, partendo dalla manipolazione operativa, principale terreno delle analisi in argomento.

2.2 La manipolazione operativa e l'AI

La *trade-based manipulation* è definita nell'art. 12, par. 1, del Regolamento (UE) *MAR*, lett. a) e b)[145].

Si rileva come la condotta di cui alla lettera a) sia, a sua volta, suddivisa in due fattispecie entrambe sottoposte ad una medesima duplice condizione:

a) la conclusione di un'operazione, l'inoltro di un ordine di compravendita o qualsiasi altra condotta che:

i) invii, o è probabile che invii, segnali falsi o fuorvianti in merito all'offerta, alla domanda o al prezzo di uno strumento finanziario, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni; oppure

ii) fissi, o è probabile che fissi, il prezzo di mercato di uno o più strumenti finanziari, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni a un livello anormale o artificiale;

a meno che la persona che conclude un'operazione, inoltra un ordine di compravendita o ha posto in essere qualsiasi altra condotta dimostri che tale operazione, ordine o condotta sono giustificati da legittimi motivi e sono conformi a una prassi di mercato ammessa, come stabilito a norma dell'articolo 13.

145 L'origine delle definizioni adottate dal legislatore può essere rilevata in un lavoro del 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; (...)*".

Si osserva come nella condotta sub i) il successo della strategia faccia leva sulla reazione della condotta sugli altri partecipanti alle contrattazioni, i quali potrebbero essere ingannati dai "falsi o fuorvianti segnali" trasmessi dalla condotta del manipolatore, grazie a ordini immessi o grazie alle relative conseguenti operazioni; diversamente, nella condotta sub ii) il successo della condotta deriva direttamente dall'azione di forza del manipolatore, il quale, indipendentemente dalla reazione degli altri partecipanti al mercato, "fissa" il prezzo a "un livello anormale o artificiale" (in quanto gli torna per qualche motivo conveniente).

Entrambe le condotte influiscono sul processo di formazione dei prezzi.

Orbene, è evidente che sono moltissimi gli ordini che quotidianamente influiscono (o, *rectius*, è probabile che influiscano) sul processo di formazione dei prezzi, proprio perché questi ultimi si formano sul mercato a valle dell'interazione di una moltitudine di soggetti, i quali inserendo i propri ordini allineano la quotazione, almeno approssimativamente, con le aspettative generali. Fermo restando che alcune frizioni possono rallentare questo processo, esso ha natura dinamica: il prezzo che si è appena formato è oggetto di nuova rielaborazione da parte degli operatori, i quali a loro volta reagiscono con nuovi ordini che, quindi, concorrono alla formazione di un ulteriore valore, consentendo, in via iterativa, la convergenza verso il *fair value* che esprime i valori dei *fundamentals* dello strumento finanziario sottostante, in linea con l'insieme delle informazioni pubblicamente disponibili. È così assicurata l'efficienza informativa di tipo semi-forte del mercato e, pertanto, l'efficienza allocativa delle risorse, andando queste più facilmente verso gli investimenti che più meritano di essere finanziati.

I potenziali effetti che scaturiscono dalla condotta illecita, cioè i "segnali falsi o fuorvianti" o i prezzi a livelli "anormali o artificiali", evidenziano l'importanza di una valutazione controfattuale, incentrata sulla differenza tra quello che la condotta ha provocato e quello che, invece, sarebbe successo in assenza della stessa.

Trattandosi di definizioni volutamente *effect-based* e *non intent-based*, disegnate in modo da sanzionare anche i comportamenti non dolosi, i richiami alla falsità, alla fuorvianza e all'artificiosità non dovrebbero presupporre il riconoscimento di una condotta malevola, quanto il mero potenziale impatto sul processo di formazione dei prezzi.

Se così è, come sembra che sia, allora, come si diceva, sono moltissimi gli ordini immessi sul mercato che quotidianamente incidono o potrebbero incidere su tale processo fornendo segnali falsi o fuorvianti o che portano o potrebbero portare il prezzo a valori anormali.

Si pensi a quanti ordini provocano forti variazioni dei prezzi, in una direzione opposta a quella coerente con l'insieme delle informazioni pubblicamente disponibili e che trovano, ad esempio, chiara giustificazione nella necessità di liquidità da parte di uno degli investitori (*liquidity trader*).

Ecco allora che, per non cadere nell'assurdo di qualificare come manipolative centinaia di manipolazioni ogni giorno, soccorre la prima delle due condizioni previste dall'art. 12, par. 1, lett. a), "*a meno che la persona che conclude un'operazione, inoltra*

un ordine di compravendita o ha posto in essere qualsiasi altra condotta dimostri che tale operazione, ordine o condotta sono giustificati da legittimi motivi (...)"[146].

Diviene quindi cruciale la possibilità di riscontrare la sussistenza di legittimi motivi, quali, tipicamente, quelli rientranti in strategie di arbitraggio, di investimento o di speculazione.

La *black box* dei sistemi di AI forti inibisce però la possibilità di chiarire se la condotta sia giustificata da legittimi motivi; di qui il rilievo del tema della ammissibilità dell'operatività sui mercati finanziari tramite sistemi di AI forti e, in caso positivo, della adeguatezza della definizione di manipolazione del mercato di tipo operativo fornita dal Regolamento (UE) *MAR*.

Esiste invero un'altra disposizione in grado di ricomprendere le condotte manipolative realizzate attraverso l'utilizzo di sistemi di AI, siano essi deboli o forti: si tratta della disposizione contenuta nell'art. 12, par. 1, lett. b), che considera manipolativa "*la conclusione di un'operazione, l'inoltro di un ordine di compravendita o qualsiasi altra attività o condotta che incida, o sia probabile che incida, sul prezzo di uno o più strumenti finanziari, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni, utilizzando artifici o qualsiasi altra forma di raggiro o espediente*".

Come evidenziato dalla dottrina, tuttavia, l'art. 12, par. 1, lett. b) "*suscita così problemi a causa della sua genericità, accresciuta dall'assenza di ogni riferimento ai potenziali effetti sul prezzo degli strumenti finanziari*"[147]; il che porta a considerare questa disposizione più che altro una norma di chiusura della fattispecie di manipolazione operativa alla quale fare ricorso soltanto in via eccezionale.

È vero che strategie di *layering & spoofing* (perpetuate da sistemi di AI) sono state oggetto di sanzione in altri ordinamenti anglosassoni facendo leva sui concetti di artificiosità della condotta, ma è pur evidente che una tale soluzione non sarebbe coerente con il più ricco, trasparente e rigoroso approccio del Regolamento (UE) *MAR*, che sin da questi primi anni di vita sembra aver dato buona prova di sé.

Occorre anche riconoscere che l'approccio del Regolamento (UE) *MAR* già fornisce un'altra strada per rispondere all'operatività dei sistemi di AI, che non passa per la definizione della fattispecie ma per la diretta illustrazione dell'esempio manipolativo. Questa strada è stata battuta per arginare le prime manifestazione di operatività di sistemi di AI che lavorano ad alta frequenza, gli *High Frequency Traders* (*HFT*)[148].

146 Sottolineatura aggiunta.

147 La norma non è accompagnata da indicatori nell'Allegato I del Regolamento (UE) MAR e nell'Allegato II del Regolamento delegato (UE) 2016/522.

148 Sulle caratteristiche della negoziazione algoritmica si rinvia a 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 ss., e, con riferimento all'arbitraggio statistico e all'arbitraggio di latenza, a M. BERTANI, Trading algoritmico *ad alta frequenza e tutela dello* slow trader, in *Analisi giur. econ.*, n. 1, 2019, p. 268. La negoziazione algoritmica (c.d. *algorithmic trading*) e la negoziazione algoritmica ad alta frequenza (c.d. *high frequency trading*) devono essere considerate espressamente legittime per il riconoscimento ricevuto dalla normativa interna dall'art. 1, comma 6-*quinquies* e comma 6-*septies*, TUF, le cui nozioni sono state introdotte nell'art. 4, nn. 39 e 40, della dir. 2014/65/UE (*Markets in financial instruments directive*, c.d. *MiFID*

L'art. 12, par. 2, lett. c) chiarisce con tre esempi che costituiscono una manipolazione rilevante: "*l'inoltro di ordini in una sede di negoziazione, comprese le relative cancellazioni o modifiche, con ogni mezzo disponibile di negoziazione, anche attraverso mezzi elettronici, come le strategie di negoziazione algoritmiche e ad alta frequenza, e che esercita uno degli effetti di cui al paragrafo 1, lettere a) o b), in quanto: i) interrompe o ritarda, o è probabile che interrompa o ritardi, il funzionamento del sistema di negoziazione della sede di negoziazione; ii) rende più difficile per gli altri partecipanti al mercato individuare gli ordini autentici sul sistema di negoziazione della sede di negoziazione, o è probabile che lo faccia, anche inserendo ordini che risultino in un sovraccarico o in una destabilizzazione del book di negoziazione (order book) degli ordini; oppure iii) crea, o è probabile che crei, un segnale falso o fuorviante in merito all'offerta, alla domanda o al prezzo di uno strumento finanziario, in particolare inserendo ordini per avviare o intensificare una tendenza*"[149]. In aggiunta l'Allegato II del Regolamento delegato (UE) 2016/522 fornisce specifici indicatori ed importanti esempi delle fattispecie di cui sopra all'art. 12(1)(a) denominati "*quote stuffing*", "*momentum ignition*", "*layering and spoofing*" e "*smocking*"[150].

Tuttavia, sono i considerando (5-9) del Regolamento delegato (UE) 2016/522 che, oltre a chiarire bene la portata indicativa e non esaustiva degli indicatori e degli esempi di prassi manipolative e a chiarire bene che sussiste la finalità di tener conto degli sviluppi tecnici sui mercati, precisano, tra l'altro, che: "*Taluni esempi di prassi riportati nel presente regolamento descrivono casi che sono compresi nella nozione di manipolazioni del mercato o che, sotto alcuni aspetti, fanno riferimento a una condotta di manipolazione. Dall'altro canto, alcuni esempi di prassi possono essere considerati*

II), implementando le ESMA *Guidelines on system and controls in an automated trading environment for trading platforms, investment firms and competent authorities*, (ESMA/2012/122), 24 febbraio 2012. In particolare, per "negoziazione algoritmica" si intende «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). Per "tecnica di negoziazione algoritmica ad alta frequenza" si intende «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).

149 Sottolineatura aggiunta.

150 "*Quote suffing*": "inserire quantitativi ingenti di ordini di compravendita e/o cancellazioni e/o aggiornamenti di tali ordini per creare incertezze tra gli altri partecipanti, rallentare il loro processo e/o mascherare la propria strategia". "*Momentum ignition*": "inserire ordini di compravendita o una serie di tali ordini o effettuare operazioni o serie di operazioni che sono probabilmente in grado di avviare o accentuare un trend e di incoraggiare altri partecipanti ad accelerare o ampliare tale trend per creare l'opportunità di chiudere o aprire una posizione a un prezzo favorevole". "*Layering and spoofing*": "trasmettere ordini di negoziazione multipli o ingenti, spesso con parametri distanti da quelli presenti su un lato del *book* di negoziazione, per effettuare una negoziazione sull'altro lato di detto *book*. Una volta effettuata tale negoziazione, gli ordini non destinati a essere eseguiti sono rimossi"."*Smoking*": "inserire ordini di compravendita per attirare altri partecipanti al mercato che utilizzano tecniche di negoziazioni tradizionali («*slow trader*»), e poi modificare rapidamente tali ordini rendendo le condizioni meno generose, nella speranza che la loro esecuzione sia redditizia rispetto al flusso in arrivo degli ordini di compravendita degli *slow trader*". Sulle nuove modalità commissive del reato di manipolazione del mercato si veda 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 ss.

legittimi se, ad esempio, una persona che compie operazioni o inoltra ordini di compravendita che possono configurarsi come una manipolazione del mercato è in grado di dimostrare che le motivazioni alla base di tali operazioni o tali ordini erano legittime, e che le operazioni e gli ordini in questione erano conformi alle prassi ammesse sul mercato considerato"[151].

Questi esempi, essendo mirati al contrasto dell'eventuale operatività manipolativa degli *HFT*, riescono sì a cogliere condotte dei sistemi di AI, ma, da un lato, non risultano generali e, dall'altro lato, fanno riferimento a sistemi di AI deboli e non superano il problema centrale del rapporto tra il legittimo utilizzo dei sistemi di AI forti ed i rischi connessi alla difficoltà di ricostruire il percorso logico-motivazionale alla base dell'operatività di tali sistemi.

In definitiva, dall'analisi della disciplina della manipolazione operativa emerge con evidenza che l'attuale quadro normativo – nel lodevole intento di contemperare la tutela del regolare processo di formazione dei prezzi e la libertà di intermediari e investitori di assumere condotte e strategie giustificate da legittimi motivi – rischi (forse in modo non voluto) di non supportare adeguatamente – ed anzi, di fatto, già finisca per ostacolare - la diffusione e lo sviluppo dei sistemi di AI forti nei mercati finanziari, così limitando altresì il progresso scientifico e tecnologico e i significativi benefici che essi sono suscettibili di apportare alla crescita dei mercati stessi e dell'economia in generale.

2.3 La manipolazione informativa e l'AI

I sistemi di AI forti producono un dirompente ampliamento delle possibili strategie di manipolazione informativa applicabili con successo da malintenzionati. Si considerino ad esempio il fenomeno delle *app* che producono *fake news* con il supporto di immagini o voci umane, rendendo estremamente realistica la falsa informativa offerta al pubblico.

Queste estensioni presentano naturalmente criticità che investono ambiti più ampi di quelli che toccano i mercati finanziari e, nello specifico, la manipolazione del mercato. Si è innanzi a problemi di carattere sociale e politico che riguardano la *privacy*, la formazione del consenso, la tutela delle fasce deboli della popolazione ma anche di *leader* politici e di personaggi pubblici.

Nei casi di eventuali eclatanti abusi, tra i quali, ad esempio, quello del sistema di AI forte che dovesse adottare tecniche di *deepfake* per trasmettere false informazioni tramite "finte" immagini di persone che hanno capacità di influenzare le scelte degli operatori o dell'opinione pubblica, diventerebbe importante, come per le altre *fake news*, la velocità di reazione con cui i soggetti coinvolti, cioè in primo luogo le persone lese, ma anche i giornalisti e i *media*, riescono a rivelare al pubblico l'errore così da limitare la durata dell'impatto sui prezzi di mercati.

151 Sottolineatura aggiunta.

In tali casi è tipicamente evidente la riconducibilità oggettiva della condotta alle fattispecie proprie della manipolazione informativa, specie se la stessa è accompagnata da operazioni sul mercato atte a trarre vantaggio dall'effetto prodotto sui prezzi (si rammenta che il Regolamento (UE) *MAR* non richiede che per incorrere nella manipolazione informativa sia necessario effettuare operazioni sui mercati). La semplice idoneità delle dichiarazioni non veritiere a produrre effetti sui mercati rende le stesse illecite e sanzionabili, indipendentemente dall'eventuale finalità ludica del *deepfake* e, più in generale, dalla circostanza che gli autori del *deepfake* intendano o meno manipolare il prezzo di uno o più strumenti finanziari.

OItre ai casi eclatanti di chiara natura fraudolenta, sono di interesse anche i casi più subdoli in cui l'utilizzo di sistemi di AI consente di indurre una pluralità di soggetti (o anche pochi soggetti con potere di mercato) a comportarsi in modo coordinato, così da influenzare i prezzi dei titoli in una direzione conveniente al sistema di AI forte. In tali casi potrebbe essere difficile riconoscere il carattere manipolativo delle condotte e reagire prontamente per scongiurare che l'effetto sui prezzi si prolunghi ulteriormente.

La fattispecie prevista dall'art. 12, par. 1, lett. c) del Regolamento (UE) *MAR* sembra adeguata a contrastare la condotta ipotizzata, consentendo a che la condotta manipolativa sia effettuata non solo "*tramite i mezzi di informazione, compreso Internet*" ma anche "*tramite ogni altro mezzo (...) compresa la diffusione di voci*".

Tuttavia, la fattispecie richiede il soddisfacimento della condizione che "*la persona che ha proceduto alla diffusione sapeva, o avrebbe dovuto sapere, che le informazioni erano false o fuorvianti*". Si torna allora alle difficoltà già individuate per un sistema di AI forte tali requisiti.

Anche sotto questo profilo, appare dunque, opportuno un intervento correttivo delle fattispecie previste dal Regolamento (UE) *MAR*.

Altre situazioni di manipolazione informativa possono scaturire "automaticamente" se il sistema di AI, per esempio, acquista sul mercato quantitativi che comportano la pubblicazione della partecipazione ai sensi dell'art. 120 TUF. Tali messaggi possono infatti trasmettere informazioni false o fuorvianti in quanto non rispondenti alla "volontà" che ha generato la decisione di operare in quella direzione. Ancora una volta il sistema di AI forte non sarebbe in grado di fornire risposte attendibili, non potendo quella volontà essere ricostruita *ex post* e, financo, essere "ricordata".

Infine, torna ancora il caso dei *robo-advisor*, che potrebbero generare raccomandazioni di investimento "*errate o tendenziose o manifestamente influenzate da interessi determinanti*", così rientrando negli indicatori di manipolazione di cui all'art. 12, par. 1, lett. b), se accompagnate da operazioni opportunisticamente effettuate immediatamente prima o dopo la diffusione delle stesse raccomandazioni.

3 Gli illeciti di abusi di mercato commessi da più AI collusi

L'ambito del *trading* diviene ancora più rilevante se si guarda alle interazioni che il sistema di AI può avere sia con gli investitori umani sia con altri traders algoritmici.

Innanzitutto, alcuni sistemi di AI godono di un elemento competitivo più marcato rispetto a qualsiasi forma di negoziazione: la velocità di inserire una quantità molto elevata e temporalmente ravvicinata di ordini di esecuzione, modifica o cancellazione di operazioni. Ciò evidenzia una marcata differenza di dotazioni tra queste negoziazioni algoritmiche e qualsiasi investitore umano sul mercato finanziario. Indubbiamente la capacità di gestire, a distanza di centesimi, millesimi o milionesimi di secondo, la direzione degli investimenti mediante una pluralità di ordini e operazioni con l'intento di sfruttare questo vantaggio competitivo e attirare l'attenzione degli altri operatori, specie degli *slow traders*, in termini profittevoli, evoca una maggiore possibilità di condotte abusive[152]. Ma il potenziale competitivo non riguarda necessariamente transazioni "superveloci" in quanto può insinuarsi in dinamiche di scambio meno veloci[153], nei quali la c.d. *black box* algoritmica elabora decisioni di *trading*, fondate su motivi, calcoli e strategie, più difficilmente comprensibili rispetto all'agire dell'uomo, anche per il produttore, il programmatore o l'utente del sistema di AI[154].

A ciò si aggiunge che attraverso l'utilizzo delle intelligenze artificiali è possibile che operatori umani elaborino una pluralità di innovativi meccanismi di intervento nelle negoziazioni. In particolare, gli algoritmi possono essere utilizzati come strumento di attuazione, realizzazione o facilitazione di un accordo collusivo di alcuni operatori finanziari[155]. In queste ipotesi, i fenomeni collusivi sono agevolmente imputabili agli operatori coinvolti.

Già l'approfondito esame del *flash crash* del 6 maggio 2010 sul *E-Mini S&P 500 Futures* aveva messo in luce come i vari *HFTs* avessero risposto in modo simile (*herding*) e violento ad un ingente ordine di vendita disposto da un investitore istituzionale che si avvaleva di un algoritmo per coprirsi dal rischio legato alla crisi della Grecia per le proprie posizioni sul mercato azionario statunitense. Ciò a prescindere dalla presenza negli scambi di un manipolatore seriale, Navinder Sarao, che abitualmente, anche quel giorno, aveva messo in azione algoritmi che applicavano una strategia di *layering & spoofing*.

Posto che ormai sugli strumenti finanziari più liquidi gli ordini provenienti da algoritmi raggiungono l'80% del totale degli scambi, l'interazione degli stessi fa parte

152 In questo senso M. BERTANI, Trading *algoritmico ad alta frequenza e tutela dello* slow trader, cit., *passim*, spec. p. 267, che fa riferimento ad un'asimmetria informativa dello *slow trader* rispetto ai *traders* algoritmici. Ciò si rispecchia poi in una riduzione del rischio per l'operatore algoritmico e un incremento per rischio per lo *slow trader*, ovvero per l'investitore umano.

153 In questo senso A. AZZUTTI – W.G. RING – H. S. STIEHL, *The Regulation of AI trading from an AI Life Cycle Perspective*, cit. p. 13.

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

155 Si tratta del rischio della c.d. associazione «uomo-macchina», così definito da G. TEUBNER, *op. cit.*, pp. 105-113.

della ordinaria modalità di formazione dei prezzi. Pertanto, in una prospettiva di vigilanza, i *flash crash* e le operazioni di manipolazione appaiono come la parte visibile di un fenomeno, quello dell'interazione degli algoritmi, che, invece, di norma, non sembra generare problemi.

Tuttavia, come il citato caso di manipolazione di Navinder Sarao ha mostrato, l'azione di vigilanza potrebbe non essere rapida nel rilevare abusi di mercato che avvengono ad alta velocità. È, cioè, ben possibile che, nell'ambito di una apparente calma dei mercati, si celino, in realtà, una pluralità di micromanipolazioni a danno degli altri partecipanti e con effetti significativi sulle grandezze che esprimono la qualità dei mercati.

Venendo poi a considerare i sistemi di AI più evoluti, basati sul c.d. "*reinforcement learning*", la loro reciproca interazione può generare, in modo spontaneo e senza programmazione iniziale, tacite condotte collusive[156] non imputabili all'uomo[157]. Come riportano le cronache, infatti, «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». Tutto ciò potrebbe cagionare fenomeni di sostanziale impunità in quanto le disposizioni in vigore sanzionano unicamente comportamenti coscienti e volontari o, quantomeno, riconducibili ad eventuali forme di negligenza di produttori e programmatori[158].

Sul piano della repressione di queste dinamiche manipolative illecite (o più latamente abusive), al pari delle condotte illecite concordate da due o più *traders*, la dottrina, seppure con riferimento esclusivo all'*high frequency trading*, ha evidenziato che le forme di collusione algoritmica tacita sfuggono di per sé al tradizionale modello di regolamentazione e di vigilanza basato sull'uomo. In questi casi le implicazioni reciproche dei *traders* algoritmici, nonché quelle di questi con gli investitori tradizionali, sono difficili da controllare in quanto l'interazione tra i *traders* «rischia di essere così tanto correlata che se anche uno di questi sfugga ai controlli *ex ante* e di conformità,

156 Una definizione di "collusione tacita" derivante dall'impiego degli algoritmi si rinviene in ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *Algorithms and collusion. Competition Policy in the Digital Age*, 2017, p. 19, ove si precisa che essa «*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*».

157 Questo rischio è stato individuato dapprima dagli studiosi di diritto della concorrenza. Si rinvia con riferimento alle questioni di *enforcement antitrust* pertanto a M. FILIPPELLI, *La collusione algoritmica*, in *Orizz. dir. comm.* (*orizzontideldirittocommerciale.it*), fasc. speciale, 2021, pp. 375 ss.; P. MANZINI, *Algoritmi collusivi e diritto antitrust europeo*, in *Mer. Conc. Reg.*, n. 1, 2019, pp. 163 ss.; 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 ss.; 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.). Sugli effetti della collusione algoritmica nei mercati finanziari, con speciale riguardo alla stabilità dei mercati di capitale A. AZZUTTI – W.G. RING – H. S. STIEHL, *Machine learning, market manipulation and collusion on capital markets: why the "black box" matters*, cit., i quali individuano i fattori di mercato che possono facilitare la produzione della collusione algoritmica (*market trasparency, a higher frequency of interactions, product homogeneity, market concentration, entry barrier and innovations*).

158 Così J. HANSEN, *Ci sono anche i pc delinquenti*, in *ItaliaOggi*, 11 maggio 2019, pp. 1 e 11.

tutti i controlli effettuati sugli altri partecipanti sino a quel momento risulterebbero essere stati vani»[159]; in particolare, anche nell'ipotesi in cui l'operatività di un *trader* possa essere prevedibile «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»[160].

Queste preoccupazioni sono certamente estensibili ai sistemi di AI, i cui meccanismi di funzionamento, già imperscrutabili, possono sviluppare comportamenti collusivi non captabili sulla base di autonome dinamiche relazionali, indipendentemente dalla velocità di negoziazione degli algoritmi. Un siffatto fenomeno potrebbe non soltanto integrare condotte illecite di manipolazione, non riconducibili all'uomo, ma produrre effetti sul funzionamento complessivo del settore finanziario.

4 La manipolazione informativa nei *social network* e l'AI

Il *trading* algoritmico va esaminato anche in relazione alle potenzialità dei *social media* e dei *social network*[161]. I nuovi contenitori *on line* di notizie hanno radicalmente mutato le modalità diffusive delle informazioni, caratterizzate ormai da due principali caratteristiche: la rapidità della circolazione e la decentralizzazione delle informazioni[162].

I *social network* consentono a ciascun individuo di essere non solo fruitore di notizie ma altresì produttore di notizie, veicolate in tempo reale in *internet* nei confronti di tutti gli utenti/individui connessi[163]. La combinazione delle nuove modalità di comunicazione con i *traders* algoritmici può produrre effetti sistemici sulla stabilità del

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

160 Ivi, pp. 310-311. Nel medesimo senso 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, per il quale il fenomeno non può considerarsi circoscritto all'high frequency trading ma all'utilizzazione di una varietà di tecnologie dinamiche e aggressive che portano tutte al fenomeno della c.d. *ghost liquidity*. In particolare, è possibile che i volumi scambiati si impennino a causa di due circostanze illustrate dall'A.: «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».

161 È opportuno avvertire che il pericolo insito nei social network non è limitato alla potenza diffusiva dei traders algoritmici. Si può fare riferimento al caso *Gamestop* nel quale non è stata la potenza algoritmica a sovvertire la dinamica speculativa dei fondi di investimento ma una massa di piccoli investitori, la cui alleanza è stata resa possibile dalla appartenenza di costoro alla medesima *digital community*. In questo senso 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 ss.

162 Su queste caratteristiche si rinvia ampiamente a G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in *Rivista di diritto dei media* (*medialaws.eu*), n. 1, 2018, p. 22.

163 Ibidem. Si veda altresì F. Donati, *L'art. 21 della Costituzione settanta anni dopo*, in *Rivista di diritto dei media* (*medialaws.eu*), n. 1, 2018, pp. 93 ss.

mercato finanziario. I *traders* algoritmici, mediante la loro capacità di acquisizione ed elaborazione di tutte le fonti di comunicazione, comprese quelle derivanti dal canale della *mass information*, possono produrre un effetto "rimbalzo" sul prezzo degli strumenti finanziari quotati. Una decisione di investimento di un *trader* algoritmico può basarsi sul «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»[164], senza essere in grado di individuare segnali di anomalia che spingerebbero un trader umano a non negoziare[165].

La dinamica di condizionamento del *trading* da parte dei *social media* e dei *social network* può essere acuita da una manifestazione del fenomeno più invasiva, ovvero quello della *mass disinformation*, consistente nella diffusione di informazioni errate e *fake news* e qualificato da parte della dottrina come «*the most damaging form of market manipulation in terms of market value and investor confidence*»[166]. Queste informazioni, infatti, non sono sempre affidabili e riconducibili ad un soggetto facilmente individuabile[167]; esse potrebbero altresì sottintendere anche vere e proprie "raccomandazioni di investimento", dalle quali derivano gli obblighi previsti dal Regolamento (UE) *MAR*[168], qualora la pubblicizzazione attenga direttamente a prodotti finanziari, soprattutto da parte di soggetti non abilitati, ovvero non sottoposti all'adempimento delle regole specifiche in materia finanziaria per indirizzare le scelte degli investitori in funzione delle loro conoscenze e della loro propensione al rischio[169].

In effetti, la *mass disinformation* può configurare nuove modalità di commissione di manipolazione informativa, alterare il fisiologico incontro tra domanda ed offerta e incidere sul valore degli strumenti finanziari. I relativi effetti possono essere vieppiù fuorvianti e dirompenti qualora queste informazioni siano "catturate" dagli algoritmi di negoziazione, specialmente da quelli di alta velocità, producendo episodi di forte volatilità dei titoli finanziari (i cc.dd. *flash crash* già accennati), evidenziati da alcune notizie di cronaca[170]. Ciò accade per la capacità di questi algoritmi «di sfruttare

164 M. PALMISANO, *op. cit.*, p. 135.

165 P. LUCANTONI, *L'*high frequency trading *nel prisma della vigilanza algoritmica del mercato*, cit., p. 300.

166 T.C.W. LIN, *The new market manipulation*, cit., pp. 1292-1294, spec. p. 1293.

167 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, sottolinea che le notizie circolanti in rete «possono (e spesso è così) non avere una paternità evidente, trattandosi di *meme*, articoli anonimi, estratti di *blog*, i cui contenuti vengono divulgati mediante strumenti quali la condivisione o il *retweet* che consentono di perpetuare l'anonimato».

168 Art. 3, par. 1, 35), Regolamento (UE) *MAR* relativo agli abusi di mercato offre una definizione di «raccomandazione in materia di investimenti» in termini di «informazioni destinate ai canali di distribuzione o al pubblico, intese a raccomandare o a consigliare, in maniera esplicita o implicita, una strategia di investimento in merito a uno o a più strumenti finanziari o emittenti, ivi compresi pareri sul valore o sul prezzo presenti o futuri di tali strumenti».

169 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 ss., spec. pp. 311 e 321.

170 Si veda M. LONGO, *Allarme* social network. *Così insidiano le Borse*, in *Il Sole 24 ore*, 22 marzo 2018, pp. 1 e 3. L'articolo ricorda almeno quattro casi di diffusione di *fake news* via *social network* che hanno provocato episodi di alta volatilità del mercato finanziario o di alcuni titoli su di esso. Il primo riguarda la notizia falsa nel 2010 di un aereo della compagnia australiana *Qantas* precipitato in Indonesia; il secondo si è verificato nell'aprile del 2013 quando alcuni hacker hanno boicottato l'*account Twitter* dell'agenzia di stampa *Associated Press* diffondendo la falsa notizia di un attacco alla Casa Bianca; il terzo episodio ha preso avvio nel 2013 dalla creazione da parte di un trader di falsi *account Twitter*

al meglio i movimenti rapidi e spesso violenti che i mercati manifestano dopo la pubblicazione di dati macro o notizie importanti»[171].

È quindi opportuno valutare se il tradizionale divieto di dichiarare il falso, che vale per tutti quanti abbiano un potere di mercato (*manager*, investitori istituzionali, *guru*, analisti finanziari, politici, giornalisti, ecc.), sia adeguato a contrastare casi di *mass disinformation* e, più in generale, la pubblicazione di informazioni false o fuorvianti tramite modalità decentralizzate.

di società di ricerca finanziaria che diffondevano la falsa notizia che la società *Sarepta Therapeutics* fosse sotto inchiesta; il quarto, avvenuto nel 2009, riguarda alcune false notizie diffuse da due soggetti su alcuni titoli sulla Borsa di New York. Sui primi due episodi si veda C. Mottura, *Decisione robotica negoziale e mercati finanziari*, cit., pp. 272-274.

171 A. Puorro, High Frequency Trading*: una panoramica*, *op. cit.*, p. 16.

III Profili penalistici

1 La delimitazione oggettiva degli illeciti di abuso di mercato e l'AI

Non c'è reato finanziario che non possa essere commesso dall'intelligenza artificiale[172] e quest'ultima, lasciata a se stessa, è incline a delinquere perché enormemente più veloce dell'essere umano nel cogliere le occasioni propizie.

Eppure, considerate le già illustrate differenti declinazioni, non è chiaro cosa sia l'intelligenza artificiale[173]. Prova ne è che sono state individuate più di settanta definizioni alternative[174], oltre a una 'ufficiale', elaborata dalla Commissione in una recente proposta di regolamento in materia di AI[175]. Quella forse più nota è di McCarthy, che ebbe a chiamarla la scienza e l'ingegneria di creare macchine intelligenti, specialmente programmi informatici intelligenti, parlando al contempo dell'intelligenza come della parte computazionale dell'abilità di raggiungere scopi nel modo, la quale ha varie tipologie e livelli[176]. Anche altre che si sono succedute sono senza dubbio parimenti efficaci nel tratteggiare un nucleo semantico promettente per una riflessione in chiave giuridica, ad esempio si pensi a quella di Russel e Norvig secondo cui l'agente artificiale si riassume in quattro caratteri: «*thinking like a human; acting like a human; thinking rationally, and acting rationally*»[177].

172 Sull'incertezza nella definizione dell'intelligenza artificiale, 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 ss.

173 Che l'intelligenza artificiale non è un concetto univoco è evidenziato da C. Burchard, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, *op. cit.*, p. 1914.

174 S. Legg – M. Hutter, *A collection of definitions of intelligence*, in *Frontiers in Artificial Intelligence and Applications*, Vol. 157, 2007, pp. 17 ss. (https://arxiv.org).

175 Commissione Europea, Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione, COM/2021/206 *final*. La proposta di regolamento UE, all'art. 3(1) definisce un sistema di IA come: «un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono». Questa definizione è stata modificata nella posizione elaborata dal Consiglio dell'Unione europea il 6 dicembre 2022 e ha assunto il seguente tenore letterale: «un sistema progettato per funzionare con elementi di autonomia e che, sulla base di dati e input forniti da macchine e/o dall'uomo, deduce come raggiungere una determinate serie di obiettivi avvalendosi di approcci di apprendmento automatico e/o basati sulla logica e sulla conoscenza, e produce output generati dal sistema quali contenuti (sistemi di AI generative), previsioni raccomandazioni o decisioni, che influenzano gli ambienti con cui il Sistema di IA interagisce».

176 J. Mccarthy, *What Is Artificial Intelligence?*, 12 novembre 200, (www.formal.stanford.edu).

177 S. Russell – P. Norvig, *Artificial Intelligence: A Modern Approach*, Hoboken, 2021, p. 2.

Quel che è sottesa a quest'ultima definizione e pare più importante agli occhi del penalista è stato ulteriormente chiarito da una semplice notazione di Jacob Turner secondo cui ciò che è più tipico dell'AI è la sua abilità, pur essendo un'entità non naturale, di compiere scelte attraverso un processo di valutazione[178]. Caratteri comuni alle forme oggi note di intelligenza artificiale sono la capacità di rilevare e analizzare i dati costitutivi dell'ambiente in cui operano, al fine di raggiungere nel modo più efficiente l'obbiettivo caratteristico, che nel campo dei mercati finanziari è, tendenzialmente, identificabile con il profitto[179].

Proprio questa propensione alla scelta ponderata ha implicazioni notevoli per una disciplina che mira a regolare, *ex ante*, e a punire, *ex post*, scelte non conformi alle opzioni di tutela espresse dal legislatore.

L'ossimoro di una decisione libera dal diritto e dalle sue conseguenze non è tollerabile dal sistema giuridico e la frustrazione dell'impotenza dei legislatori contemporanei viene camuffata con la scelta di soluzioni variegate e non sempre efficienti nell'attribuzione a qualche persona fisica il fatto dell'algoritmo.

Quello dei mercati è certamente il settore che più di ogni altro consente di confrontarsi con le sfide dell'intelligenza artificiale, perché l'attività da regolare è già oggi per lo più compiuta da operatori non fisici. Quanto diremo vale dunque principalmente per questo settore, al netto del fatto che sono davvero molti i reati che possono essere commessi da un agente artificiale, perfino l'acquisto di stupefacenti sul *deep web*, come dimostrato dalla vicenda del *bot shopper* (precisamente *Random Darknet Shopper*, un programma dedicato all'acquisto di prodotti *on line*), costruito per finalità artistiche nel 2014: proprio grazie alla dimostrazione di aver agito a questo scopo i programmatori che avevano congegnato l'esibizione furono scagionati da ogni accusa[180].

La presenza di una forma cibernetica di *market abuse* rappresenta una sfida a prima vista impossibile per i regolatori, poiché all'incertezza in merito ai tratti salienti di un agente artificiale si somma l'imprecisione di ogni definizione di manipolazione, vale a dire come la si possa oggettivamente distinguere da forme di speculazione mobiliare legittima[181], seppure magari aggressiva, e persino la trasfigurazione dei connotati del mercato finanziario. Siamo infatti da tempo al cospetto di una vera e propria

178 J. Turner, *Robot Rules: Regulating Artificial Intelligence*, Cham, 2019, p. 16.

179 Si vedano i punti fermi tracciarti dal Comitato sull'intelligenza artificiale del Consiglio d'Europa, su cui 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.

180 Sulla vicenda cfr. M. Power, *What happens when a software bot goes on a darknet shopping spree?*, reperibile alla seguente url https://www.theguardian.com).

181 Sulle perenni difficoltà di trovare un accordo in letteratura sul concetto di manipolazione, A. Verstein, *Benchmark Manipulation*, *B.C. L. Rev.*, Vol. 56, 2015, pp. 272 ss.; sulla incertezza nella distinzione tra legittimi programmi di *trading* e vera e propria turbativa, T.E. Levens, *Comment, Too Fast, Too Frequent? High Frequency Trading and Security Class Actions*, *U. Chi. L. Rev.*, Vol. 82, 2015, pp. 1515 ss. e, in Italia, sia consentito il rinvio a F. Consulich, *La giustizia e il mercato*, Milano, 2010, 37 ss.

balcanizzazione degli scambi[182], poiché anche il luogo di incontro di domanda e offerta, un tempo istituzionalizzato, è un *asset* contendibile, oggetto di concorrenza tra gestori, sottoposto ad un'evoluzione senza sosta alla ricerca della migliore efficienza per gli operatori 'clienti'.

In un contesto in cui ogni riferimento è mobile, le esternalità si concentrano sui soggetti meno reattivi ai cambiamenti, caratteristica che tende a coincidere con i piccoli investitori, o *slow traders*; è una constatazione ricorrente, fin dal lavoro di Michael Lewis, *Flash Boys*[183].

Al crescere dell'entropia del mercato, aumenta il vantaggio competitivo di coloro che fanno della velocità di decisione la propria cifra identitaria, cioè gli algoritmi per la negoziazione ad alta frequenza (o *High Frequency Traders*), per quanto deve essere ben chiaro che questi non esauriscono le forme di manifestazione dell'intelligenza artificiale sui mercati e in generale nell'ambito dell'applicazione dell'intelligenza artificiale nei vari contesti sociali.

Allora l'azione preventiva/repressiva resa possibile dalle fattispecie penalistiche in materie di mercati finanziari deve adeguarsi al mutato scenario criminologico, confermato dalla stessa SEC, che ha definito gli *HFT* come uno dei più significativi sviluppi nella struttura dei mercati negli ultimi anni[184].

Fatta questa precisazione, nell'intento di delimitare il più precisamente possibile l'ambito dell'indagine, è chiaro che il delitto per antonomasia che può essere perpetrato per mezzo (e non già da) dell'intelligenza artificiale è la manipolazione del mercato. L'utilizzo di algoritmi, da un lato, ha agevolato l'esecuzione di tecniche manipolative comuni, dall'altro, ha consentito l'ideazione di nuove forme che richiedono necessariamente l'impiego di *HFT*. L'espressione per mezzo, dunque, va in qualche misura riletta: non si deve intendere in senso puramente meccanicistico, ma nella consapevolezza di una strumentalità creativa, in cui l'uomo pone le premesse e fissa un risultato in termini di genere o classe di eventi che si desidera produrre, e l'agente artificiale colma la distanza tra le prime e il secondo in modalità non predefinibili. È infatti chiaro che il sistema intelligente può apprendere e financo 'inventare' nuove tecniche e occasioni di turbare gli scambi e i prezzi degli strumenti quotati. Rimane fuori dal perimetro di analisi il caso in cui la distorsione dei corsi azionari che occorra accidentalmente, vale a dire in ragione di un errore di interpretazione della realtà delle contrattazioni da parte dell'algoritmo o da un deficit di informazione dello stesso, che ne condiziona le scelte rendendole oggettivamente manipolative. Quest'ultima ipotesi

182 L'espressione è di T.C.W. LIN, *The new market manipulation*, cit., p. 1296. Sulla inadeguatezza della disciplina dei Paesi finanziariamente più avanzati rispetto alle modalità di distorsione cibernetica degli scambi 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.

183 M. LEWIS, *Flash Boys: A Wall Street Revolt*, New York-London, 2014, p. 171.

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

è estranea al campo del penalmente rilevante in considerazione non tanto della mancanza di intenzionalità dell'intelligenza artificiale (in quanto tale inattingibile da connotazioni psicologiche) quanto della persona fisica che se ne sia avvalso: ci troviamo qui al cospetto di una manipolazione colposa, rilevante solo sul piano amministrativo, se si possa rinvenire una mancata prevenzione da parte dell'operatore fisico di errori prevedibili di quello informatico.

È chiaro che, per i risvolti normativi già implementati dai regolatori, per le emergenze pratiche e per le riflessioni della dottrina, il settore dei mercati si pone come campo di studio elettivo. Non può essere indifferente per il penalista, infatti, il dato normativo già esistente. Tra i vari settori in cui l'intelligenza artificiale gioca un ruolo, quello della finanza è il campo in cui il legislatore ha maggiormente esplicato la propria *vis normativa* (anche se certamente non è l'unico[185]). Che sia stata all'altezza delle necessità questo è un diverso piano, tanto che possibili manifestazioni lesive dell'intelligenza artificiale rimangono all'ordine del giorno, come esempi di cronaca recentissima dimostrano[186]. Peraltro, deve incidentalmente rilevarsi che la dimensione trasversale della rischiosità dell'intelligenza artificiale (percepita anche dai non addetti ai lavori[187]) ha ormai spinto a riflettere su una disciplina orizzontale, che offra tutele in settori non finanziari, a rilevanza pubblica e privata[188].

Lasciamo qui programmaticamente in disparte il caso opposto a quello finora considerato, vale a dire quello in cui il sistema di intelligenza artificiale non inganna, ma è ingannato, poiché anche i nuovi algoritmi di intelligenza artificiale che operano sul mercato in modo automatico sono in grado di cogliere i mutamenti artificiosamente sollecitati dagli speculatori, con il rischio di venire fuorviati. Dal punto di vista criminologico, però, questa ipotesi non ha peculiarità spiccate rispetto al caso in cui le persone offese sono operatori umani: l'unica differenza è che l'inganno patito da un *HFT* può tradursi in un numero ben maggiore di atti dispositivi compiuti per effetto dell'errore, con un conseguente danno molto più grave[189].

185 Certamente deve essere menzionato, fuori dalla disciplina dei mercati, l'art. 22 del Reg. UE 2016/679 (c.d. *GDPR*) che, al comma 1, stabilisce: «L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

186 Si veda l'episodio occorso sulle principali piazze europee ai primi di maggio del 2022, su cui 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.

187 Si vedano ad esempio le considerazioni di J. HANSEN, op. cit., nonché il caso descritto da A. LANA, *Alexa sfida una bimba a inserire una moneta nella presa elettrica: Amazon aggiorna il* software, in *Corriere della sera*, 29 dicembre 2021.

188 Il riferimento corre alla già citata Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, reperibile alla seguente url: https://eur-lex.europa.eu

189 D'altra parte, a dispetto del nome, l'intelligenza artificiale non brilla spesso per perspicacia, essendo privo di *common sense*, è stata ribattezzata *artificial stupidity* da P. DOMIGOS, *The Master Algorithm*, New York, 2015, pp. 23 ss., 57 ss. Sui *bias* che affliggono l'AI S. BAROCAS – A.D. SELBST, *Big Data's disparate impact*, in *Cal. Law Rev.*, Vol. 104, 2016, pp. 671 ss.

2 Le aree di rilevanza penalistica dell'intelligenza artificiale in ambito finanziario

Come sopra illustrato, dal punto di vista punitivo, la tipizzazione delle condotte riprovate si riviene agli artt. 184 e 185 TUF, sul versante penale, nonché agli artt. 187-*bis* e 187-*ter* TUF, su quello amministrativo.

Non deve stupire che il riferimento corra anche all'*insider trading* e non già solo alla mera manipolazione del mercato. Certo, è più probabile che l'agente non umano consumi quest'ultimo reato, ma è concepibile anche la creazione, e poi l'abuso, di informazioni privilegiate in ragione delle capacità di analisi ed elaborazione dati che l'operatore algoritmico possiede in qualità enormemente superiore a quella degli intermediari in carne ed ossa: l'agente artificiale sa, per definizione, più dell'uomo e dunque agisce più informato. Ovviamente ci si riferisce alle informazioni circolanti sulla rete e comunque aventi una dimensione informatica, nonché a quelle che si possano ricavare dall'analisi combinata di queste ultime; non certo a quelle che rimangono confinate nella immane concretezza di rapporti confidenziali tra questo e quell'esponente aziendale, alle indiscrezioni *brevi manu* consegnate a un investitore, insomma a fenomeni strettamente riservati che avvengono tra singoli e *off records*, per definizione inaccessibili all'AI, che si muove tra codici binari e si nutre di *byte* (e relativi multipli)[190].

Ma vi è anche un ulteriore profilo da considerare per comprendere perché si debba fare riferimento anche agli art. 184/187-*bis* TUF. L'operatore algoritmico può ben impossessarsi di informazioni dell'istituzione finanziaria cui appartiene e poi impiegarle a profitto della stessa in piena autonomia. Se non adeguatamente sorvegliato, nulla impedisce al programma di interfacciarsi con la struttura che è titolare di dati riservati e infiltrarsi nelle pieghe più recondite della stessa. La sua autonomia non va intesa come semplice automazione: non è mera capacità di svolgere un compito senza un operatore umano, ma indipendenza da istruzioni esterne di azione, libertà da determinazioni altrui. Ciò rende imprevedibili le sue interazioni con l'ambiente circostante cui si tende a adattarsi o che mira a modificare[191]: nulla, dunque, esclude che l'AI possa comportarsi come il più callido dei *raiders* e approfittarsi di dati carpiti all'organizzazione di appartenenza, eludendo ogni controllo.

Se rispetto alla manipolazione del mercato la casistica ha già reso autoevidente la rilevanza dell'intelligenza artificiale malevola, non altrettanto lampante è l'incidenza sull'*insider trading*. Solo poche parole sono sufficienti però per chiarire il tema: basti considerare la conformazione attuale dell'informazione finanziaria ponendola in filigrana con il ruolo giocato dall'intelligenza artificiale nel sistema degli scambi.

Il mercato finanziario è il paradigma della condizione di incertezza situazionale in cui ciascuno è costretto ad agire. Secondo alcuni, la presenza di agenti artificiali

190 Sul punto si veda F. ANNUNZIATA, *Artificial intelligence and market abuse legislation. A European perspective*, cit., pp. 6 e 114.

191 Il dato dell'autonomia viene impiegato di recente per strutturare una tassonomia dei tipi di intelligenza artificiale e di interazione tra agente fisico e artificiale da M. SIMMLER – R. FRISCHKNECHT, *A taxonomy of human–machine collaboration: capturing automation and technical autonomy*, in *Ai & Society*, Vol. 36, 2021, pp. 239 ss.

preclude agli operatori umani di nutrire aspettative fondate di comportamento[192]; al cospetto di transazioni anonime non è dato comprendere chi rappresenti la controparte, e nemmeno se essa sia umana o digitale, né è oggettivamente possibile comprendere in base a quali elementi l'operatore algoritmico si determinerà ad agire e in quale direzione. Con l'avvento degli agenti artificiali ci si potrebbe allontanare dal modello, già per taluni aspetti idealistico, del *level playing field*, cui tende come noto l'intera disciplina *anti insider trading*[193]. La distribuzione disomogenea dell'informazione caratterizza di fatto l'operatività sui mercati finanziari ma la regolamentazione interviene per vietare l'utilizzo di informazioni non ancora pubbliche e per consentire a tutti gli investitori che lo desiderano di accedere (a costi ragionevoli) all'insieme delle informazioni pubblicamente disponibili.

Un'altra considerazione si impone. Non ci si deve far ingannare da una sorta di sineddoche che fa coincidere il tutto (l'intelligenza artificiale) con una sua manifestazione peculiare (gli algoritmi per la negoziazione ad alta frequenza), per quanto quotidiana.

Studi elaborati dall'ESMA evidenziano infatti come a partire soprattutto dal 2018 l'incremento del *trading algoritmico*, con riferimento al mercato azionario europeo (inferiore, per il vero, l'incidenza nel settore obbligazionario e dei derivati), sia del 50-70%[194]. Con riferimento al contesto nazionale, gli scambi riconducibili agli *High frequency traders* nel Mercato Telematico Azionario (MTA) si sono attestati nel periodo 2016 – 2019 intorno al 30% del totale degli scambi conclusi, con una contrazione nell'ultimo anno di riferimento al 26%[195].

Non è questa la sede per tipizzare le condotte manipolative rese possibili dalla tecnologia degli *HFT*, non solo perché ormai già compiuta dalla prassi e da Autori che se ne sono occupati in precedenza[196], ma anche perché gli algoritmi ad alta frequenza sono le forme di intelligenza non umana ormai più note e studiate. Vi sono invece ulteriori e vari autori artificiali che possono turbare gli scambi di cui ancora poco si è detto nel campo del diritto penale dell'economia e su cui conviene riflettere.

192 Lo nota S.R. McNamara, *The Law and Ethics of High-Frequency Trading*, in *Minn. J.L. Sci. & Tech.*, Vol. 17, Issue 1, 2016, pp. 135 ss.

193 Si vedano le considerazioni in ordine a questo concetto di 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; in giurisprudenza resta fondamentale Sec. Exch. Comm'n u. Texas Gulf Sulphur Co., 401 F.2d 833, 852 (2d Cir. 1968), che reiteratamente evidenzia come lo scopo della legislazione in materia è che «*all members of the investing public should be subject to identical market risks*». Sulla difficoltà di adeguare la realtà dei mercati all'ideale politico-criminale si veda la scettica presa di posizione della giurisprudenza 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 nonpublic information is unchecked by law*».

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

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

196 Di recente una tassonomia è tracciata da G. Ruta, *op. cit.*, pp. 65 ss., in precedenza noi stessi ne avevamo trattato in F. Consulich, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, cit., pp. 195 ss.

Nel campo del c.d. *Fintech* (etichetta quanto mai in evoluzione), tra i principali ambiti di applicazione, oltre alla negoziazione ad alta frequenza, si può fare riferimento alle piattaforme non regolamentate di scambio che, in combinato disposto con i condizionamenti dei social media, attraverso un meccanismo diffusivo esponenziale, possono produrre rilevanti effetti distorsivi sugli scambi.

Siamo su un piano in cui l'operatività si compenetra con la comunicazione, poiché il *social media* può essere luogo di scambio o luogo di discussione in ordine allo scambio.

Di qui il ruolo duplice degli strumenti di intelligenza artificiale, poiché oltre a vettori di transazioni manipolative, essi possono essere utilizzati per diffondere notizie false e così influenzare, dall'esterno del mercato, il corso dei titoli. In particolare, attraverso i c.d. «*Bots*» (programmi che operano autonomamente in rete) informazioni non veritiere su società quotate possono essere ripetute molteplici volte e influenzare il *sentiment* intorno l'azienda stessa o uno strumento finanziario.

Sono proprio episodi recenti, che hanno raggiunto l'apice alla fine di gennaio 2021, ad aver dimostrato come una volatilità molto elevata di alcuni titoli statunitensi, legata a un significativo accumulo di posizioni corte, sia stata indotta da un comportamento complessivamente coerente di investitori al dettaglio. Influenzati e limitati nelle opzioni di comportamento da informazioni condivise sui *social media*, costoro si sono mossi quasi fossero un unico centro di interesse[197].

Fenomeni di condizionamento all'investimento sono tanto più frequenti quanto più è facile quando gli scambi vengano de-istituzionalizzati, cioè siano collocati ad esempio nelle cc.dd. piattaforme di *trading*[198]. Accessibili tramite semplici applicazioni dedicate ai dispositivi di tipo mobile, espongono i clienti al dettaglio ad una manovra 'a tenaglia', da una parte si somministrano consigli su come investire, dall'altra, dopo pochi 'clic', si può agevolmente iniziare a fare investimenti[199].

Si manifestano altresì anche in ipotesi di consulenza *online* operata da *robo advisor*, prima e a prescindere dalla somministrazione di un'infrastruttura atta a compiere negoziazioni.

Il tema dell'impatto di *social media* e piattaforme non regolamentate nello svolgimento di operazioni di *trading* è, come visto, strettamente collegato alla realizzazione di consulenze *online*, idonee ad incidere sulla determinazione degli investitori potenzialmente al di fuori di ogni controllo.

197 Per una ragionata sollecitazione alla riflessione sul punto, nella nostra dottrina, G. RUTA, *op. cit.*, 61 ss.

198 La "piattaforma di trading" non è una "sede di negoziazione". Non si tratta né di un sistema multilaterale di negoziazione – MTF, né di sistema organizzato di negoziazione – OTF, né tantomeno di mercati regolamentati, ma di uno strumento informatico inserito nella struttura di *broker/dealer* autorizzati, che li impiegano nell'interazione con la clientela e che consentono di veicolare il flusso di ordini verso le sedi di negoziazione e/o le controparti, attraverso algoritmi che verificano le condizioni migliori per la successiva esecuzione.

199 Sia ESMA, che CONSOB, hanno già dedicato la loro attenzione al fenomeno, per il potenziale di rischio che incamerano dal punto di vista della manipolazione per il tramite di investitori non adeguatamente informati, cfr., rispettivamente, ESMA, Statement, 17 febbraio 2021, in https://www.esma.europa.eu e la "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.

In questa prospettiva, va segnalato che nell'agosto del 2021 la SEC ha lanciato una pubblica richiesta di informazioni in merito all'utilizzo delle piattaforme digitali per gli investimenti, ai cc.dd. *broker online* e ai *robo-advisor*[200].

È chiaro allora che le fattispecie penali destinate a subire l'impatto dell'*artificial agency* nei prossimi anni sono quelle di abusivismo finanziario, alla luce di quanto appena rilevato, nonché di abuso di informazioni privilegiate e manipolazione del mercato.

3 Asimmetrie tecnologiche e informazione societaria

Si è sempre pensato che la rilevanza delle transazioni ad alta frequenza fosse ristretta ai fenomeni di aggiotaggio, ma ad un'analisi più attenta deve rilevarsi che una simile prospettiva rischia di essere parziale.

Occorre prendere le mosse dalla constatazione che l'*HFT* sfrutta ogni possibile oscillazione dei prezzi dei titoli quotati e proprio per questo si potrebbe dire che i traders algoritmici guardino solo alle variazioni numeriche delle quotazioni dei titoli, effettuando scelte di investimento disinteressate rispetto al c.d. valore fondamentale degli strumenti finanziari[201].

Il primo paradosso che si incontra riflettendo sul rapporto tra algoritmi ad alta frequenza e mercati è che tali operatori, pur effettuando una parte cospicua degli scambi di titoli quotati, sono influenzati in misura nulla o del tutto limitata dai dati disponibili riguardo agli strumenti finanziari oggetto di investimento, ai loro emittenti, nonché al mercato in generale, infatti, il brevissimo orizzonte temporale delle posizioni che aprono difficilmente potrebbe risentire di tali informazioni; anzi, se si presenta il rischio che ne risentano, allora essi preferiscono ritrarsi[202]. In sintesi: l'informazione finanziaria societaria e macroeconomica è una variabile trascurabile per una cospicua parte degli operatori finanziari, ovvero quelli algoritmici ad alta frequenza.

La sensibilità degli *HFT* al flusso informativo concernente il singolo strumento finanziario ovvero l'andamento generale delle contrattazioni dipende, infatti, dalla tipologia di algoritmo impiegato per la definizione delle scelte di acquisto e vendita.

200 Il testo è reperibile all'indirizzo https://www.sec.gov/rules/other/2021/34-92766.pdf. Nello specifico, la SECURITIES AND EXCHANGE COMMISSION ha richiesto informazioni e commenti pubblici su questioni relative a: *broker-dealer* e consulenti per gli investimenti, utilizzo di pratiche di coinvolgimento digitale, inclusi suggerimenti comportamentali, marketing differenziale, funzionalità simili a giochi (si assiste qui alla cd. *gamification* dell'investimento) e altri elementi di progettazione o funzionalità per interagire con gli investitori al dettaglio su piattaforme digitali (ad esempio, siti *web*, portali e applicazioni), nonché gli strumenti e i metodi analitici e tecnologici utilizzati in relazione a tali pratiche di coinvolgimento digitale; nonché, appunto, sull'uso della tecnologia da parte di un consulente per gli investimenti per sviluppare e fornire consulenza in materia.

201 Deve ammettersi che questa caratteristica è propria anche di alcuni investitori non algoritmici come i *day traders*, i *market makers* e così via, ma mentre per questi ultimi è una possibile attitudine, per gli *HFT* è una costante strutturale.

202 Numerose verifiche empiriche hanno mostrato come l'operatività degli *HFT* si riduca sensibilmente nei minuti in cui è attesa la pubblicazione di informazioni macroeconomiche (AMF, *Study of the behaviour of high frequency traders in Euronext Paris*, Risks & Trends, January 2017, p. 12).

Ciò posto, in prospettiva, non si può eludere l'interrogativo in ordine all'impatto che la presenza così invasiva di operatori algoritmici negli scambi finanziari ad alta e bassa frequenza possa avere sulla nozione di informazione finanziaria, anche per il tramite della trasmutazione della figura dell'investitore ragionevole: ad essere coinvolte potrebbero essere le stesse architravi della tutela penale contro gli abusi di mercato.

L'interrogativo è analogo a quello che si pone con preoccupazione quando si immagina, sul piano sociologico, che pochi grandi intermediari possano guidare l'andamento dei mercati a loro piacimento compromettendo quella "democrazia dei mercati" che, "votando ogni giorno", restituisce alle varie attività il loro giusto valore. Ed è analogo a quello che, di recente, si pone la letteratura economico-finanziaria quando rileva che a livello globale pochi grandi investitori istituzionali hanno posizioni capaci di indirizzare le principali *public companies* e quindi l'economia reale del pianeta[203].

Ma l'interrogativo è decisamente più inquietante. Mentre, infatti, le valutazioni dei suddetti intermediari e investitori istituzionali devono essere in qualche misura legate, in via antropica, ad una stima dei fondamentali, che, per quanto molto soggettiva, elitaria o di comodo, difficilmente può essere meramente arbitraria, quanto meno perché deve essere accompagnata da una narrativa persuasiva, quelle valutazioni generate dagli operatori algoritmici possono, invece, davvero essere arbitrarie o apparire ragionevolmente tali, posto che, anche volutamente, tali operatori rifiutano l'informazione finanziaria ma restano pronti a investire in modo massiccio nella direzione indicata da una incomprensibile rete neurale o, come si è visto sopra, da più reti neurali che rispondono, in modo involontariamente coordinato, ai medesimi *inputs*, fornendo poi al pubblico, di ritorno, una informazione finanziaria priva di contenuti valoriali o, comunque, se pure esistenti, non possono essere rappresentati, narrati e, quindi, in ultima analisi, neanche apprezzati o criticati.

3.1 Il volto attuale dell'investitore ragionevole e la 'trappola' della competenza: alla ricerca dell'informazione finanziaria nei mercati contemporanei

Il diritto del mercato finanziario si basa sull'assunto che l'informazione rilevante sia quella che motivi all'azione l'investitore ragionevole, ponendosi a fondamento delle sue determinazioni.

La correlazione versa oggi in una condizione di stallo poiché, come noto, la nozione di *reasonable investor* è alquanto tormentata, posto che è ben difficile trovare un punto di accordo nell'universo degli Autori che si sono occupati del tema[204]. Segnalano in molti, soprattutto dal versante statunitense come, benché ci si trovi di fronte

203 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.

204 Tra i miti del mercato mobiliare rientrano a pieno titolo le nozioni di investitore medio e di investitore ragionevole, per tutti, H. Kripke, *The Mith of Informed Layman*, in *Bus. Law.*, Vol. 2, n. 2, 1973, pp. 631 ss.; di recente B. Black, *Behavioral Economics and Investor Protection: Reasonable Investors, Efficient Markets*, in *Loyola U. Chi. L. J.*, Vol. 44, 2013, pp. 1494 ss.

ad una figura anonima e sfuggente, per non dire misteriosa ed elusiva, la descrizione più accreditata di tale soggetto dovrebbe essere quella di un *homo economicus*, di stampo neoclassico[205], con connotati dell'investitore di lungo periodo e non dello *short trader*[206].

Secondo altri, il paradigma da ultimo accennato sarebbe del tutto irrealistico e quindi inutile; meglio sarebbe sollecitare l'emersione di un nuovo modello ermeneutico dei mercati finanziari, quello dell'investitore irrazionale, che non comprende a pieno le informazioni finanziarie, che si fa influenzare da fattori irrilevanti ed è condizionato da emozioni e pregiudizi[207].

Si è tentato di ricomporre la radicale dicotomia attraverso un nuovo schema esplicativo, quello dell''investitore senza qualità', strutturalmente meglio informato di un investitore occasionale ed irrazionale, ma certo non in grado di dominare la grande mole di dati che riceve; sempre più veloce nelle proprie decisioni di investimento grazie ad un crescente supporto tecnologico, tale operatore non è immune da pulsioni imitative non meditate, soprattutto di fronte a particolari scenari di mercato (si pensi a massicci crolli degli indici o a improvvise impennate dei titoli); pur tentando di diversificare i propri investimenti, egli è comunque consapevole dei propri limiti emotivi[208].

Ciò che è certo è che una nozione monolitica di investitore ragionevole non ha alcun contenuto informativo rispetto alla realtà dei mercati finanziari e rischia di decentrare la tutela penale rispetto alle esigenze di tutela effettive, generando una disciplina insoddisfacente sia rispetto alle pretese di protezione degli investitori professionali (in qualche modo sottostimati nelle loro capacità), sia per quelle dei piccoli investitori (al contrario sovrastimati nelle proprie competenze)[209].

Questo scenario, già di per sé assai problematico, è ulteriormente stressato dal crescente ruolo rivestito negli ultimi anni dagli operatori algoritmici; prescindere dalla loro considerazione rischia di condurre alla costruzione della nozione di investitore ragionevole ancora più mitologica e inafferrabile, se intesa come personificazione di aspettative di informazione nutrite da singole e occasionali controparti negoziali dell'iniziato: tali soggetti possono, al pari degli operatori umani, essere molto eterogenei tra loro per obiettivi perseguiti, conoscenze iniziali e competenze specifiche per

205 In questo senso 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.

206 Così T.C.W. LIN, *The New Investor*, in *UCLA L. Rev.*, Vol. 60, 2013, p. 695.

207 Sul punto 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 ss.

208 Per un riassunto di tali attributi dell'investitore moderno, tale da farlo assomigliare ad un "*modest cyborg*", T.C.W. LIN, *The New Investor*, cit., pp. 700 ss.

209 Alla luce di tali notazioni, pur esorbitando dalle finalità del presente contributo, si segnala solo che, *de lege ferenda*, il legislatore dovrebbe forse impostare la disciplina dei mercati finanziari consapevole dell'esistenza di almeno tre grandi classi di investitori, al fine di approntare una tutela penale realistica e maggiormente fedele al sostrato empirico di riferimento e alle esigenze di tutela che da questo emergono.

comporre una figura di sintesi cui parametrare le qualità dell'informazione privilegiata[210].

Spesso, la decisione di investimento è infatti il frutto della imprevedibile 'reazione' tra le caratteristiche intrinseche dell'informazione e le conoscenze proprie del destinatario che ne prende contezza. L'art. 181, comma 4, TUF, anche alla luce della legislazione eurounitaria (in particolare art. 7, par. 4, del Regolamento (UE) *MAR*), infatti, pare chiaro nell'indicare l'informazione privilegiata come uno degli elementi, non dunque l'unico, che l'investitore ragionevole può assumere a base delle proprie decisioni, anche nel caso in cui da sola la notizia non avrebbe avuto la forza sufficiente a determinare una decisione di investimento[211].

Può scorgersi un'immediata correlazione di proporzionalità diretta: al crescere delle capacità e conoscenze dell'operatore che acquisisce la notizia corrisponde l'aumento del novero delle informazioni che, inutili per un investitore comune non particolarmente qualificato, sono, invece, assai rilevanti per le scelte di investimento di quello ipercompetente, in grado cioè di cogliere l'importanza di informazioni a prima vista trascurabili[212]. D'altra parte, a conferma, si tenga presente che l'investitore ragionevole non è l'investitore medio, sicché ben possono qualificarsi *price sensitive* le informazioni che sono rilevanti solo per una minoranza di investitori, se queste sono in grado di influenzare i prezzi[213].

Di qui, si intravedono le premesse di una vera e propria 'anafilassi' per il diritto dei mercati. Se la maggiore competenza induce la genesi di nuove informazioni privilegiate, è presto detto ciò che può accadere rispetto ad un soggetto dotato di capacità di analisi incomparabilmente superiore a quella di qualsiasi operatore professionale umano, quale un operatore algoritmico di seconda generazione: l'ampliamento incon-

210 Per un'analisi della nozione di investitore ragionevole alla luce degli ultimi interventi del legislatore eurounitario in materia 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 ss. Nella sterminata letteratura in argomento, si segnalano in questa sede, del tutto curiosamente, una serie di recenti contributi che nella letteratura statunitense pongono in discussione, fin dalle radici, l'adeguatezza del concetto in considerazione della diversificazione, in termini di competenze, tra gli investitori; si veda T.C.W. LIN, *Vistas of Finance*, in *UCLA L. Rev. Disc.*, Vol. 61, 2013, pp. 78 ss.; ID., *The New Investor*, cit.; S.M. BAINBRIDGE, *The New Investor Cliffhanger*, in *UCLA L. Rev. Disc.*, Vol. 61, 2013, pp. 678 ss.; B. BLACK, *Behavioral Economics and Investor Protection: Reasonable Investors, Efficient Markets*, in *Loy. U. Chi. L.J.*, Vol. 44, 2013, pp. 1493 ss.; J. MACLEOD HEMINWAY, *op. cit.*, pp. 291, 297. Definisce quello di investitore ragionevole come una delle nozioni nucleo della regolazione dei mercati finanziari D.A. HOFFMAN, *The "Duty" to Be a Rational Shareholder*, in *Minn. L. Rev.*, Vol. 90, 2006, pp. 537, 537-39. Per una recente ricognizione giurisprudenziale T.M. MADDEN, *Significance and the Materiality Tautology*, in *J. Bus. & Tech. L.*, Vol. 10, 2015, pp. 217 ss.

211 Sul punto, si vedano 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, e F. MUCCIARELLI, *Sub art. 184*, in M. FRATINI – G. GASPARRI (a cura di), *Il testo unico della finanza*, Torino, 2012, p. 2338.

212 In questo senso, ad esempio, F. DENOZZA, *La nozione di informazione privilegiata tra "*Shareholder Value*" e "*Socially Responsible Investing*"*, in *Giur. comm.*, n. 5, 2005, pp. 593 ss., e F. ANNUNZIATA, *Abusi di mercato e tutela del risparmio*, Torino, 2006, 15. Rileva conseguentemente G. STRAMPELLI, *L'informazione societaria*, cit., p. 1037, che devono formare oggetto di *disclosure* anche le informazioni considerate *price sensitive* solo da una minoranza di investitori, se costoro sono in grado con la propria condotta di influenzare i prezzi.

213 Sia consentito il rinvio a F. CONSULICH – F. MUCCIARELLI, *Informazione e tutela penale dei mercati finanziari nello specchio della normativa eurounitaria sugli abusi di mercato*, cit., pp. 184 ss.

trollabile della *price sensitivity* dell'informazione, e dunque della nozione di informazione privilegiata, con la conseguente proliferazione delle occasioni di abuso della stessa[214].

Il tema si è già posto a livello globale con l'ascesa degli *hedge fund*, i quali, con le loro sofisticate capacità di analisi e di valorizzazione di informazioni, dati e aspetti apparentemente trascurabili per molti analisti finanziari e per le stesse società quotate, riescono a conseguire cospicui profitti. La soluzione regolamentare negli Stati Uniti e nell'Unione europea è stata quella di obbligare le società a rendere pubbliche le eventuali informazioni fornite in incontri bilaterali o ristretti[215].

Si tenga presente che tali obblighi per gli emittenti comportano per gli stessi nuovi oneri: di individuazione e di gestione di tali dettagli informativi onde evitare che arrivino in modo selettivo agli *hedge fund*.

Orbene, con l'avvento di *big data* e *alternative data*, cioè con la disponibilità di una abnorme massa di dati e informazioni di dettaglio su scala globale, le possibilità di profitto per le strategie di *trading* algoritmico che si basano su correlazioni nascoste tra tali informazioni di dettaglio aumentano significativamente e portano, di converso, nuovi oneri per le società quotate che intendano conformarsi (volontariamente?) alle regole di *fair disclosure* verso il mondo degli investitori. Informazioni quali il numero di ore lavorate in un'area geografica, il consumo di energia di uno stabilimento, il numero di clienti acquisiti giornalmente nei vari punti vendita, ecc. potrebbero ben essere utilizzati per estrapolare *trend* e predire i risultati trimestrali di una società quotata o di un settore o di settori appartenenti alla stessa *supply-chain*.

L'espansione dell'informazione *price sensitive* può dunque volgersi, in breve tempo, in un'ipertrofia incontrollabile dei doveri di comunicazione e astensione che sostanziano la disciplina degli abusi di informazione privilegiata, onerando gli operatori di tali e tanti adempimenti da rendere impossibile ogni operazione economica senza una giustificazione razionale, posto che le informazioni considerate dagli algoritmi sono spesso prive di rilevanza economica e attengono, ad esempio, a episodici e rapidissimi disallineamenti di prezzo tra domanda ed offerta di un titolo, di valore per altro per lo più infinitesimo.

Si pensi ancora a cosa accadrebbe se si dovesse imporre l'obbligo di comunicazione o di *fair disclosure* o il divieto di operare in relazione ad informazioni del tutto trascurabili, eppure rilevanti per i soli algoritmi, come la ricorrenza di una data parola o gruppo di termini nel contesto dei sistemi informativi di mercato.

Una delle fenomenologie più note del *trading* ad alta frequenza è, infatti, il c.d. *trading on news*, che può essere commesso sfruttando il continuo flusso informativo dei principali servizi di informazione finanziaria. L'*HFT* è in grado di associare una strategia di *trading* a determinati gruppi di parole che statisticamente sono correlate a un preciso andamento delle contrattazioni, sia in positivo che in negativo, declinando

214 Il punto è notato da G. STRAMPELLI, *L'informazione societaria*, cit., p. 1038.

215 Art. 17, par. 8, MAR.

le strategie secondo la risonanza della notizia, quantificata, ad esempio, verificando quante volte la notizia viene riportata nei sistemi informativi[216].

Ecco, quindi, che l'innalzamento della competenza di analisi degli operatori può chiudere la disciplina *anti – insider trading* in una vera e propria trappola: determinare l'emersione di informazioni rilevanti (per alcuni intermediari assai importanti per l'andamento delle quotazioni, quelli algoritmici ad alta frequenza), ma non ragionevoli, perché del tutto indipendenti da profili di meritevolezza economica dell'oggetto della transazione.

Presto detto allora l'effetto che determina l'ingresso degli operatori algoritmici sull'informazione finanziaria, con particolare riferimento alla nozione di informazione privilegiata: l'emersione di informazioni *price sensitive*, vale a dire in grado di influire sui prezzi perché importanti per gli *HFT*, ma non ragionevoli, in quanto (sia pure solo apparentemente) prive di qualità economica, potendo non essere (per quanto noto) correlate al valore del titolo, alla struttura dell'emittente o alle condizioni del mercato di riferimento.

3.2 La nascita dell'informazione *price sensitive but not reasonable*

Gli *HFT*, ma anche i sistemi di *deep learning* a bassa frequenza[217], si relazionano con il concetto di informazione in due modi:

1) scoprono informazioni nuove: sono *information producers* e proprio per questo si procurano occasioni di *front running* basate su asimmetrie informative dovute alla maggiore capacità di analisi e operative[218]; gli algoritmi cc.dd. di seconda generazione sono in grado di rielaborare un ingente numero di dati, attingendo a tal fine ai circuiti informatizzati di diffusione di notizie e, dunque, creano nuovi scenari di mercato di cui per primi vengono a conoscenza. Si pensa spesso all'*insider* come un soggetto occasionalmente coinvolto nel processo di produzione di un'informazione privilegiata, in funzione di una contingente posizione di vantaggio ricoperta; gli operatori algoritmici rientrano invece tra i cc.dd. *insiders* strutturali,

216 Sul *trading on news* si veda ad esempio A. Puorro, *op. cit.*, p. 16.

217 Il c.d. *deep learning* è una sottocategoria del *machine learning* (che letteralmente viene tradotto come apprendimento automatico) e indica quella branca dell'intelligenza artificiale che ricorre ad algoritmi ispirati alla struttura e alla funzione del cervello. Siamo qui al cospetto di vere e proprie reti neurali artificiali e vi si ricorre ad esempio nei programmi di riconoscimento automatico della lingua parlata, nell'elaborazione del linguaggio naturale, nel riconoscimento audio e nella bioinformatica.

218 Per un approfondito studio su un modello predatorio di operatività degli *HFT* basato sul *front running*, ovvero sulla possibilità che gli *HFT* hanno di agire prima degli altri operatori, profittando della conoscenza anticipata di un ampio ordine di acquisto o vendita su un mercato, grazie alla maggiore velocità di acquisizione ed elaborazione di informazioni rispetto ad ogni altro operatore, 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 ss., nonché, più di recente 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, che segnala il collegamento tra la volatilità delle quotazioni e strategie predatorie degli HFT che determinano prezzi di vendita o acquisto più bassi o più alti senza alcuna logica razionale.

che sono cioè tali per il solo fatto di esistere con le caratteristiche di acquisizione ed elaborazione di *big data* che li caratterizzano[219];

2) impiegano spesso, sul presupposto che siano economicamente rilevanti, informazioni del tutto trascurabili per gli investitori 'fisici': sono *information consumers*.

Per quanto già espresso nei paragrafi 3 e 3.1, gli operatori algoritmici di seconda generazione, proprio per la circostanza di effettuare molte operazioni che non sono informative (la loro attività è paragonabile spesso ad uno spasmo del mercato, piuttosto che ad un'azione cosciente), non veicolano informazioni significative in ordine al valore intrinseco dei titoli scambiati. Rischia, così, di andare in frantumi il postulato del diritto dei mercati finanziari contemporaneo secondo cui le operazioni e, più in generale, i comportamenti degli investitori siano al contempo informazioni[220], cioè rechino con sé una traccia utile ad interpretare il contesto di riferimento per l'osservatore ragionevole che guarda a quella transazione. Il ritiro degli investitori 'ordinari' da mercati che percepiscano come tiranneggiati da operatori 'diversi' strutturalmente è un rischio più che concreto[221].

Come detto, gli *HFT* operano, infatti, sulla base di analisi matematiche quantitative attinenti alle oscillazioni dello strumento finanziario in un dato periodo oppure ancora alla ricorrenza del nome dell'emittente sui mezzi di informazione del settore: si potrebbe trattare di informazioni del tutto inconferenti rispetto alle variabili economiche rilevanti per un operatore professionale. In generale, come detto, l'*HFT* non ha alcuna prospettiva sul lungo termine, ma mira a sfruttare i movimenti di brevissimo periodo di un titolo per lucrare sull'anticipazione degli stessi, senza dare alcun peso alle prospettive di crescita dell'emittente o del mercato, né ai valori economici di fondo. Naturalmente occorre rifuggire da affermazioni troppo categoriche, dato che un'intelligenza artificiale 'ben sorvegliata' potrebbe certo veicolare una maggiore efficienza allocativa sui mercati, ma non può negarsi il rischio che gli algoritmi possano determinare, se imitati dagli operatori professionali, una complessiva degradazione della qualità delle transazioni, nel quadro di un più ampio fenomeno di allontanamento del prezzo di scambio dall'intrinseco valore dei titoli[222].

Il problema è ben conosciuto dagli stessi operatori finanziari, a tal punto che, per evitare di essere captati ed imitati da algoritmi ad altra frequenza, ormai frequentemente tendono ad allontanarsi dal mercato istituzionale per operare su piattaforme di negoziazione a basso tasso di trasparenza (i cc.dd. *Dark pools*), in cui chi opera non

219 Sulla presenza di *Structural insiders* nei mercati contaminati dalla contrattazione algoritmica Y. YADAV, *Insider Trading and Market Structure*, in *UCLA L. Rev.*, Vol. 63, 2016, pp. 978 ss., 1013 ss., che evidenzia (1032) come la contemporanea disciplina dell'abuso di informazioni privilegiata sia oggi messa in profonda crisi dagli operatori algoritmici che, oltre a sicuri benefici agli scambi, causano però danni molto simili al convenzionale *insider trading* compiuto dalle persone fisiche. Altri tipi di *insider* strutturali possono essere gli intermediari che eseguono ordini di elevata dimensione, i consulenti di operazioni di M&A, i *top manager* delle società quotate.

220 Il punto è ben focalizzato, ad esempio in G. STRAMPELLI, *L'informazione societaria*, cit., p. 998 e 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 ss. Sulla teoria per cui i mercati rappresentano lo strumento più efficiente per aggregare informazioni disperse tra i consociati F.A. HAYEK, *The Use of Knowledge in Society*, in *The Amer. Econ. Rev.*, Vol. 35, n. 4, 1945, pp. 519-211.

221 Sul punto T.C.W. LIN, *Reasonable Investor(s)*, in *Boston Univ. L. Rev.*, Vol. 95, 2015, pp. 461 ss.

222 Su cui H.T.C. HU, *Too Complex to Depict?*, cit., p. 1707.

è tenuto a comunicare agli altri operatori una serie di dati *pre-trading* ed in generale qualsiasi informazione che possa rappresentare un indizio in ordine alla propria strategia di negoziazione[223].

È, dunque, evidente che la massiccia presenza di operatori algoritmici potrebbe richiedere la predisposizione di una disciplina *ad hoc*, diversa a quella attualmente apprestata dai legislatori nazionali perché basata su postulati diversi da quelli finora condivisi.

Si rende allora opportuno riflettere, *de lege ferenda*, sulla introduzione di una normativa specificamente diretta a regolare la responsabilità derivante dall'impiego di tale tipologia di strumenti e a disciplinarne l'operatività, prendendo le mosse:

i) dalla difficoltà di adottare una nozione onnicomprensiva di investitore ragionevole per definire gli obblighi informativi per gli emittenti, a causa della granularità delle informazioni che possono rilevare per l'operatività degli algoritmi;

ii) dall'ignoto "ragionamento" che porta i sistemi di AI forti a valorizzare nella loro operatività tali informazioni, e della difficoltà di recuperare tale ragionamento *ex post*;

iii) dalla possibile dissociazione tra azione di mercato e informazione finanziaria, in considerazione i) della capacità, specie per l'*HFT*, di 'scindere' l'operazione dall'informazione, ostacolando il processo di incorporazione nei prezzi delle informazioni disponibili (secondo la nota teorica della *efficient capital markets hypothesis*) e ii) del progressivo prevalere dell'operatività dei sistemi di AI nei mercati finanziari[224].

4 Il ruolo del diritto penale nella regolazione dell'intelligenza artificiale

Al cospetto di uno scenario di rischio così marcato per l'investitore che interagisca con forme di intelligenza artificiale (spesso nemmeno percepito dalle potenziali vittime), è stato formulato da più parti, a livello internazionale e domestico, l'auspicio che il diritto proceda ad un controllo più severo, che giunga anche all'impiego del diritto penale[225].

223 Sul fenomeno G. STRAMPELLI, *L'informazione societaria*, cit., p. 1000; da ultimo J. Adrian, *op. cit.*, p. 264; in precedenza, il fondamentale contributo di M.J. MCGOWAN, *op. cit.*, p. 38, che stimava, già nel 2010, in 40 i *dark pools* operativi; Brown, Chasing the Same Signals, cit., 116. Ancora T.C.W. LIN, *The New Investor*, cit., p. 690 ss. e più di recente, sulla sfida per i regolatori rappresentato dalla presenza di c.d. *private electronic venues*, ID., *The New Market Manipulation*, cit.

224 Si rimanda all'essenziale contributo di E.F. FAMA, *Efficient Capital Markets. A Review of Theory and Empirical Work*, in *Journal of Finance*, Vol. 25, 1970, pp. 373 ss.; sulla capacità degli *HFT* di interrompere il processo di assimilazione delle informazioni finanziarie nei prezzi Z. GOSHEN – G. PARCHOMOVSKY, *The Essential Role of Securities Regulation*, in *Duke L.J.*, Vol. 55, 2006, pp. 733 ss.

225 Il problema è l'identificazione del responsabile in presenza di sistemi di AI che autoapprendano, come rilevato da E. HILGENDORF, *Autonome Systeme, künstliche Intelligenz und Roboter*, in *Festschrift für Thomas Fischer*, München, 2018, pp. 111 ss. Che uno dei profili più problematici dell'AI sia quello dell'autonomia dei programmi che si adeguano al contesto per il tramite del mutamento delle loro caratteristiche di azione G. COMANDÈ, *op. cit.*, p. 172. È proprio sull'autonomia del robot che pone l'accento, al considerando AA, la Risoluzione recante raccomandazioni alla Commissione

La prospettiva penalistica è però tutt'altro che di facile adozione; il personalismo che la caratterizza, con riguardo al disvalore dei fatti repressi, che dei principi di garanzia che la connotano (almeno negli ordinamenti democratici), si rivela incompatibile con la fenomenologia delle offese all'investimento. La sfida è dunque impegnativa per i legislatori contemporanei e impone un approfondimento per comprendere se si tratti di ostacoli che possono essere aggirati, seppure con fatica, o se invece siano del tutto insuperabili.

È bene parlare di ostacoli (al plurale) non solo perché sono numerosi, ma soprattutto perché hanno ben diversa consistenza e morfologia, a seconda della posizione che il diritto adotti al cospetto di una scelta di fondo. Prima di procedere ad un intervento penalistico, occorre infatti sciogliere una alternativa radicale: se l'agente artificiale sia o non sia un soggetto capace di responsabilità giuridica prima che strettamente penalistica.

4.1 La prospettiva 'evoluzionistica': la responsabilità penale diretta dell'agente artificiale

In una prospettiva già accennata, si potrebbe ritenere che i destinatari dei precetti penali non rappresentino un numero chiuso, ma siano destinati, quasi naturalmente, a crescere al mutare della società: prima gli individui, poi gli enti, infine gli agenti artificiali. Se si prendesse la via di una responsabilizzazione dell'intelligenza artificiale la strada sarebbe però in salita. Prima di tutto, come si può concepire, anche solo in chiave normativa, l'idea di una colpevolezza di questa entità[226]?

Se volessimo ricorrere ad una sanzione senza colpevolezza, ricorrendo ad una imputazione puramente oggettiva, opzione ben possibile visto che nessun diritto costituzionale potrebbe impedire simile modello rispetto all'AI, il problema immediatamente successivo sarebbe quello del sicuro effetto *spillover*[227]. Un simile destinatario non ha certo risorse economiche proprie cui attingere e se anche ci si limitasse ad interdirne in tutto o in parte l'attività, ne patirebbero le conseguenze i suoi utilizzatori.

Oltre a ciò, vi sarebbe una ben più radicale criticità.

Per gli Agenti artificiali è logicamente impossibile parlare di punizione e quindi di un diritto che lo disciplini. È pena l'inflizione di una qualche forma di sofferenza alla luce di procedure legali a seguito di un'offesa legalmente riconosciuta[228],

concernenti norme di diritto civile sulla robotica (2015/2013 INL). Sui limiti etici alla ricerca nel campo dell'intelligenza artificiale si vedano anche le linee guida della commissione europea, *Ethics Guidelines for Trustworthy AI*, 2018, p. 12 e, nel contesto della cd. grande Europa, *Responsibility and IA*, Council of Europe Study 2019.

226 Scettici anche R. Abbott – A. Sarch, *op. cit.*, p. 327.

227 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.

228 Sulla necessità che si sia della sofferenza o conseguenze normalmente considerate spiacevoli affinché ci sia una pena H.L.A. Hart, *Punishment and Responsibility: Essays in the Philosophy of Law*, Oxford, 2008, p. 4.

ma è impossibile che l'AI, qualsiasi esso sia, possa percepire anche solo una vaga diminuzione di diritti o limitazione del proprio status sociale a seguito della sanzione[229]. In difetto di questa componente, ben prima della colpevolezza, è impossibile definire e poi rispettare un vincolo di proporzione che segni la pena 'meritata' dall'AI, non esiste in somma un *malum passionis* da bilanciare con il *malum actionis*.

Quello che volesse rivolgersi all'intelligenza artificiale sarebbe un diritto penale che dovrebbe rinunciare a sé stesso, almeno nella versione costituzionale della penalità che abbiamo conquistato nelle democrazie occidentali (è ben vero che nelle esperienze anglosassoni sopravvivono ancora forme di *strict liability*, ma si tratta di ipotesi in remissione e per illeciti di minima gravità[230]).

Non sarebbe, dunque, solo oggettivo, ma anche deprivato da ogni possibilità di afflizione dei destinatari. Ci troveremmo di fronte a un meccanismo meramente ripristinatorio ed automatico che mirerebbe a reagire ad un danno causato dell'AI, dunque un diritto intrinsecamente civilistico, pur se formalmente qualificato come criminale (si dovrebbe qui invocare una sorta di *matière civile*, parafrasando il lessico convenzionale).

Solo un legislatore intenzionato a impiegare un diritto simbolico per scopi di consenso privilegerebbe l'etichetta penale, alla luce di un malriposto uso dell'AI come vero e proprio 'capro espiatorio elettronico'.

Per mera completezza, e come mera conseguenza del deficit di colpevolezza e percezione della sanzione, anche dal punto di vista degli scopi della 'punizione' si possono svolgere brevi considerazioni.

Ad esempio, dal punto di vista della prevenzione generale intimidatrice: la deterrenza è un meccanismo che potrebbe essere attivato dalla minaccia di pena solo se l'AI fosse stata costruita per rendersene conto e compiere delle valutazioni di costo-opportunità in relazione alle azioni che abbia in programma di intraprendere.

Virando sulla prevenzione speciale, la riconversione dell'agente artificiale al rispetto dei valori violati non pare possibile se non attraverso una riprogrammazione forzosa (ben lungi, dunque, dal paradigma della rieducazione) o un apprendimento del sistema di AI rispetto interessi altrui o di quelli collettivi, il che però dipende dalle istruzioni iniziali che determinano le caratteristiche di fondo del sistema e ne sanciscano la disponibilità a imparare dalle sanzioni.

229 Segnalano come al cospetto dell'AI si possa registrare una mancanza di capacità di compiere condotte colpevoli e dunque di un prerequisito generale del diritto penale R. Abbott – A. Sarch, *op. cit.*, p. 350.

230 Deve rilevarsi che la *strict liability*, benchè ancora conosciuta e praticata nella *common law* è oggetto di critiche e destinataria di progressivi ridimensionamenti.R.A. Duff, *The Realm of Criminal Law*, Oxford, 2018, p. 19. Si concorda ormai sulla indispensabilità della volontarietà della condotta considerata da una norma penale. Chiarissimo in questi termini W.R. La Fave, *Substantive Criminal Law*, Eagan, 2018, p. 572: «*criminal liability requires that the activity in question be voluntary*». Lo stesso *Model penal code* afferma che non può essere condanna una persona che abbia tenuto volontariamente una condotta commissiva o omesso una condotta di cui era comunque fisicamente capace, cfr. *Model Penal Code*, § 2.01(1) (Am. Law Inst. 1962). Sul requisito della volontarietà come atto fisico guidato da una consapevole rappresentazione mentale G. Yaffe, *The Voluntary Act Requirement*, in A. Marmor (ed.), *The Routledge Companion to the Philosophy of Law*, New York, 2012, pp. 174 s.

Si torna così a constatare che la responsabilità autonoma dell'agente artificiale è un'illusione ottica e dipende dalle scelte compiute dal programmatore: proprio guardando alle finalità della sanzione ben si può cogliere come tutto in fondo dipenda da come la persona artificiale sia stata strutturata da quella fisica. Punendo l'AI non si fa altro che far ricadere le 'colpe' del creatore sulla sua creazione.

4.2 La prospettiva tradizionale. Variazione sul tema della responsabilità della persona (fisica e/o giuridica): il modello 'vicariale'

Se l'imputazione del fatto all'intelligenza artificiale è logicamente impossibile, occorre rimanere nel solco della responsabilità dell'individuo o della aggregazione di individui.

Il supporto concettuale sarebbe fornito dal paradigma, inveterato, del *respondeat superior*, riletto in modo che il fatto dell'agente artificiale venga imputato alla persona giuridica o fisica ogni volta che il primo abbia agito nel perseguimento dell'interesse del soggetto, individuale o collettivo, chiamato poi a rispondere[231].

Due varianti sono dunque astrattamente disponibili.

i) La responsabilità della persona fisica per il fatto dell'agente artificiale.

ii) La responsabilità esclusiva della persona giuridica per il fatto dell'agente artificiale.

A bene vedere però l'opzione sub a) è impossibile nel caso dell'AI, poiché questa non si pone rispetto all'individuo come invece fa la persona fisica nei confronti della *societas*, che è una aggregazione di persone fisiche che agiscono nel suo interesse. L'AI e la persona fisica sono in rapporto di mera strumentalità. Ciò dipende dal fatto che la persona giuridica è composta da persone fisiche e tanto l'ente collettivo quanto i suoi *shareholders* hanno interessi propri, riconoscibili *ex ante*; l'AI è strutturalmente un *aliud* rispetto all'orizzonte umano. Privo di obiettivi indipendenti da allineare a quelli di un diverso individuo, l'agente artificiale è solo un mezzo che identifica per definizione i propri fini con quelli del suo utilizzatore, sicché per esso non ha alcun senso chiedersi se abbia agito o meno nell'interesse di qualcun altro.

Ben più plausibile è l'alternativa della responsabilità per l'impiego di Agenti artificiali malevoli o comunque eccessivamente rischiosi perché non controllati è quella che identificherebbe una responsabilità dell'ente che si sia avvalso di un dipendente/collaboratore che a sua volta abbia impiegato un agente artificiale. Già la dottrina americana ad aver rilevato come la sostituzione di operatori umani con agenti

231 Sull'impiego del *respondeat superior* con riguardo alla punizione della *company* 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 ss; 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, ritiene che si tratta dell'unico meccanismo adeguato a consentire un rimprovero all'individuo per il fatto dell'intelligenza artificiale al momento.

artificiali possa implicare l'imputazione all'ente di eventi prodotti dal malfunzionamento della macchina[232].

Per lo più il fatto dell'AI non è imputabile alla persona fisica, quanto meno per difetto in capo a quest'ultima dell'elemento soggettivo richiesto dal reato di volta in volta integrato, in ragione dell'autonomia di scelta dell'operatore artificiale, che di fatto decide in piena libertà come e quando delinquere. Si tratterebbe qui allora di una imputazione autonoma ed esclusiva dell'ente, che passa direttamente dall'agente artificiale alla persona giuridica senza considerare l'agente umano. Il nostro ordinamento potrebbe essere già predisposto a simile evoluzione, poiché, come noto, il disposto dell'art. 8 d.lgs. 231/2001, *in nuce* racchiude i prodromi di forma di responsabilità indipendente, pur se comunque ad oggi continua a richiedere un fatto commesso da un individuo, pur non imputabile, punibile o individuato[233].

Accanto a questa soluzione, si può pensare a forme di responsabilità penale diretta della persona fisica per l'impiego pericoloso dell'intelligenza artificiale in ambito finanziario. Per meglio comprendere simile prospettiva si impone però un preliminare chiarimento, a mo' di inciso, in merito al ruolo centrale che il concetto di rischio sta assumendo nella legislazione eurounitaria, sia con riferimento alla tutela dei mercati da turbative realizzate per tramite dell'intelligenza artificiale, che con riguardo alla più generale disciplina del danno da AI.

5 Segue: il ruolo del rischio nel controllo pubblico dei mercati, oggi

Per quanto il diritto penale non sia ancora stato impiegato per il contrasto alle turbative dolose di mercato per il tramite di *HFT* o altre forme di intelligenza artificiale, è già stato steso un reticolo di norme che, dal fronte civile a quello regolamentare, consentono di cogliere nel rischio il coefficiente da considerare per l'implementazione di disposizioni sanzionatorie. E tale modello potrebbe ben essere replicato negli altri settori di attività in cui si faccia uso di AI.

Non ci riferisce al ritardato intervento di adeguamento alla disciplina eurounitario operato da parte della legge n. 238 del 2021[234], quanto al quadro regolamentare e di vigilanza derivante dalla sintesi della normazione europea e della Consob attraverso la sottoposizione a regole stringenti e uniformi a livello continentale e all'introduzione di obblighi specifici sia per le imprese di investimento che si avvalgono delle suddette tecniche, sia per le sedi di negoziazione nell'ambito delle quali esse sono utilizzate.

232 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 ss.

233 Sia consentito qui rimandare a F. CONSULICH, *Il principio di autonomia della responsabilità dell'ente. Prospettive di riforma dell'art. 8*, in *Rivista 231*, n. 4, 2018, pp. 197 ss.

234 Per un commento alla legge Martiello, 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.

Senza voler entrare nell'analisi di siffatta disciplina, basti qui rilevare che si tratta di obblighi che trovano la loro ragion d'essere nella natura intrinsecamene pericolosa della negoziazione, dunque di un approccio normativo basato sul *risk management*[235]. Rispetto ai *traders* sono state previste regole comportamentali che impongono presidi organizzativi dell'attività, mentre, rispetto alle sedi di negoziazione sono sia imposti analoghi requisiti strutturali funzionali a testare, monitorare e garantire la resilienza del sistema in ipotesi di severi scenari di *market stress*.

Esso è ancor meglio esplicitato, su un piano di regolazione generale, nella recente Proposta di Regolamento (UE) sull'intelligenza artificiale[236], in cui si classificano i prodotti che utilizzano completamente o parzialmente il *software* AI in base al rischio di impatto negativo sui diritti fondamentali del cittadino e le infrastrutture di valore che reggono gli Stati democratici contemporanei, quali la dignità umana, la libertà, l'uguaglianza, la democrazia, il diritto alla non discriminazione, la protezione dei dati ed, in particolare, la salute e la sicurezza.

Al crescere della rischiosità del sistema di intelligenza artificiale, divengono più severe sono le misure adottate per eliminare o mitigare l'impatto negativo, fino a proscrivere l'operatività per quelli a quelli incompatibili con un rischio ragionevole.

Ad un primo livello, di rischio totalmente illecito, vi è un divieto di utilizzo pressoché assoluto. Si tratta, stando alla proposta (p. 14, nonché art. 5 a alle III alla stessa), di «sistemi di IA che utilizzano tecniche subliminali per distorcere in maniera sostanziale il comportamento di una persona, così causando, o potendo causare, danni fisici o psichici a quella persona o ad altri; sistemi di IA che sfruttano vulnerabilità legate all'età o ad una disabilità di uno specifico gruppo di persone al fine di distorcere in maniera sostanziale il comportamento di una persona appartenente a tale gruppo».

235 Oltre alla direttiva *MiFID II*, alla Direttiva delegata (UE) 2017/593, al Regolamento (UE) n. 600/2014 (c.d. *MiFIR*), devono essere considerate anche le disposizioni di cui al Regolamento Delegato (UE) n. 2017/584 La disciplina in materia di negoziazione algoritmica è poi contenuta nei provvedimenti legislativi di fonte europea di seguito indicati, adottati dalla Commissione su progetti di norme tecniche di regolamentazione (c.d. *regulatory technical standards – RTS*) presentati alla Commissione da parte della Autorità di regolamentazione dei mercati mobiliari dell'Unione Europea (ESMA).

- Regolamento delegato (UE) 2017/587 della Commissione, del 14 luglio 2016, relativo agli obblighi di trasparenza per le sedi di negoziazione e le imprese di investimento in relazione ad azioni, certificati di deposito, fondi negoziati in borsa, certificati e altri strumenti finanziari analoghi e agli obblighi di esecuzione delle operazioni per talune azioni in una sede di negoziazione o da un internalizzatore sistematico;
- Regolamento delegato (UE) 2017/589 della Commissione, del 19 luglio 2016, relativo ai requisiti organizzativi delle imprese di investimento che praticano negoziazione algoritmica;
- Regolamento delegato (UE) 2017/578 della Commissione, del 13 giugno 2016, che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio relativa ai mercati degli strumenti finanziari per quanto riguarda le norme tecniche di regolamentazione che specificano i requisiti relativi agli accordi e ai sistemi di market making;
- Regolamento delegato (UE) 2017/566 della Commissione, del 18 maggio 2016, che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio relativa ai mercati degli strumenti finanziari per quanto riguarda le norme tecniche di regolamentazione per il rapporto tra ordini non eseguito e operazioni al fine di prevenire condizioni di negoziazione disordinate;
- Regolamento delegato (UE) 2017/588 della Commissione, del 14 luglio 2016, che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione relative al regime delle dimensioni dei tick per le azioni, i certificati di deposito e i fondi negoziati in borsa.

236 Proposta di Regolamento del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione, 21 aprile 2021, in www.eur-lex.europa.eu

Vi è poi un rischio tendenzialmente illecito, in cui l'utilizzo dell'agente artificiale non è totalmente vietato, ma a seguito di una preventiva e rigorosa valutazione di conformità a stringenti requisiti obbligatori e dell'adozione di un adeguato sistema di gestione che contempli un sistema continuo di verifica e monitoraggio.

Al di sotto di questa categoria si pone quella del rischio tendenzialmente lecito, in cui rientrano sistemi che devono sottostare a minimi e precisi obblighi di trasparenza: ad esempio, i *chatbot* e gli assistenti vocali. Infine, gli agenti artificiali totalmente leciti in quanto giudicati *ex ante* non rischiosi, il cui impiego è dunque sempre consentito.

Si tratta di un modello normativo emergente anche in altri atti, come accaduto nel Libro bianco sull'intelligenza artificiale, dove la Commissione europea ha, tra l'altro, sancito il principio secondo il quale l'AI è una tecnologia strategica purché segua un approccio antropocentrico, sostenibile e rispettoso dei diritti fondamentali[237].

In sintesi, lo sforzo che è stato compiuto finora, sia in sede nazionale che eurounitaria, è stato rivolto all'imposizione di standard organizzativi e di sicurezza, per il tramite di obblighi di registrazione e comunicazione con l'Autorità pubblica, per lo più sul fronte regolamentare, e questo non è indifferente per l'*enforcement* penalistico, sia con riguardo agli abusi di mercato[238] che in una prospettiva di applicazione generale con riguardo all'AI.

Certo il diritto europeo veicola nell'ordinamento, attraverso gli strumenti di recepimento e concretizzazione, un'assimilazione della responsabilità del programmatore o beneficiario dell'attività dell'AI a quella del produttore, nel quadro di un regime di natura civilistico e amministrativo. Un simile approccio segna al contempo la cornice in cui collocare un futuribile intervento penalistico.

Ma il diritto civile non è solo riparazione, ma anche prevenzione, almeno nella prospettiva eurounitaria. Come sottolineato in dottrina[239], infatti, la citata Proposta di Regolamento (UE) sull'intelligenza artificiale presuppone le ordinarie regole di imputazione della responsabilità in capo all'uomo, ma si propone di non doverle applicare, per quanto possibile. Il danno dovrebbe essere evitato infatti attraverso l'implementazione di doveri di sorveglianza (il c.d. *duty of human oversight*), in forza dei quali i sistemi intelligenti debbono essere progettati e sviluppati in modo tale da potere essere supervisionati dall'uomo (art. 14), in un contesto di monitoraggio permanente (art. 13). In questa prospettiva, si affianca alla proposta di Regolamento la già citata proposta di Direttiva sulla responsabilità da intelligenza artificiale del 28 settembre 2022, che esclude ogni sua ricaduta penale e distingue, unicamente sotto il profilo civilistico, una responsabilità oggettiva quanto ai sistemi ad alto rischio e una responsabilità per colpa per i sistemi a basso rischio.

237 Commissione europea, Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia, 2020, in www.eur-lex.europa.eu

238 Definisce lo stato della normativa italiana dopo l'introduzione del d. lgs. 107 del 2018 ancora inadeguata ai problemi posti dalla contrattazione algoritmica ad alta frequenza M. PALMISANO, *op. cit.*, pp. 143 ss.

239 Il riferimento corre a 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 ss.

Sul piano amministrativo l'art. 71 della Proposta di Regolamento (UE) sull'intelligenza artificiale introduce alcune sanzioni pecuniarie fino ad euro 30.000.000 o, se l'autore del reato è una società, fino al 6% del fatturato mondiale totale annuo dell'esercizio precedente, sia per l'inosservanza del divieto di pratiche illecite (art. 5) sia per la violazione delle regole in tema di dati e *governance* dei dati dei sistemi di AI ad alto rischio (art. 10).

È significativo, in particolare, che l'AI venga sì percepita come fonte di rischio, ma rimanendo un oggetto e non un soggetto. L'unica persona chiamata a rispondere dei danni rimane quella fisica, considerata pregiudizialmente come quella che rimane sempre in comando. Una *command responsibility for AI* dunque[240].

6 Possibili strategie punitive dell'individuo *de lege ferenda*

Una volta compreso che la politica del diritto in materia di intelligenza artificiale ruota intorno alla gestione del rischio, se ne possono trarre indicazioni pratiche in prospettiva di riforma del diritto penale finanziario. Le problematiche che il diritto penale incontra sul campo attengono all'*enforcement* dell'incriminazione, allorquando non sia identificabile una persona fisica che abbia agito con o attraverso un sistema di AI[241].

In secondo luogo, anche ipotizzando di individuare una o più persone fisiche dietro l'azione dell'AI, si può porre il problema della irriducibilità dell'azione di quest'ultimo ad un contributo penalmente significativo degli esseri umani, dato che questi possono avere tenuto azioni del tutto neutrali in sé e per sé. Anche volendo ipotizzare una semplice colpa ci si può trovare in presenza di momentanei e irrilevanti equivoci tra programmatori, deficit impercettibili di attenzione, errori di calcolo assolutamente trascurabili e così via, inveratisi in luoghi e tempi differenziati tra loro e non connessi con il fatto offensivo: insomma l'irriducibilità pratica del fatto dell'AI alla persona fisica si congiunge qui ad una irriducibilità giuridica[242].

Detto che, almeno nel nostro ordinamento, non vi è possibilità legittima di responsabilizzare direttamente l'agente artificiale, e nemmeno chi se ne sia avvalso o lo abbia creato, a meno di non ricorrere alla disciplina della responsabilità dell'ente, sfruttando il cennato disposto dell'art. 8 d.lgs. 231/2001, si deve ragionare in termini di riforma del sistema.

Diverse le opzioni sul campo e ovviamente non possiamo considerare quelle che attengono al piano extrapenale, che pure possono avere un non trascurabile effetto

240 Lo coglie anche 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 ss. Sulla nozione di danno da prodotto C. Piergallini, *Danno da prodotto e responsabilità penale, Profili dommatici e politico criminali*, Milano 2004, pp. 40 ss.; Id., *La responsabilità del produttore: una nuova frontiera del diritto penale?*, in *Dir. pen. proc.*, n. 9, 2007, pp. 1125 ss.

241 Sulla strutturale difficoltà di dare effettività alle discipline antimanipolative, S.D. Ledgerwood – P.R. Carpenter, *A Framework for the Analysis of Market Manipulation*, in *Rev. L. & Econ.*, Vol. 8, 2012, pp. 253, 260.

242 Qui essenziale il riferimento ad R. Abbott – A. Sarch, *op. cit.*, p. 336.

di disincentivazione. Si pensi, a mero titolo di esempio, alla proposta di tassare le singole transazioni poiché questo, per operatori che ne processano migliaia al secondo, istantaneamente produrrebbe un raffreddamento della tendenza degli *HFT* a generare ordini massivi[243]. Un'altra opzione non penalistica è quella di apporre vincoli di tempo o quantitativi che l'operatore algoritmico deve rispettare, dovendo così mantenere una posizione nel mercato in cui sta operando senza potere assumere strategie speculative puramente istantanee[244].

Fuori dall'ipotesi della responsabilità diretta ed esclusiva dell'ente, di cui abbiamo già parlato, la punizione dell'individuo ruota attorno a due opzioni:

i) la posizione di garanzia rispetto al danno prodotto dall'intelligenza artificiale sul mercato;

ii) la responsabilità per il rischio illecito.

6.1 La posizione di garanzia sul 'fatto' dell'algoritmo

Sul fronte eminentemente penalistico la strategia del controllo del rischio prescelta in sede europea (e quindi italiana) sembra condurre alla strada obbligata della responsabilità omissiva per il mancato impedimento dell'evento avverso prodotto dall'agente artificiale. Ne risponderebbe il programmatore o l'utilizzatore, in quanto si siano assunti un ruolo di controllo su quello specifico sistema intelligente. La responsabilità, quindi, riguarderebbe le offese penalmente rilevanti che sarebbero state evitate attraverso una migliore gestione dell'AI stesso o la predisposizione di idonei meccanismi preventivi o una più attenta programmazione all'origine che neutralizzasse o contenesse i pericoli ad esso connessi[245].

Sia ben chiaro che addurre una posizione di garanzia, tendenzialmente nella forma della posizione di controllo su quella particolare fonte di rischi costituita dall'agente artificiale, non esaurisce i problemi di imputazione, non solo perché non consente di attribuire al garante fatti imprevedibili o inevitabili (se non evitando tout court di maneggiare agenti artificiali, il che sarebbe antistorico), ma soprattutto perché un algoritmo o un sistema di algoritmi che determinano l'insorgenza di un individuo artificiale intelligente non è opera individuale, ma il risultato di un lavoro di squadra,

243 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).

244 Sul punto si veda 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.

245 In questa direzione, con la identificazione di una *Responsible Person* (potenzialmente anche una persona giuridica che se ne avvalga per la propria attività caratteristica), a base colposa, con connessi oneri di registrazione e oneri amministrativi e assicurativi, per casi di c.d. *hard AI crime*, cioè quelli in cui non è identificabile un autore fisico immediato e diretto anche R. ABBOTT – A. SARCH, *op. cit.*, pp. 378 ss., i quali propongono poi l'istituzione di un fondo di garanzia, alimentato dai soggetti individuali o collettivi che si avvalgano di intelligenze artificiali, per i casi in cui l'A.I. responsabile del fatto non abbia una persona per lui responsabile o questa sia incapiente o non assicurata.

sempre più numerosa in ragione delle competenze diversificate che si rendono necessarie e della necessità di far convergere molteplici creatività personali[246]. Per non parlare dell'ipotesi in cui il *software* di AI sia *open source* e venga costruito da soggetti ubicati in varie parti del mondo[247].

Al problema di imputazione di fatto e dolo della persona fisica rispetto a quanto compiuto dalla persona artificiale, si assomma dunque il problema della distribuzione della responsabilità penale tra persone fisiche che siano in qualche modo intervenute nell'elaborazione del sistema intelligente, fin dalla selezione dell'apporto causale rilevante in un reticolo di fattori potenzialmente idonei a partecipare del nesso eziologico[248]. Costruire su queste basi una posizione di garanzia significa definire semplicemente un centro di accollo di responsabilità in caso di eventi dannosi, senza in realtà che ciò presupponga una rimproverabilità del garante[249].

L'attribuzione della responsabilità tra una pluralità di coagenti che cooperano tra loro implica la soluzione di quello che la dottrina angloamericana chiama *many hands problem*[250]; ma vi è anche il problema delle *many things problem*, perché sempre più spesso nella costruzione ed evoluzione di una forma di intelligenza artificiale interviene un'altra intelligenza artificiale, il che implica che i profili fattuali da considerare si moltiplichino e dilatino temporalmente[251].

Invero, tale prospettiva è già effettiva sul piano amministrativo in materia di *market abuse*. Per salvaguardare l'ordine del mercato da illeciti abusivi sono infatti applicabili le fattispecie degli artt. 187-*bis* e 187-*ter* TUF, considerato che le medesime intendono punire il comportamento dell'agente umano, oltre che a titolo doloso, a titolo colposo, ovvero anche soltanto per mera negligenza. L'eventuale introduzione di una nuova fattispecie incriminatrice generale per omesso controllo, dunque, si sovrapporrebbe a regole operanti in alcuni ordinamenti di settore – ed in particolare nel diritto dei mercati finanziari – che, come detto, già apprestano tutela avverso condotte connotate da un coefficiente psicologico di più lieve entità[252].

246 Si tratta di un problema che precede l'intervento penale e attiene alla stessa attribuibilità personale e giuridica del fatto, cfr. D.J. GUNKEL, *Mind the Gap: Responsible Robotics and the Problem of Responsibility*, in *Ethics and Information Technology*, Vol. 22, 2017, pp. 307 ss.; M. COECKELBERGH, *Artificial Intelligence, Responsibility Attribution, and a Relational justification of Explainability*, in *Science and Engineering Ethics*, Vol. 26, 2020, pp. 2051 ss.

247 Caso cui si riferiscono ad esempio R. ABBOTT – A. SARCH, *op. cit.*, pp. 323, 326.

248 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, nonchè G.Q. OLIVARES, *La Robotica ante et derecho penal*, in *Revista Electrónica de Estudios Penales y de la Seguridad*, n. 1, 2017, pp. 16 ss.

249 Sulla stessa linea già C. PIERGALLINI, *op. cit.*, p. 1758.

250 Su tale aspetto osservano M. TADDEO – L. FLORIDI, *How AI can be a force for good*, in *Science*, Vol. 361, Issue 6404, 2018, p. 751: «*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*».

251 Sul problema delle *many things* si veda M. COECKELBERGH, *op. cit.*, p. 2052.

252 L'art. 2, par. 4, *MAR* stabilisce: «I requisiti e divieti contenuti nel presente regolamento si applicano alle attività e alle omissioni nell'Unione e in un paese terzo in relazione agli strumenti di cui ai paragrafi 1 e 2».

6.2 La responsabilità penale per il rischio illecito da intelligenza artificiale

La seconda opzione punitiva che potrebbe essere adottata trae spunto dalla constatazione della natura intrinsecamente strumentale dell'AI[253]. L'intelligenza artificiale non agisce per interessi propri. Gli algoritmi e i *softwares* non hanno preferenze autonome, ma svolgono una funzione per una o più persone fisiche[254].

Quel che conta è la rischiosità dell'impiego in un dato contesto dell'AI. Occorrerà comprendere se il rischio insito in ogni tipo di intelligenza artificiale (sia pure in forme variabili a seconda dei tipi e dei settori di attività) sia stato innalzato dolosamente oltre i limiti di tolleranza.

Focalizzando il rimprovero sulla condotta rischiosa in luogo dell'evento di danno può bypassarsi il problema dell'imprevedibilità del fatto dell'intelligenza artificiale, della cesura che la scelta compiuta dall'AI opera rispetto alle generiche istruzioni inserite dal programmatore. Occorre dunque retroagire alla costruzione di reati dolosi di pericolo.

Elemento indiziario di un dolo di pericolo rispetto all'investimento e al regolare corso delle negoziazioni sarà proprio l'inoculazione negli scambi di agenti artificiali con istruzioni illecite o non adeguatamente schermati rispetto alla loro propensione alla turbativa. Alla base della responsabilità dell'individuo vi sarà l'assunzione di un rischio irragionevole, anche attraverso l'omissione dei presidi tecnici volti a garantire la corretta gestione di un sistema di intelligenza artificiale.

Non sarà allora necessario che la persona fisica si rappresenti l'*iter* produttivo dell'evento, né l'evento stesso, oggi condizione impossibile in presenza di sistemi algoritmici evoluti, ma sarà sufficiente la creazione di un rischio in grado di produrre quel tipo di evento.

Questa seconda opzione di responsabilità per assunzione di un rischio illecito sembrerebbe essere stata già recepita dal legislatore eurounitario nella già indicata Proposta di Regolamento sull'intelligenza artificiale sul piano amministrativo, con la previsione dell'irrogazione di sanzioni per inosservanza del divieto di pratiche illecite e per la violazione dei requisiti di conformità previsti per i sistemi ad alto rischio (art. 71). Affinché questa opzione più generale diventi operativa anche in materia di abusi di mercato è necessario però che i sistemi di AI di *trading* siano annoverati nell'ambito dei sistemi a rischio alto.

253 Nel diritto penale americano si parla a questo proposito di impiegare la *innocent agency doctrine*, per cui la responsabilità penale viene imputata a colui che abbia agito attraverso un agente completamente innocente, che dunque è una sorta di strumento nelle sue mani. Si veda a questo proposito 18 U.S.C. § 2(b) (2019), secondo cui «*Whoever willfully causes an act to be done which [is a crime] is punishable as a principal*». In giurisprudenza, Rosemond v. United States, 572 U.S. 65, 79-80 (2014). In dottrina, 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.

254 Sul punto si vedano già da tempo B.J. KOOPS – M. HILDEBRANDT- D.O. JAOUET-CHIFFELLE, *Bridging the Accountability Gap: Rights for New Entities in the Information Society?*, in *Minn. J. L. Sci. & Tech*, Vol. 11, 2010, pp. 497 ss.; e, ancora prima, L. FLORIDI – J.W. SANDERS, *In the Morality of Artificial Agents*, in Mind and Machines, Vol. 14, 2004, pp. 349 ss.

7 Il problema del *retribution gap* in ottica comparata

È comune nella dottrina internazionale la percezione della sussistenza di un vero e proprio *retribution gap* in materia di intelligenza artificiale[255]; la preoccupazione è al contempo quella di non colpire la persona dietro l'algoritmo solo poiché un responsabile deve comunque essere individuato. Il c.d. rischio del capro espiatorio morale è, dunque, elevato, e si accresce tanto più il livello di tecnologia sottesa all'AI è avanzato.

A fronte di questo possibile effetto collaterale, è però condiviso da molti il mantenimento di un approccio penalistico incentrato sull'uomo. Si è parlato in tale settore del principio dello *human in command*: non solo in dottrina, ma anche a livello normativo, soprattutto nel *soft law* eurounitario, ci si orienta verso la creazione di meccanismi di *accountability* e sicurezza *by design* (espressione, quest'ultima, che definisce un *software* progettato espressamente per essere sicuro, anticipando, minimizzandoli a priori, i profili di rischio che potrà manifestare successivamente). Si tratta di assicurare la verificabilità delle scelte algoritmiche, minimizzando il rischio di errori o conseguenze imprevedibili, ma soprattutto di garantire all'individuo un pronto riacquisto del controllo della situazione in caso di necessità, per evitare o gestire rischi generati dall'AI[256]. Difatti, il controllo umano sull'intelligenza artificiale – dal quale deriverebbe poi la responsabilità penale omissiva – può essere garantito solo tramite l'imposizione di presidi di progettazione, a monte, e di controllo, a valle, delle azioni algoritmiche. Il legislatore dovrebbe, quindi, attribuire all'IA il massimo di autonomia utile, ma sempre entro una sfera di controllabilità umana[257].

Ciò posto, occorre comprendere quali soluzioni sono state proposte per risolvere il *deficit* imputativo nel campo dell'intelligenza artificiale applicata ai mercati.

7.1 Le riflessioni della dottrina angloamericana

L'interazione tra intelligenza artificiale e agenti umani determina la frammentazione delle responsabilità[258]. Ci sono voci nella dottrina anglosassone che hanno

255 J. Danaher, *Robots, Law and the Retribution Gap*, in *Ethics and Information Technology*, Vol. 18, 2016, pp. 299 ss.; successivamente, sempre in senso critico in ordine queste forme di responsabilità 'accessorie' della persona fisica J. Turner, *Robot Rules*, 2018, pp.120 ss., che evidenzia anche i rischi di *over deterrence* e *chilling effect* rispetto alla ricerca tecnologica.

256 È interessante guardare alle proposte avanzate, in un contesto molto distante dal nostro, dalla SINGAPORE PERSONAL DATA PROTECTION COMMISSION, secondo la quale è necessario che, nei campi governati dall'intelligenza artificiale, sia sempre garantita la possibilità che la persona umana possa in ogni momento assumere nuovamente il controllo dello scenario operativo Singapore PDPC, *A Proposed Model Artificial Intelligence Framework* (Jan. 2019), in https://www.pdpc.gov.sg. In particolare, si propone (15) di implementare in tutti gli agenti artificiali sistemi simili alla scatola nera degli aeromobili, in modo da poter ricostruire i processi decisionali dell'AI.

257 Si veda il documento pubblicato dal Gruppo di esperti ad alto livello sull'intelligenza artificiale è indipendente, istituito dalla Commissione europea nel giugno 2018, intitolato *Etichs guidelines for Trustworthy Artificial Intelligence*, 8 aprile 2019, in www.europa.eu, 18; 30 ss.; Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Creare fiducia nell'intelligenza artificiale antropocentrica, 8 aprile 2019, in eurlex.europa.eu, 3 ss.

258 Nella dottrina italiana il tema è segnalato da M.B. Magro, *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, cit., p. 3.

avanzato l'idea di ricorrere ad un meccanismo di responsabilità vicariale dell'essere umano per il fatto dell'AI, modulata però non in senso puramente oggettivo, per cui il primo viene chiamato a rispondere per il solo fatto dell'esistenza di un danno cagionato dal secondo, ma dipendente dalla colpa del programmatore.

Il programmatore (ma si potrebbe anche coinvolgere l'utilizzatore) assumerebbe le vesti dell'*employer* e il sistema intelligente sarebbe il suo *employee*, definendo un paradigma basato sulla cd. conseguenza probabile (*natural-probable-consequence*)[259]. Quest 'ultimo meccanismo è nato per ascrivere all'agente un fatto non voluto (dunque riconducibile ad una mera *negligence* o al più *recklessness*) realizzatosi nel contesto di un accordo per commettere un diverso reato meno grave (è in sostanza una disciplina strettamente imparentata, dal punto di vista concettuale, al nostro art. 116 c.p.)[260].

Una diversa soluzione potrebbe essere, per alcuni studiosi, quella della c.d. *perpetration by another*: siamo lontani da un meccanismo vicariale e ben più vicini ad un'impostazione strettamente concorsuale, che consente di punire chi si avvalga dell'agente artificiale o lo abbia costruito[261], a condizione però che sia possibile identificarne l'*intent* di commettere il reato. Il sistema di AI sarebbe una sorta di concorrente inconsapevole di colui che, per suo tramite, mira a commettere l'illecito.

Siffatte formule rimandano dunque al tema del possibile concorso di persone, tra quelle fisiche e quelle artificiali. Il penalista continentale, soprattutto di area culturale tedesca, sarebbe subito allettato dalla spendita del concetto di autore mediato[262], tipico caso in cui vi è un soggetto che detiene il dominio del fatto e un altro, al primo subordinato che esegue senza possedere una propria autonomia imputativa, mentre quello anglofono al paradigma del *perpetretor-by-another* (o *by means*) o ancora dell'*innocent agency*[263].

A nostro avviso, non essendo possibile parificare agente umano e artificiale, non sarebbe corretto appellarsi ad un paradigma concorsuale, seppure rinnovato nei soggetti partecipi, perché siamo in presenza di un semplice processo di affinamento

259 Così G. Hallevy, *The Criminal Liability of Artificial intelligence Entities*, in *Akron Intellectual Property Journal*, Vol. 4, Issue 2, 2010, pp. 171 ss.

260 Per un suo impiego nel campo dell'intelligenza artificiale 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. Su questo modello di responsabilità si vedano, a mero titolo di esempio, K.R. Bird, *Natural and probable consequences doctrine: "Your acts are my acts!"*, in *W. St. UL Rev*, Vol. 34, 2006, p. 43; in precedenza 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.

261 Sul punto 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*, in www.ijcai.org; si leggano anche 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.

262 Celeberrimo il lavoro di C. Roxin, *Täterschaft und Tatherrschaft*, Hamburg, 1963 (10. Auf., Berlin, 2019), 67 ss., pp. 119 ss. Di tale figura concorsuale vi è un espresso riconoscimento nel codice penale spagnolo del 1995 (art. 28), nonché nello statuto della corte penale internazionale, all'art. 25 (3)(a).

263 Su innocent agency e 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 ss.

dell'*instrumentum sceleris*. Per quanto peculiare, l'AI rimane un mero strumento nelle mani dell'unico autore, umano, del reato.

Echi penal-internazionalistici si leggono poi nelle pagine di chi propone l'importazione in sede penale 'comune' del modello della *command responsibility*. Tipica delle organizzazioni gerarchiche di natura militare (o assimilate) e mutuata dall'art. 28 dello Statuto di Roma della Corte penale internazionale, finisce per ascrivere la responsabilità al soggetto in posizione di preminenza organizzativa che sapesse del reato in corso di svolgimento da parte del subordinato e ciò non di meno non abbia assunto iniziative ragionevoli per impedire la perpetrazione del fatto[264].

Trasposta nel campo del fatto illecito dell'AI, la soluzione renderebbe più agevole la contestazione all'individuo poiché non richiede in capo a quest'ultimo, identificato come colui che possiede una funzione a questo punto direzionale (più che direttiva) sull'agente artificiale, la dimostrazione di alcun tipo *intent* rispetto alla commissione del fatto di reato, ma si accontenta della consapevolezza (*knowledge*) rispetto alla realizzazione dello stesso nel perimetro organizzativo di sua competenza in cui si muove il soggetto artificiale[265].

7.2 Cenni alla giurisprudenza statunitense

Con specifico riguardo allo scenario statunitense, precisamente al formante giurisprudenziale, le previsioni più spesso applicate sono state quelle dirette a contrastare la manipolazione del mercato. Ad esempio, si è invocata la responsabilità per la fraudolenta rappresentazione artificiosa della realtà ai sensi del § 10(b) dell'*Exchange act* e della *Rule 10b-5* promulgata dalla SEC, che come noto sono state ritenute dalla giurisprudenza, pur senza un espresso *placet* normativo in tal senso, come possibili fonti di azioni civili, fin dal 1971[266].

In alternativa, viene evidenziata la possibilità di azionare la § 9 dell'*Exchange act*, che si differenzia dalle disposizioni precedenti per la necessità della dimostrazione dello specifico intento di indurre l'acquisto o la vendita di strumenti finanziari da parte di altri o di creare una falsa apparenza dell'andamento dei titoli, ragione per cui, tanto i privati quanto i *prosecutors*, raramente azionano questa disposizione nel procedimento per manipolazione del mercato[267].

La prima azione per *market manipulation*, nella specie del *marking the close*, compiuta da HFT è stata intrapresa dalla SEC il 16 ottobre 2014, per violazione della

264 Secondo 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 ss., sarebbe applicabile anche ai casi fatto illecito commesso da intelligenze artificiali.

265 Per un primo approccio al tema 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 ss. Per tutti, su questo paradigma, nella propria sede originaria, vale a dire il diritto penale internazionale, C. Meloni, *Command Responsibility in International Criminal Law*, The Hague, 2010, 31 ss.

266 Si veda Superintendent of Insurance of New York v Bankers Life & Casualty Co, 404 US 6, 13 n 9 (1971).

267 Si veda sul punto, 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.

Rule 10b-5[268], ma sono state intraprese anche *class actions*, come nel *leading case City of Providence v BATS Global Markets, Inc*[269].

Le strategie di manipolazioni compiute per il tramite di *HFT* rispondono perfettamente, in effetti, ai requisiti di artificiosità richiesti dalle norme indicate, generano un'errata rappresentazione della realtà di mercato in capo agli *slow traders*, e così paiono soddisfatti i requisiti per la condanna nel caso di azioni civili[270].

Un cenno merita la *Section 747 del Dodd-Frank Wall Street and Consumer Protection Act*, legge federale del 2010 voluta da Obama dopo la crisi economica del 2008, che ha emendato il *Commodity Exchange Act* e ha introdotto nell'ordinamento americano una previsione che punisce ogni forma di *trading* che possa costituire *spoofing*, vale a dire l'inserimento di ordini con immediata cancellazione prima dell'esecuzione, se vi è prova dell'*intent* dell'operatore (7 U.S.C. § 6c(a)(5)(c))[271]. Come noto, la *CFTC* ha basato sulla *section* 6c(a)(5)(C) alcune note azioni legali, sia sul piano civile che sotto forma vere e proprie *criminal charge* in tema di trading algoritmico, come nel noto caso *Coscia*[272].

Il refrain della difficile prova dell'*intent* è risuonato anche in quest'ultima vicenda giudiziaria. La giurisprudenza (precisamente la Corte di Appello - Settimo Circuito) ha lamentato che tale requisito sia alquanto limitante rispetto alle potenzialità applicative della disposizione, ma ciò non di meno ha confermato la condanna in sede penale dell'accusato[273].

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

269 *Complaint for Violation of the Federal Securities Laws, Civil Action No 14-2811* (SDNY filed Apr 18, 2014). In proposito si legga T.E. LEVENS, *op. cit.*, p. 1534.

270 Lo nota T.E. LEVENS, *op. cit.*, pp.1546 ss.

271 Cfr. 7 U.S.C. § 6c(a)(5)(C), su cui 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 ss. La disposizione recita infatti «*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)» (sottolineature aggiunte).

272 *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), in cui peraltro la Corte ha negato che la norma introdotta dal Dodd-Frank act fosse incostituzionalmente vaga. Sugli sforzi, in termini di enforcement della CFTC in tema di HFT si veda la panoramica di M. WOODWARD, *op. cit.*, pp. 1382 ss.

273 *Coscia*, 866 F.3d. al punto 794, dove si può leggere infatti: «*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*». Anche per la dottrina, la prova dell'elemento centrale delle frodi finanziarie, cioè l'*intent*, è davvero un miraggio nel contesto nelle transazioni cibernetiche, cfr. G. SCOPINO, *op. cit.*, p. 233; anche T.C.W. LIN, *The New Market Manipulation*, cit., p. 1301, rileva che l'*intent* è assente in un contesto in cui il contributo umano si limita all'iniziale messa in opera dell'algoritmo e al suo inserimento del mercato, quando poi l'AI sia privo di direzione da parte di un operatore fisico e continui a modificare le proprie strategie di trading.
Sullo scarso *enforcement* nel mercato americano nei confronti delle turbative connesse all'impiegato di *HFT* 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 ss. Molti Autori nella letteratura nordamericana ha evidenziato come sia difficile pretendere che la legge, non solo quella penale, ma anche quella riferibile a società e mercati, naturalmente riferibile a persone fisiche

7.3 Le iniziative tecniche e normative delle autorità di settore statunitensi

La *SEC* non si è mossa solo sul piano sanzionatorio, ma anche attraverso attività regolatoria e implementazione tecnologica della propria attività di *enforcement* sui mercati, pur tra le difficoltà operative scaturenti da un livello di risorse umane e tecnologiche inferiori a quelle che sarebbero necessarie per tenere il passo dell'evoluzione informatica dei sistemi di trading, come denunciato ad esempio dall'allora presidente della SEC Mary Jo White al Congresso statunitense nel 2013[274].

Quanto al fronte tecnologico, sono stati nel tempo implementati, analogamente a quanto già implementato in Italia dalle società di gestione dei mercati, i meccanismi di interruzione di emergenza delle contrattazioni come i *circuit breakers* o, agli *execution throttles*, di cui si è discusso per quanto attiene ai derivati anche in seno alla *CFTC* (*Commodity Futures Trading Commission*): si tratta di presidi indispensabili per prevenire pratiche manipolative come l'*order stuffing*, pratica in cui un gigantesco numero di ordini viene immesso sul mercato e subito rimosso prima di essere eseguito[275]. Si sono registrate in questo settore anche le proposte della *Securities Industry* and *Financial Markets Association* (*SIFMA*), volte ad introdurre tutele 'tecniche' per la protezione degli investitori, come ad esempio bande predefinite di oscillazione dei prezzi, contenute entro limiti di ragionevolezza, così come meccanismi di pausa automatica all'operatività quando necessario a promuovere una corretta *price discovery*[276].

Sul fronte normativo, sono state istituite le cd. *Limit-Up* e *Limit-Down rules*, che impediscono una fluttuazione eccessiva del valore di un titolo rispetto alla media di prezzo registrata in un dato periodo antecedente[277]. Inoltre, già nel 2014 la SEC ha approvato il Regolamento sulla conformità e l'integrità dei sistemi (*Regulation Systems Compliance and Integrity*, c.d. *SCI*), imponendo il rispetto rigoroso dei requisiti di monitoraggio e documentazione alla maggior parte delle piattaforme di *trading*[278].

o al più a enti possa applicarsi a sistemi di intelligenza artificiale. Tra le molte riflessioni in questo senso di S. CHOPRA – L.F. WHITE, *A Legal Theory for Autonomous Artificial Agents*, Ann Arbor, 2011, 153 ss.; nonchè le pionieristiche considerazioni di L.B. SOLUM, *op. cit.*, pp.1231-33.

274 B. PROTESS, *White Makes Case for Bigger S.E.C. Budget*, in *N.Y.* TIMES, 7 maggio 2013.

275 In questo senso si veda il documento predisposto dalla CFTC, *Concept Release on Risk Controls and System Safeguards for Automated Trading Environments*, 78 FR 56542-01 (proposed Sept. 12, 2013), disponibile in http://www.cftc.gov.

276 Si veda a tale proposito SIFMA, Flash Crash Resource Center, in http://www.sifma.org.

277 FINRA Rules, Rule 6190; NMS Plan to Address Extraordinary Market Volatility (come modificato dall'*Approval Order* della SEC, *Exchange Act Release* No.77679) 11 (2016), http://www.finra.org. Osservatori come Charles Korsmo (C. KORSMO, *High-Frequency Trading: A Regulatory Strategy*, in *U. Rich. L. Rev.*, Vol. 48, 2014, pp. 523, 608) ripongono grande fiducia in queste misure, osservando che gli interruttori automatici e il meccanismo di limitazione a priori delle oscillazioni «sono i modi più semplici per evitare che si ripeta delle principali dislocazioni del Flash Crash». Sulla stessa linea, M.B. FOX-GLOSTEN – G.V. RAUTERBERG, *The New Stock Market: Sense and Nonsense*, in *Duke L. J. 191*, Vol. 65, 2015, pp. 272 ss.

278 Si veda 17 C.F.R. §§ 242.1000-07 (2017). Ai sensi di questa disciplina, le *trading venues* devono altresì prontamente rendere noti problemi tecnologici non conosciuti in precedenza alla SEC. Il regolamento SCI non riguarda direttamente gli *HFT* ma induce le *trading venues* a monitorarne da vicino l'attività. Si veda in questo senso *Regulation SCI Adopting Release*, *Exchange Act Release* No. 73639, 79 Fed. Reg. 72252, 72410 (Dec. 5, 2014). Si veda, per un elenco di proposte dottrinali e di iniziative effettivamente assunte dalla SEC per migliorare il monitoraggio degli *HFT*, M. MORELLI, *op. cit.*, pp. 220 ss.

Nell'ottica del miglioramento della trasparenza dei mercati, un supporto essenziale può rivelarsi la *Rule 613* adottata dalla *SEC*, che ha imposto ai mercati e alla *FINRA* (*Financial Industry Regulatory Authority*)[279] di creare e mantenere il c.d. *CAT* (*consolidated audit rail*), strumento pensato per tracciare il ciclo degli ordini di tutte le transazioni finanziarie e così consentire di ricostruire *ex post* l'eziologia e la fenomenologia delle condotte manipolative eventualmente tenute su più mercati contemporaneamente anche da operatori algoritmici, soprattutto nell'ottica di facilitare il private *enforcement* sui mercati, anche in chiave di *class action* dei risparmiatori[280]. Per monitorare gli scambi, nel 2013 ha istituito entro la propria struttura il *MIDAS* (*Market Information Data Analytics System*)[281]. In questo quadro si è inserita già dal 2010 la regola che proibisce il c.d. *naked access*, prima usato dalle *HFT firms* per accedere ai mercati attraverso le credenziali di un *broker* registrato presso la *SEC*, rendendo opaca la propria presenza sul mercato[282].

La dottrina, per parte propria, conferma da tempo che le più importanti previsioni nella lotta agli abusi algoritmici siano effettivamente la c.d. *Bedrock Rule* della *SEC* (10b-5)[283] e la *Rule 180.1*[284] della *CFTC*[285], ma ha aggiunto che si può al contempo impiegare discipline come la *Market Access Rule*[286] per migliorare, in ottica preventiva, la propria supervisione sui mercati e così indirettamente combattere le nuove forme di manipolazione, senza doversi imbattere nella spinosa questione dell'elemento soggettivo degli operatori fisici[287].

7.4 Lo scenario britannico

Dopo l'uscita del Regno Unito dall'Unione europea, la comparazione è tornata utile anche con il sistema d'Oltremanica, sottratto ormai all'azione integratrice delle istituzioni eurounitarie e, in particolare, dell'ESMA. Il riferimento principale è qui costituito dalla *section* 90(1) dello *UK Financial Service Act* del 2012, che pur non riferendosi alla negoziazione algoritmica, si presta, alla luce delle ampie formule linguistiche impiegate, a punire coloro che si avvalgano di strategia di *trading* avvalendosi di

279 Si tratta dell'autorità indipendente di autoregolamentazione del settore finanziario statunitense. FINRA nello specifico è una organizzazione non-profit autorizzata dal governo degli Stati Uniti, il cui compito è sovrintendere all'attività delle entità finanziarie USA.

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

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

282 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).

283 17 C.F.R. § 240.10b-5 (2017).

284 17 C.F.R. § 180.1 (2017).

285 In questi termini, rispetto alla 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 giurisprudenza, sempre sulla rule 10b-5.

286 Si pensi alla section 15 U.S.C. § 78o(b)(4)(E) (2012) alla section 17 C.F.R. § 240.15c3-5 (2017) e alla section 17 C.F.R. § 166.3 (2017); in giurisprudenza, 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).

287 T.C.W. Lin, The New Market Manipulation, cit., p. 1301.

HFT che creino una falsa o fuorviante impressione sul prezzo o sul valore di un emittente o di uno strumento finanziario[288]. Si tratta di una fattispecie punita con la pena della reclusione e con quella pecuniaria. Precedentemente, la *section* 397(3) del *Financial services and Markets Act* del 2000 richiedeva la prova dell'induzione di un terzo ad una condotta di investimento, requisito che aveva di fatto impedito l'applicazione della disposizione nei 12 anni di vigenza della stessa.

Proprio l'eliminazione di questo requisito nella incriminazione vigente, a parere della dottrina, dovrebbe consentirne una più agevole contestazione, anche perché, dal punto di vista del c.d. *mental element*, non è richiesta solo l'*intention* e la consapevolezza della natura falsa e fuorviante per gli altri del proprio comportamento, ma è sufficiente la *recklessness*[289].

Ciò non di meno, la FCA (*Financial Conduct Authority*, deputata alla vigilanza sul mercato inglese) ha sì incrementato i propri controlli rispetto agli *HFT*, ma ricorrendo alla *section* 118 FSMA che proibisce gli abusi di mercato: ciò è avvenuto sia nel caso *Coscia* (per quanto di competenza britannica)[290] che in quello *Da Vinci*[291], conclusosi nel 2015 davanti all'Alta Corte di Giustizia adita dalla FCA, che nel precedente *Swift trade*[292]. Si è trattato di turbative in cui principalmente la tecnica impiegata è

288 La previsione, rubricata Misleading Impressions, recita: «*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)».

Le successive subsections 2, 3 e 4 dispongono: «*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». Sulla disposizione ed il rapporto con gli *HFT* si vedano 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 ss.

289 In questo senso J. Fisher – A. Clifford – F. Dinshaw – N. Werle, *op. cit.*, p. 115.

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

291 Per la decisione sul caso cfr. https://www.fca.org.uk

292 Si veda 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; nonchè 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/finalnotices/7722656-canada-inc.pdf.

stata quella del *layering*[293] e rispetto ad esse, pur rinvenendosi gli estremi per procedere penalmente, l'autorità di vigilanza ha scelto di agire solo in sede civile[294].

Sostanzialmente analogo il caso *Paul Axel Walter* nel 2017, culminato nell'irrogazione di una sanzione amministrativa dalla FCA nei confronti di un impiegato della Bank of America Merrill Lynch International Limited (BAML) per aver attuato nel 2014 una strategia che prevedeva l'inserimento di ordini che avevano quale obiettivo quello di indurre gli altri operatori del mercato che seguivano l'andamento dei titoli ad aumentare o a diminuire le quotazioni di modo da beneficiare di tale variazione del prezzo[295].

293 Si tratta di una tecnica che consiste nell'immettere un ordine nascosto (non visibile nel book di negoziazione) in acquisto o vendita e un altro ordine palese visibile nel book dal lato opposto (vendita/acquisto) in modo da indurre gli altri operatori a credere che il mercato si stia muovendo verso un ribasso del prezzo e ad agire di conseguenza. Per una descrizione dei tre casi si veda G. RUTA, *op. cit.*, pp. 67 ss. Nel caso *Da Vinci*, la condotta di manipolazione contestata rientra nella categoria del *Layering* o *Spoofing*, in relazione alle quali il giudice ha fornito le seguenti definizioni: il *Layering* consiste nella pratica di inserire relativamente grandi ordini su un lato del *book* di scambio senza una genuina intenzione di dargli esecuzione: gli ordini vengono inseriti a prezzi che difficilmente sono in grado di attrarre controparti, almeno nelle intenzioni di chi li inserisce, ma che sono comunque idonei a determinare una variazione del prezzo dell'azione, come conseguenza dell'adeguamento del mercato per effetto di un apparente spostamento dell'equilibrio tra domanda e offerta. Al movimento consegue l'esecuzione di un'operazione sull'altro lato del libro degli ordini, con l'ottenimento di un profitto. Questo scambio è a sua volta seguito dalla cancellazione rapida dei grandi ordini che erano stati inseriti allo scopo di provocare il movimento del prezzo. L'operazione viene ripetuta più volte. Da tale descrizione si rileva come il termine *Layering* identifichi l'immissione di più ordini progettati per non essere scambiati su un lato del *book*, mentre *Spoofing* si riferisca al fatto che tale immissione crea una falsa impressione sulle vere intenzioni commerciali del *trader*.

294 Per una riflessione sul punto J. FISHER – A. CLIFFORD – F. DINSHAW – N. WERLE, *op. cit.*, p. 117.

295 Il riferimento completo del caso si trova al seguente link: https://www.fca.org.uk/publication/finalnotices/paul-axel-walter-2017.pdf. Particolarmente interessante che la manipolazione sia stata resa possibile sfruttando l'uso di algoritmi da parte degli altri operatori del mercato. Nello specifico, l'impiegato ha approfittato degli algoritmi in uso ad altri operatori che monitoravano le migliori offerte per attirarli verso le sue quotazioni e quindi negoziare poi a prezzi più alti o più bassi.

Conclusioni

Il lavoro si incentra sulla distinzione tra sistemi di AI deboli e sistemi di AI forti: mentre i primi dipendono dalle istruzioni prestabilite di produttori, programmatori o utenti, i secondi sono dotati di capacità di auto-apprendimento e producono *outputs* autonomi ed imprevedibili rispetto agli *inputs* iniziali.

La diffusione nel mercato finanziario di tali tecnologie - avvertita in misura maggiore nell'ambito del *trading* più che nell'ambito della formazione e circolazione delle informazioni privilegiate - sollecita l'interprete a interrogarsi sulla tenuta del quadro normativo, con particolare riferimento all'imputazione degli illeciti finanziari realizzati con l'intervento dell'agente artificiale ed impone che si accerti, in particolare, se il Regolamento (UE) *MAR* sia o meno idoneo a ricomprendere le condotte illecite perfezionatesi con l'utilizzo di sistemi di intelligenza artificiale, la cui autonomia e imprevedibilità potrebbe dare luogo ad aree di non punibilità.

Invero, mentre per i sistemi di AI deboli le regole giuridiche in vigore possano essere applicate estensivamente per contrastare tali condotte illecite, per i sistemi di AI forti è invece necessario adottare *ex novo* criteri di imputazione della responsabilità, che rendano effettivi i presidi che tutelano il regolare funzionamento degli scambi.

La capacità dei sistemi di AI forti sembrerebbe incrinare l'applicazione del principio di neutralità tecnologica in sede di regolamentazione («*same risk, same activity, same treatment*») e il raggiungimento di un *level playing field*, cui tende peraltro l'intera disciplina in materia di intermediazione finanziaria. Con l'intelligenza artificiale autonoma emergono inedite esigenze di tutela a fronte di un apparato normativo orientato unicamente sulla condotta (commissiva o omissiva) dell'uomo. Non sempre è possibile individuare, infatti, un apporto umano nella causazione di un danno, per cui la disciplina vigente non appare totalmente adeguata di fronte «ai rischi e alla rilevanza dei rischi» che le nuove modalità di *trading* dischiudono per la clientela in particolare e per il sistema finanziario in generale. In tal senso si esprime, tra l'altro, la Risoluzione del Parlamento europeo sulla tecnologia finanziaria del 17 maggio 2017, là dove è ben evidenziato che il principio di neutralità tecnologica non consente di lasciare l'intero settore finanziario sottoposto ad una normazione identica sia per le attività tradizionali sia per le attività digitali.

È stato rilevato, infatti, che i sistemi di AI forti sono in grado di manipolare il mercato, sia mediante inserimento di un quantitativo di ordini di esecuzione e cancellazione superveloci in intervalli temporali di millesimi di secondo, sia mediante dinamiche meno veloci ma comunque difficilmente comprensibili, data l'imperscrutabilità

della *black box* algoritmica. L'eventuale consumazione di illeciti comporta conseguentemente difficoltà probatorie per l'individuazione del responsabile, l'accertamento della colpa o del dolo e la sussistenza del nesso causale. Tuttavia, specie con riguardo alle fattispecie di manipolazione operativa, le previsioni di *MAR* frenano (forse inconsapevolmente) l'utilizzo di sistemi di AI forti, richiedendo a tutti i soggetti che con le loro condotte incidano sul processo di formazione dei prezzi, di essere in grado di fornire le motivazioni che hanno portato alle stesse: richiesta che i sistemi di AI forti, essendo *black box*, non riescono paradossalmente a fornire.

Anche nella eventuale prospettiva di consentire l'utilizzo consapevole di tali sistemi, che sono potenzialmente forieri di benefici economici per la collettività, lo studio individua, in alternativa tra loro, tre possibili soluzioni dirette a reprimere le condotte dei sistemi di AI che, in modo autonomo e imprevedibile rispetto al produttore, al programmatore o all'utente, abbiano assunto comportamenti dannosi o più specificamente lesivi dell'integrità del mercato. Tuttavia, ciascuna di queste soluzioni presenta peculiari profili di criticità a seconda dei settori dell'ordinamento che entrano in gioco in conseguenza della condotta illecita degli agenti non umani.

La prima proposta consiste nell'attribuire una soggettività giuridica ai sistemi di intelligenza artificiale più avanzati. E tuttavia, l'assegnazione di una funzione giuridica analoga a quella prevista per le persone giuridiche integrerebbe una *fictio juris* fine a sé stessa, che non risolverebbe il problema – particolarmente arduo da risolvere in ambito penalistico e amministrativo - dell'attribuzione della responsabilità, basata tradizionalmente sui criteri di colpa e dolo, né quello dell'*enforcement* della sanzione comminata. Vanno infatti attentamente valutate, non solo le difficoltà insite nell'applicare la sanzione ad un agente artificiale, ma anche la circostanza che, con specifico riferimento alle sanzioni pecuniarie ed al risarcimento del danno, la configurazione di una personalità giuridica per i sistemi di AI richiederebbe in ogni caso l'individuazione dei soggetti tenuti a costituire un patrimonio separato a tal fine.

La seconda soluzione prospettata si propone di superare le difficoltà legate alla diretta attribuzione della responsabilità all'agente artificiale, riconducendo gli illeciti materialmente compiuti da quest'ultimo alla responsabilità oggettiva di colui il quale (produttore, programmatore, o financo utente), mettendo in servizio il sistema di AI, abbia creato il rischio – poi verificatosi – dell'illecito; e ciò a prescindere dalla consapevolezza di tale rischio. È però di tutta evidenza che tale soluzione – essa pure difficilmente compatibile coi tradizionali principi dell'imputazione penale – quand'anche adottata esclusivamente in ambito civilistico o amministrativo potrebbe compromettere significativamente la spinta all'innovazione tecnologica nel settore considerato.

La terza proposta configura un superamento del concetto stesso di responsabilità, incentrandosi essa sulla socializzazione del danno (*recte*: del suo costo) da porre a carico, non tanto del singolo individuo, quanto piuttosto della comunità nel suo insieme, con il vantaggio di non deprimere lo sviluppo dell'innovazione tecnologica e di favorire al contempo la realizzazione di un sistema economico complessivamente più efficiente. Anche quest'ultima opzione, tuttavia, presenta alcuni inconvenienti, a partire dai potenziali riflessi della mutualizzazione sulle dinamiche di mercato.

In ambito UE una soluzione che non inibisca lo sviluppo tecnologico ma che prevenga la diffusione su larga scala di illeciti commessi dai sistemi di AI potrebbe essere quella già incorporata nella Proposta di Regolamento (UE) sull'intelligenza artificiale che cerca di contemperare l'utilizzazione dell'intelligenza artificiale con la tutela dei diritti fondamentali secondo un approccio basato sul rischio mediante la combinazione dell'applicazione del principio di precauzione e di prevenzione, rispettivamente per i sistemi di AI a rischio inaccettabile e i sistemi di AI a rischio alto.

Per imputare la responsabilità in capo a produttore, programmatore o utente non dovrebbe essere necessario che questi soggetti si rappresentino l'evento o la possibile verificazione del medesimo ma dovrebbe essere sufficiente unicamente la creazione di un rischio in grado di produrre l'evento.

L'applicazione di questa *regula iuris* in campo finanziario potrebbe portare ad un'estensione delle attività e dei servizi qualificabili "ad alto rischio", tra cui potrebbe essere ricompresa anche l'attività di *trading*, con relativo obbligo da parte dei soggetti della filiera produttiva di osservare una serie di requisiti di conformità in mancanza dei quali sorgerebbe una responsabilità di natura amministrativa.

Qualsiasi soluzione prescelta dovrà contemperare l'opportunità di non comprimere eccessivamente i margini di sviluppo tecnologico con l'esigenza di assicurare adeguati livelli di tutela del regolare funzionamento del mercato e, più in generale, la pari dignità di reintegrazione delle posizioni giuridiche lese dall'operato degli agenti artificiali.

Bibliografia

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 ss.

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 ss.

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

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

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 ss.

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

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

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

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 ss.

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

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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

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

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 ss.

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

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 ss.

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 ss.

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 ss.

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

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 ss.

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

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

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

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 ss.

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 analusis*, 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 ss.

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 ss.

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

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 ss., spec. 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 ss.

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 ss.

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 ss.

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 ss.

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

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

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

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

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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

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 ss.

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 ss.

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 ss.

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

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

CONSULICH F., *La giustizia e il mercato*, Milano, 2010.

CONSULICH F., *Manipolazione dei mercati e diritto eurounitario*, in *Soc.*, n. 2, 2016, pp. 203 ss.

CONTALDI G., *Intelligenza artificiale e dati personali*, in *Ord. int. dir. um.*, n. 5, 2021, pp. 1193 ss.

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 ss.

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 ss.

COUNCIL OF EUROPE STUDY, *Responsibility and IA*, 2019.

CRISCI S., *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm.*, n. 10, 2018, pp. 1787 ss.

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 ss.

D'ALESSANDRO F., *Market Abuse*, in CERA M. – PRESTI G. (a cura di), *Il testo unico finanziario*, Vol. II, Bologna, 2020, pp. 2166 ss.

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 ss.

DAVOLA A. – PARDOLESI R., *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?*, in *Danno resp.*, n. 5, 2017, pp. 616 ss.

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 ss.

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 ss.

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 ss.

DI CIOMMO F., Smart contract *e (non-) diritto. Il caso dei mercati finanziari*, in *Nuovo diritto civile*, n. 1, 2019, pp. 257 ss.

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 ss.

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 ss.

DONATI F., *Intelligenza artificiale e giustizia*, in *Riv. AIC* (*rivistaaic.it*), n. 1, 2020, pp. 415 ss.

DONATI F., *L'art. 21 della Costituzione settanta anni dopo*, in *Rivista di diritto dei media* (*medialaws.eu*), n. 1, 2018, pp. 93 ss.

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 ss.

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 ss.

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 ss.

FINOCCHIARO G., *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ.*, n. 2, 2018, pp. 441 ss.

FINOCCHIARO G., *Intelligenza artificiale e protezione dei dati personali*, in *Giur. it.*, n. 7, 2019, pp. 1670 ss.

FINOCCHIARO G., *Intelligenza artificiale e responsabilità*, in *Contr. impr.*, n. 2, 2020, pp. 713 ss.

FINOCCHIARO G., *La conclusione del contratto telematico mediante i software agents: un falso problema giuridico?*, in *Contr. impr.*, n. 2, 2002, pp. 500 ss.

FINOCCHIARO G., *La proposta di Regolamento sull'intelligenza artificiale: il modello basato sulla gestione del rischio*, in *Dir. inf.*, n. 2, 2022, pp. 303 ss.

FISCHEL D.R. – ROSS D.J., *Should the Law Prohibit Manipulation in Financial Markets*, in *Harvard Law Review*, Vol. 105, 1991, pp. 503 ss.

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 ss.

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 ss.

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 ss.

FLORIDI L. – SANDERS J.W., *In the Morality of Artificial Agents*, in *Mind and Machines*, Vol. 14, 2004, pp. 349 ss.

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 ss.

FROSINI T.E., *L'orizzonte giuridico dell'intelligenza artificiale*, in *Dir. inf.*, n. 1, 2022, pp. 465 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

GUNKEL D.J., *Mind the Gap: Responsible Robotics and the Problem of Responsibility*, in *Ethics and Information Technology*, Vol. 22, 2017, pp. 307 ss.

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 ss.

HALLEVY G., *The Criminal Liability of Artificial intelligence Entities*, in *Akron Intellectual Property Journal*, Vol. 4, Issue 2, 2010, pp. 171 ss.

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 ss.

HILGENDORF E., *Autonome Systeme, künstliche Intelligenz und Roboter*, in *Festschrift für Thomas Fischer*, München, 2018, pp. 111 ss.

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 ss.

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 ss.

Hu Y., *Robot Criminals*, in *Univ. Mich. Journal of Law Reform*, Vol. 52, n. 2, 2019, pp. 487 ss.

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 ss.

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 ss.

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 ss.

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 Kapitalmarkttrecht*, 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 ss.

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 ss.

KORSMO C., *High-Frequency Trading: A Regulatory Strategy*, in *U. Rich. L. Rev.*, Vol. 48, 2014, pp. 523 ss.

KRIPKE H., *The Mith of Informed Layman*, in *Bus. Law.*, Vol. 2, n. 2, 1973, pp. 631 ss.

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 ss.

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 ss.

LEDGERWOOD S.D. – CARPENTER P.R., *A Framework for the Analysis of Market Manipulation*, in *Rev. L. & Econ.*, Vol. 8, 2012, pp. 253 ss.

LEGG S.– HUTTER M., *A collection of definitions of intelligence*, in *Frontiers in Artificial Intelligence and Applications*, Vol. 157, 2007, pp. 17 ss. (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 ss.

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 ss.

LIN T.C.W., *Reasonable Investor(s)*, in *Boston Univ. L. Rev.*, Vol. 95, 2015, pp. 461 ss.

LIN T.C.W., *The New Investor*, in *UCLA L. Rev.*, Vol. 60, 2013, pp. 678 ss.

LIN T.C.W., *The new market manipulation*, in *Emory Law Journal*, Vol. 66, Issue 6, pp. 1252 ss.

LIN T.C.W., *Vistas of Finance*, in *UCLA L. Rev. Disc.*, Vol. 61, 2013, pp. 78 ss.

LINA D., *Could AI Agents Be Held Criminally Liable*, in *South Carolina L. Rev.*, Vol. 69, Issue 3, 2018, pp. 677 ss.

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 ss. (Parte I), e n. 4, 2020, pp. 1080 ss. (Parte II)

LOGLI A., *Poteri istruttori della Consob* e nemo tenetur se detegere, in *Giur. comm.*, n. 2, 2020, pp. 230 ss.

LOMBARDO S., *L'*insider *di se stesso alla luce della decisione della Corte di Cassazione (civile)*, in *Giur. comm.*, n. 4, 2018, pp. 666 ss.

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 ss.

LUCANTONI P., *L'*high frequency trading *nel prisma della vigilanza algoritmica del mercato*, in *Analisi giur. econ.*, n. 1, 2019, pp. 297 ss.

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 ss.

LUCIANI M., *La decisione giudiziaria robotica*, in *Riv. AIC* (*rivistaaic.it*), n. 3, 2018, 872 ss.

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 ss.

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 ss.

MADDEN T.M., *Significance and the Materiality Tautology*, in *J. Bus. & Tech. L.*, Vol. 10, 2015, pp. 217 ss.

MAGGINO F. – CICERCHIA G., *Algoritmi, etica e diritto*, in *Dir. inf.*, n. 6, 2019, pp. 1161 ss.

MAGRO M.B., *Biorobotica, robotica e diritto penale*, in PROVOLO D. – RIONDATO S. – YENISEY F., *Genetics, robotics, law punishment*, Padova, 2014, pp. 499 ss.

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 ss.

MAGRO M.B., *Robot, cyborg e intelligenze artificiali*, in CADOPPI A. – CANESTRARI S. – MANNA A. –PAPA M., *Cybercrime*, Torino, 2019, pp. 1180 ss.

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 ss.

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 ss.

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 ss.

MATTHIAS A., *The responsibility gap: Ascribing responsibility for the actions of learning automata*, in *Ethics Inf. Tech.*, n. 6, 2004, pp. 175 ss.

MAUGERI M., *Offerta pubblica di acquisto e informazioni privilegiate*, in *Riv. dir. comm.*, n. 2, 2018, pp. 267 ss.

MAUGERI M., *Cripto-attività e abusi di mercato*, in *Oss. dir. civ. e comm.*, Speciale/2022, pp. 413 ss.

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 ss.

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 ss.

MCNAMARA S.R., *The Law and Ethics of High-Frequency Trading*, in *Minn. J.L. Sci. & Tech.*, Vol. 17, Issue 1, 2016, pp. 135 ss.

MELONI C., *Command Responsibility in International Criminal Law*, The Hague, 2010, pp. 31 ss.

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 ss.

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 ss.

MONTALENTI P., *Abusi di mercato e procedimento Consob: il caso Grande Stevens e la Sentenza CEDU*, in *Giur. comm.*, n. 3, 2015, pp. 478 ss.

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 ss.

MOSCO G.D., *L'intelligenza artificiale nei consigli di amministrazione*, in *Analisi giur. econ.*, n. 1, 2019, pp. 247 ss.

MOSTACCI E., *L'intelligenza artificiale in ambito economico e finanziario*, in *DPCE online*, n. 1, 2022, pp. 361 ss.

MOTTURA C., *Decisione robotica negoziale e mercati finanziari*, in CARLEO A., *Decisione robotica*, Bologna, 2019, pp. 265 ss.

MUCCIARELLI F., *Sub art. 184*, in FRATINI M. – GASPARRI G. (a cura di), *Il testo unico della finanza*, Torino, 2012, pp. 2319 ss.

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 ss.

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 ss.

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 ss.

OLIVARES G.Q., *La Robotica ante et derecho penal*, in *Revista Electrónica de Estudios Penales y de la Seguridad*, n. 1, 2017, pp. 16 ss.

OPPO G., *Disumanizzazione del contratto*, in *Riv. dir. civ.*, 1998, pp. 525 ss.

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 ss.

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 ss.

PAPA M., Future crimes*: intelligenza artificiale e rinnovamento del diritto penale*, in *diSCrimen* (*discrimen.it*). 4 marzo 2020, pp. 9 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

PIERGALLINI C., *La responsabilità del produttore: una nuova frontiera del diritto penale?*, in *Dir. pen. proc.*, n. 9, 2007, pp. 1125 ss.

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 ss.

PITRUZZELLA G., *La libertà di informazione nell'era di Internet*, in *Rivista di diritto dei media* (*medialaws.eu*), n. 1, 2018, pp. 19 ss.

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 ss.

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 ss.

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 ss.

RESTA G., *Cosa c'è di 'europeo' nella proposta di Regolamento UE sull'intelligenza artificiale*, in *Contr. impr.*, n. 2, 2002, pp. 323 ss.

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 ss.

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 ss.

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 ss.

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 ss.

RUFFOLO U., *La "personalità elettronica"*, in RUFFOLO U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, pp. 213 ss.

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 ss.

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 ss.

SALANITRO U., *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, in *Riv. dir. civ.*, n. 6, 2020, pp. 1246 ss.

SALVADORI I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. proc. pen.*, n. 1, 2021, pp. 83 ss.

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 ss.

SARTORI F., *La consulenza finanziaria automatizzata: problematiche e prospettive*, in *Riv. trim. dir. econ.* (*fondazionecapriglione.luiss.it*), n. 3, 2018, pp. 253 ss.

SASSI S., *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, *Analisi giur. econ.*, n. 1, 2019, pp. 109 ss.

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 ss.

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 ss.

SCHWALBE U., *Algorithms, Machine Learning, and Collusion*, June 2018, in www.ssrn.com, pp. 1 ss.

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 ss.

SEYFERT R., *Algorithms as Regulatory Objects*, in *Information Communication and Society*, 2021, https://doi.org/10.1080/1369118X.2021.1874035, pp. 1 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

SOLUM L.B., *Legal Personood for Artificial Intelligences*, in *North Carolina L. Rev.*, Vol. 70, n. 4, 1994, pp. 1231 ss.

SPERA P., voce *Intelligenza artificiale*, in ZACCARI G.– PERRI P. (a cura di), *Dizionario Legal Tech*, Milano, 2020, pp. 535 ss.

STEINBERG M.I., *The Sec and the Securities Industry Respond to September 11*, in *International Lawyer*, Vol. 36, n. 1, 2002, pp. 131 ss.

STRAMPELLI G., *L'informazione societaria a quindici anni dal T.U.F.: profili evolutivi e problemi*, in *Riv. soc.*, n. 5, 2014, pp. 991 ss.

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 ss.

THOMAS W.R., *The Ability and Responsibility of Corporate Law to Improve Criminal Punishment*, in *Ohio St. L.J.*, Vol. 78, 2017, pp. 601 ss.

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 ss.

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 ss.

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 ss.

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 ss.

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 ss.

VERSTEIN A., *Benchmark Manipulation*, *B.C. L. Rev.*, Vol. 56, 2015, pp. 272 ss.

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 ss.

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 ss.

YADAV Y., *The Failure of Liability in Modern Markets*, in *Virginia L. Rev. Ass.*, Vol. 102, 2016, pp. 1031 ss.

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.

Recenti pubblicazioni

29 – maggio 2023
Quaderni giuridici
AI e abusi di mercato:
le leggi della robotica si applicano alle operazioni finanziarie?
F. Consulich, M. Maugeri, C. Milia, T.N. Poli, G. Trovatore

28 – aprile 2023
Quaderni giuridici
La mappatura dei prodotti finanziari nella prospettiva della tutela del risparmiatore
F. Annunziata, D. Colonnello, A. Lupoi
con prefazione di A. Sciarrone Alibrandi

27 – marzo 2023
Quaderni giuridici
Riforma della giustizia civile e tutela stragiudiziale: quali opportunità per cittadini e imprese?
Atti del convegno ACF – ANSPC – Sapienza Università di Roma
Roma, Auditorium CONSOB, 24 ottobre 2022

26 – febbraio 2023
Quaderni giuridici
Autorità indipendenti, anticorruzione e *whistleblowing*: le questioni aperte
Atti del convegno CONSOB - AGCM - Università degli Studi di Roma "Tor Vergata"
Roma, Auditorium CONSOB, 14 ottobre 2022

25 – gennaio 2023
Quaderni giuridici
Tokenizzazione di azioni e azioni *tokens*
P. Carrière, N. de Luca, M. de Mari, G. Gasparri, T.N. Poli;
con presentazione di A. Stagno d'Alcontres

11 – novembre 2022
Discussion papers
Profilazione della clientela ai fini della valutazione di adeguatezza
Follow up dello studio del 2012 su un campione di intermediari italiani
F. Adria, N. Linciano, F. Quaranta, P. Soccorso

89 – settembre 2022
Quaderni di finanza
Attitudine alla pianificazione finanziaria delle famiglie italiane
M. Brunetti, R. Ciciretti, M. Gentile, N. Linciano, P. Soccorso

24 – giugno 2022
Quaderni giuridici
Piccole e medie imprese e finanziamento del progetto imprenditoriale:
una ricerca per un nuovo tipo di emittente
D. Colonnello, E.R. Iannaccone, G. Mollo, M. Onza; con prefazione di R. Sacchi

23 – maggio 2022
Quaderni giuridici
Gli sviluppi tecnologici del diritto societario
a cura di
M. Bianchini, G. Gasparri, G. Resta, G. Trovatore, A. Zoppini

10 – luglio 2021
Discussion papers
L'industria del post-trading
S.G. Lo Giudice

9 – gennaio 2021
Discussion papers
Le OPA in Italia dal 2007 al 2019
Evidenze empiriche e spunti di discussione
F. Picco, V. Ponziani, G. Trovatore, M. Ventoruzzo; con introduzione a cura di R. Lener

22 – ottobre 2020
Quaderni giuridici
The Prospectus Regulation. The long and winding road
S. Alvaro, R. Lener, P. Lucantoni; in collaboration with V. Adriani, F. Ciotti, A. Parziale
introduced by Carsten Gerner-Beuerle

88 – novembre 2019
Quaderni di finanza
Who intends to become financially literate?
Insights from the Theory of Planned Behaviour
F.C. Billari, M. Gentile, N. Linciano, F. Saita

21 – settembre 2019
Quaderni giuridici
A 20 anni dal TUF (1998-2018): verso la disciplina della *Capital Market Union*?
Atti del convegno Banca d'Italia – Consob
Roma, Banca d'Italia, 6 novembre 2018

20 – gennaio 2019
Quaderni giuridici
La nuova via della seta e gli investimenti esteri diretti in settori ad alta intensità tecnologica
Il *golden power* dello Stato italiano e le infrastrutture finanziarie
S. Alvaro, M. Lamandini, A. Police, I. Tarola

19 – gennaio 2019
Quaderni giuridici
Investitori istituzionali, governo societario e codici di *stewardship*:
Problemi e prospettive
S. Alvaro, M. Maugeri, G. Strampelli

18 – dicembre 2018
Quaderni giuridici
Nuovi strumenti di politica industriale
per lo sviluppo e la quotazione delle PMI
S. Alvaro, S. Caselli, D. D'Eramo

7 – ottobre 2018
Position papers
La mappatura delle sedi di negoziazione in Italia
dopo l'entrata in vigore di MiFID II/MiFIR
Divisione Mercati, Ufficio Vigilanza Infrastrutture di Mercato

17 – settembre 2018
Quaderni giuridici
Le partecipazioni dei fondi alternativi riservati
in società quotate e in altri fondi
S. Alvaro, F. Annunziata; con prefazione a cura di M. Stella Richter jr

87 – settembre 2018
Quaderni di finanza
Boardroom gender diversity and performance
of listed companies in Italy
G.S.F. Bruno, A. Ciavarella, N. Linciano