UNIVERSITÀ COMMERCIALE “LUIGI BOCCONI”

SCUOLA DI DOTTORATO

Dottorato di Ricerca in Legal Studies

Ciclo: XXXVII

Settore Disciplinare: IUS/17

Negoziazione algoritmica, intelligenza artificiale e *market abuse* oltre l’*high frequency trading*: i profili di rilevanza penale

Advisor: Francesco MUCCIARELLI

Co-Advisor: Enrico BASILE

Tesi di Dottorato di

Maria DELLAGIACOMA

Matricola: 3176785

Anno 2025

INDICE

Introduzione..... VII

CAPITOLO I

IL TRADING ALGORITMICO, OLTRE L'*HIGH FREQUENCY TRADING*

1. Cenni storici sul progresso tecnologico in ambito finanziario: dai primi computer al *trading* algoritmico 1

1.1. La 'rivoluzione algoritmica' 8

2. Il trading algoritmico 9

3. L'*high frequency trading* 14

3.1. Definizioni 15

3.2 Le strategie di high frequency trading 19

3.2.1. Il market making 19

3.2.2. Il tick trading 19

3.2.3. L'arbitraggio 20

3.2.4. La liquidity detection 21

3.2.5. Lo smoking e lo spoofing 21

3.3. L'impatto *dell'high frequency trading* sui mercati: i benefici 23

3.4. L'impatto *dell'high frequency trading* sui mercati: i rischi 24

4. Intelligenza artificiale e strategie di trading 26

4.1. IA deboli e IA forti 31

4.2. IA assistita, IA aumentata, e IA autonoma 31

4.3. *Machine learning*: apprendimento supervisionato, non supervisionato e 'per rinforzo' 33

4.4. Autonomia e *black box*: la rilevanza penale 40

CAPITOLO II

IL CONTESTO NORMATIVO

1. Premessa 44
2. Le fonti normative sovranazionali 46
2.1. La Direttiva MAD II 48
2.2. Il Regolamento MAR 51
2.3. La Direttiva MiFID II 63
2.4 Gli interventi normativi più recenti: *AI Act* e *AI Liability Act Proposal* 69
3. La disciplina italiana 75
3.1. Premessa 75
3.2. Il reato di abuso di informazioni privilegiate 77
3.3. L'illecito amministrativo di abuso di informazioni privilegiate 80
3.4. Il reato di manipolazione del mercato 81
3.5. L'illecito amministrativo di manipolazione del mercato 87
3.6 Profili regolamentari 88

CAPITOLO III

LA RILEVANZA PENALE DEL *TRADING* ALGORITMICO

1. Il *trading* algoritmico: il necessario punto di partenza del dibattito sul potenziale offensivo dell'intelligenza artificiale 92
2. I concetti fondamentali del diritto penale finanziario e l'impatto del *trading* algoritmico: la nozione di informazione e il paradigma dell'investitore ragionevole 93
2.1. L'investitore ragionevole 95
2.2. L'informazione finanziaria 97
2.3. Le necessità di riforma 99
3. L'agire algoritmico e la sua riconducibilità al 'tipo' 100
3.1. Premessa 100
3.2. Le condotte astrattamente rilevanti come manipolazioni di mercato 101

3.2.1. Il *quote stuffing* 103
3.2.2. Lo *smoking*, lo *spoofing*, il *layering* e il *pinging* 103
3.2.3. La *liquidity detection* e il *momentum ignition* 104
3.2.4. Il *pump and dump*, il *trash and cash* e il *marking the close* 105
3.2.5. Le altre condotte potenzialmente abusive 106
3.3. Le condotte astrattamente rilevanti come abuso di informazioni privilegiate 107
3.4. La riconducibilità alle fattispecie incriminatrici 109
4. Le condotte concrete: casistica e simulazioni di mercato 113
4.1. Premessa 113
4.2. I procedimenti amministrativi: i casi Athena Capital Research LLC, Da Vinci Invest Limited e Paul Axel Walter 114
4.3. I procedimenti penali: United States v. Coscia e United States v. Navinder Singh Sarao 120
4.4. Gli studi sui mercati simulati 125
5. *Trading* algoritmico e *market abuse*: quale sanzione? 129
5.1 La prospettiva della responsabilità diretta della 'macchina' 130
5.1.1. Gli argomenti a sostegno della responsabilità penale diretta della 'macchina' 132
5.1.2. Gli argomenti contrari alla responsabilità penale diretta della 'macchina' 135
5.2 La responsabilità penale dell'uomo 144
5.2.1. Algoritmi, intelligenza artificiale e la prospettiva del rischio 145
5.2.2. Il *trading* algoritmico come attività a rischio consentito 150
5.2.3. I confini del *trading* algoritmico consentito: i doveri di organizzazione e controllo delle sedi di negoziazione e di chi svolge l'attività 154
6. Gli 'abusi di mercato algoritmici': i principali profili di problematicità 159
7. Gli 'abusi di mercato algoritmici': l'utilizzo di sistemi di negoziazione algoritmica 'tradizionali' 160
7.1. Gli 'abusi di mercato algoritmici' tradizionali: il primo scenario 160
7.2. Gli 'abusi di mercato algoritmici' tradizionali: il secondo scenario 165

8. I sistemi di negoziazione algoritmica basati su sistemi di intelligenza artificiale 'forte' 171

8.1. I sistemi di intelligenza artificiale forte e la crisi delle categorie tradizionali del diritto penale 172

8.2. La crisi del diritto penale d'evento e le specificità degli 'abusi di mercato algoritmici' 174

8.3. Sistemi di intelligenza artificiale 'forte' e gli 'abusi di mercato algoritmici': primo scenario 177

8.4. Sistemi di intelligenza artificiale 'forte' e gli 'abusi di mercato algoritmici': secondo scenario 177

8.5. Sistemi di intelligenza artificiale 'forte' e gli 'abusi di mercato algoritmici': terzo scenario 182

8.5.1. I limiti del rischio consentito: il fallimento delle regole cautelari che disciplinano l'attività 185

8.5.2. L'incertezza scientifica 188

8.5.3. La ridefinizione legislativa dell'area di rischio consentito 194

CAPITOLO IV

CONSIDERAZIONI CONCLUSIVE

1. *The American Way*: il *Financial Artificial Intelligence Risk Reduction Act* 197

1.1. La responsabilità del programmatore 198

1.1.1. Le previsioni che regolano l'*an* della responsabilità dell'uomo 198

1.1.2. Le previsioni che regolano il *quantum* della responsabilità dell'uomo. 199

1.2. I doveri del *Financial Stability Oversight Council* 200

1.3. Un bilancio sulla soluzione americana 201

2. Gli algoritmi di *trading* basati su sistemi di intelligenza artificiale c.d. 'forte' *e* il nuovo capitolo della 'società del rischio' 203

3. Una possibile prospettiva *de iure condendo* 208

BIBLIOGRAFIA 213

Introduzione

Il settore dei mercati finanziari, è ormai da decenni un osservatorio privilegiato per indagare quali siano le principali sfide poste dall'evoluzione tecnologica e dall'utilizzo di sistemi di intelligenza artificiale e in che termini si possa ipotizzare una responsabilità penale 'per il fatto dell'algoritmo'.
Si tratta infatti di un ambito in cui da tempo si fa ampio uso di sistemi automatizzati, non solo per la consulenza finanziaria (*robo-advisory*) e la valutazione del merito creditizio, ma anche e soprattutto per la negoziazione.

Quest'ultima attività, infatti, negli ultimi anni è stata oggetti di una vera e propria 'rivoluzione algoritmica', che ha visto il diffondersi di sistemi caratterizzati da differenti livelli di autonomia rispetto all'agire umano, nonché da vari gradi di capacità di autoapprendimento e di opacità nei meccanismi operativi.
La diffusione di tali sistemi, da un lato, apporta significativi benefici ai mercati in termini di efficienza e di aumento di liquidità; dall'altro lato, tuttavia, il loro impiego malevolo può determinare il turbamento del buon andamento dei mercati e della corretta formazione dei prezzi degli strumenti finanziari.
L'uso dei sistemi di negoziazione algoritmica può dunque costituire una nuova fonte di rischio per i mercati, poiché gli illeciti posti in essere 'da o tramite' sistemi algoritmici possono avere una portata offensiva incommensurabilmente maggiore, a causa dei volumi e della interconnessione che caratterizzano i mercati finanziari moderni.

Il presente studio pone perciò l'accento sulla negoziazione algoritmica, analizzandone in modo compiuto le caratteristiche e tentando di superare la genericità del dibattito sul ruolo degli algoritmi in questo settore.
L'analisi delle diverse funzioni svolte dagli algoritmi di *trading* consente infatti di individuare le specifiche tipologie di rischio e pericolosità di cui ciascuna di esse è foriera, al fine di comprendere la capacità dell'attuale sistema di tutelare efficacemente l'integrità dei mercati, bene giuridico attorno al quale sono costruite le fattispecie penali in materia finanziaria.
Si tratta, in altri termini, di stabilire se e in quali termini i suddetti sistemi possano essere coinvolti nella commissione di abusi di mercato e se l'attuale sistema sanzionatorio sia in grado di fornire un'adeguata risposta a tale fenomeno.

A tal fine, innanzitutto, si illustrerà, nel primo capitolo, l'evoluzione storica dell'utilizzo delle tecnologie nel settore finanziario, i sistemi di negoziazione

attualmente in uso e le principali strategie che tali sistemi sono in grado di porre in essere.

Mentre, nel secondo capitolo, si analizzerà l'attuale disciplina – nazionale e sovranazionale – che regola i reati di *market abuse*¸ con specifico riferimento alle disposizioni che riguardano l'uso di sistemi di negoziazione algoritmica.

Al terzo capitolo è dedicata invece l'indagine sui possibili profili di rilevanza penale del *trading* algoritmico.

Si valuterà, in primo luogo, se l'introduzione dei sistemi di negoziazione algoritmica influisca su alcuni concetti fondamentali del diritto penale finanziario. In secondo luogo, si analizzerà la riconducibilità delle strategie di *trading* realizzate da o tramite algoritmi alle fattispecie incriminatrici attualmente vigenti, nella loro componente oggettiva.

In terzo luogo, si individuerà il soggetto responsabile dell''abuso di mercato algoritmico'. Con riferimento a quest'ultimo profilo, si valuterà a che titolo ed entro quali limiti l'essere umano possa rispondere delle conseguenze dannose determinate dall'operare dell'algoritmo, con specifico riferimento agli algoritmi di *trading*, collocando il *trading* algoritmico nell'ambito delle attività a rischio consentito e illustrando le ragioni per cui l'agire abusivo degli algoritmi di *trading* segni nuova fase della moderna 'società del rischio'.

Posta questa considerazione generale, al fine di individuare il soggetto responsabile, si distinguerà fra diverse ipotesi di 'abuso di mercato algoritmico': i) l'utilizzo deliberato e malevolo dell'algoritmo di *trading*; ii) la mancata o inadeguata programmazione dell'algoritmo rispetto alle norme che governano l'attività e iii) la mancata adozione di misure ulteriori rispetto a quelle previste dalle regole che governano l'attività, di cui era prevedibile il fallimento.

Proprio rispetto a quest'ultima ipotesi si coglierà, infine, il principale punto di contatto fra potenziale diffusione di sistemi di negoziazione algoritmica capaci di agire sui mercati in modo, per così dire, 'autonomo' e la categoria del rischio consentito. Si tratta di uno scenario che apre la strada a tematiche ampiamente affrontate dalla dottrina che si è occupata del tema del rischio consentito – i limiti dell'affidamento che l'agente può riporre nella regola cautelare, il suo fallimento e il suo intrecciarsi con l'assenza di conoscenze scientifiche circa la pericolosità di una determinata attività – e che verrà affrontato attraverso un confronto con il la disciplina del rischio ambientale.

Tanto porterà a concludere che, pur ritenendosi che l'attuale sistema fornisca adeguati strumenti di contrasto agli 'abusi di mercato algoritmici' e che rispetto ai reati finanziari non si possa parlare di 'crisi del diritto penale d'evento',

ciò nonostante, pare auspicabile intervento legislativo, in una duplice direzione. Da un lato, si propone una rivalutazione dell'adeguatezza delle regole che governano l'attività di negoziazione algoritmica in relazione a tecnologie che allo stato attuale non hanno la stessa diffusione degli algoritmi di *trading* 'tradizionali', ma di cui si può prospettare il prossimo utilizzo. Dall'altro lato, si ipotizza una riformulazione delle fattispecie di manipolazione del mercato e abuso di informazioni privilegiate, capace di presidiare con la sanzione penale anche gli abusi di mercato colposi commessi utilizzando sistemi automatizzati.

CAPITOLO I

IL TRADING ALGORITMICO, OLTRE L'*HIGH FREQUENCY TRADING*

SOMMARIO: 1. Cenni storici sul progresso tecnologico in ambito finanziario: dai primi computer al *trading* algoritmico – 1.1. La 'rivoluzione algoritmica – 2. Il *trading* algoritmico – 3. L'*high frequency trading* – 3.1. Definizioni – 3.2. Le strategie di *high frequncy trading* – 3.2.1. Il *market making* – 3.2.2. Il *tick trading* – 3.2.3. L'arbitraggio – 3.2.4. La *liquidity detection* – 3.2.5. Lo *smoking* e lo *spoofing* – 3.3. L'impatto dell'*high frequency trading* sui mercati: i benefici – 3.4. L'impatto dell'*high frequency trading* sui mercati: i rischi – 4. Intelligenza artificiale e strategie di trading – 4.1. IA deboli e IA forti – 4.2. IA assistita, IA aumentata, e IA autonoma – 4.3. *Machine learning*: apprendimento supervisionato, non supervisionato e 'per rinforzo' – 4.4. Autonomia e *black box*: la rilevanza penale

1. Cenni storici sul progresso tecnologico in ambito finanziario: dai primi computer al *trading* algoritmico

Una compiuta analisi delle implicazioni penalistiche del *trading* algoritmico (incluso quello basato su sistemi di intelligenza artificiale), impone innanzitutto di esaminare l'evoluzione e lo stato attuale dei sistemi utilizzati nella realtà dei mercati.

Il progresso tecnologico in ambito finanziario, così come in tutti i settori dell'agire umano, non è certo un fenomeno inedito[1].

[1] In questa sede ci si concentra sull'evoluzione dei sistemi di *trading* algoritmico, anche basati su sistemi di intelligenza artificiale.
Per analizzare lo sviluppo dell'intelligenza artificiale nel suo complesso, si deve tornare indietro al 1956 per individuare il momento della nascita dell'IA come nuova disciplina scientifica (a seguito degli studi pionieristici di Alan Turing negli anni '40 sull'intelligenza delle macchine e l'elaborazione del celebre test di Turing del 1950).
Nei primi anni, la ricerca sull'intelligenza artificiale (1956-1974), si risolveva sostanzialmente nella programmazione di sistemi per risolvere compiti sulla base di regole logiche "se-allora".
La seconda fase di evoluzione dell'IA come oggetto di studi scientifici risale invece agli anni '80, in concomitanza con il progetto giapponese del computer di quinta generazione (FGCS). Il progetto aveva l'obiettivo di sviluppare computer in grado di portare avanti conversazioni, tradurre lingue, interpretare immagini, e ragionare come gli esseri umani (c.d. sistemi esperti). In questa fase si collocano anche lo sviluppo del sistema MYCIN (sviluppato per aiutare i medici a diagnosticare le infezioni batteriche), del sistema XCON, (utilizzato dalla Digital Equipment Corporation per configurare i loro ordini di computer)

Nel corso dell'ultimo secolo, il *trading* sui mercati finanziari ha subito un profondo cambiamento, tanto da rendere particolarmente obsoleta l'immagine cinematografica dell'agente di borsa che in una mano tiene la cornetta del telefono e con l'altra si sbraccia urlando per concludere una transazione.
Storicamente e fino agli anni '70, le borse valori erano luoghi fisici in cui le persone si incontravano per negoziare e compiere transazioni. Il *trading* nei mercati finanziari comportava elevati costi di transazione e il livello di tecnologia utilizzato era assai contenuto[2]. In quel contesto storico gli scambi erano quindi estremamente dipendenti dalle capacità e dall'esperienza del singolo essere umano.

Negli Stati Uniti, il processo di 'elettronificazione' del *trading* prese avvio nel 1969 con l'istituzione da parte della Institutional Networks Corporation[3] di Instinet, il primo sistema elettronico di scambio titoli, grazie al quale era possibile visualizzare le offerte e concludere transazioni tramite computer. L'obiettivo dei fondatori era infatti quello di competere con la Borsa di New York, mettendo a disposizione di banche, fondi comuni di investimento e compagnie di assicurazioni collegamenti informatici che garantissero scambi immediati, minori costi e maggiore velocità ed efficienza rispetto al sistema tradizionale.
A ciò si aggiunse, due anni dopo, la creazione del Nasdaq: la prima borsa esclusivamente elettronica. In origine, i computer servivano solo per diffondere le informazioni dei prezzi in modo continuo e non anche a connettere gli operatori: il passaggio degli ordini, fino al 1987, avveniva infatti via telefono. La diffusione delle quotazioni per via telematica, comunque, garantiva un notevole aumento della trasparenza e dell'efficienza di mercato[4].

La terza fase, iniziata a metà degli anni '90 e tuttora in corso, è caratterizzata dall'emergere dell'apprendimento automatico (*machine learning*) e delle reti neurali. Queste tecnologie permettono ai computer di migliorare le loro prestazioni analizzando grandi quantità di dati invece di essere programmati con regole esplicite. Questo cambiamento di paradigma è stato reso possibile dai progressi nell'hardware, dalla disponibilità di grandi dataset e dallo sviluppo di nuovi algoritmi.

[2] D. LEIS, *High Frequency Trading: Market Manipulation and Systemic Risks from an EU Perspective*, in https://ssrn.com/abstract=2108344., 2012, pp. 1-81.

[3] La società è stata fondata da Jerome M. Pustilnik e Herbert R. Behrens. Per una ricostruzione storica, con specifico riferimento a Instinet, si veda R.A. SCHWARTZ−J.A. BYRNE−E. STEMPEL, *Rapidly Changing Securities Markets: Who Are the Initiators?*, Springer, 2017, pp. 1-13.

[4] https://www.borsaitaliana.it/notizie/sotto-la-lente/nasdaq.htm.

Nel 1976, fu il NYSE[5] a compiere un ulteriore passo verso l'automazione, lanciando il sistema DOT (*Designated Order Turnaround*), seguito dal super-DOT nel 1984. Questi sistemi permettevano ai c.d. *broker on the floor* di trasmettere elettronicamente la maggior parte degli ordini agli schermi degli specialisti.

Diversamente, nel contesto europeo, e in particolare nel Regno Unito, un importante contributo verso il progresso tecnologico nella finanza è dipeso da una serie di interventi legislativi adottati nel 1986 dall'amministrazione Thatcher, il c.d. "Big Bang". Quest'ultimo aveva previsto, tra l'altro, la creazione di un sistema di *trading* completamente nuovo, che consisteva in una rete di *trading* elettronico denominato "SEAQ".

Nel loro complesso, i cambiamenti tecnici e normativi sin qui descritti hanno determinato un primo ed enorme impatto sul sistema degli scambi, rendendo sempre meno indispensabile la presenza fisica dell'essere umano e sempre più irrinunciabile il ricorso alla tecnologia e all'informatica.

Non solo, gli sviluppi citati hanno incrementato la globalizzazione dei mercati, la concorrenza, stimolato l'innovazione finanziaria e posto le basi per una "corsa alla tecnologia", tuttora in atto.

Per anni, l'avvento della tecnologia nel settore finanziario è stato descritto come fenomeno avveniristico, lontano a venire, di cui erano ignoti l'impatto sui mercati, i rischi e i benefici e le sfide che avrebbe posto dal punto di vista legislativo.

Per contro, negli ultimi decenni si è assistito a un rapido processo evolutivo che ha reso quantomai reale l'integrazione e la progressiva sostituzione dell'essere umano da parte delle 'macchine intelligenti'.

Al termine degli anni Novanta, infatti, si è iniziato a porre le basi, tecnologiche e normative, per la diffusione del c.d. *trading* algoritmico, divenuto oggi un fenomeno diffuso, ampiamente conosciuto e regolato dal legislatore italiano ed europeo. Si tratta di una trasformazione che ha mutato l'essenza della finanza moderna, rendendolo a tutti gli effetti un contesto in cui le macchine e gli esseri umani condividono potere e operatività.

Di fatto, oggi, praticamente ogni istituzione finanziaria utilizza forme di forme di tecnologia avanzata – se non di intelligenza artificiale – per l'analisi del rischio e la gestione degli investimenti, attività prima ad appannaggio dei soli esseri umani. Alcuni *hedge fund* utilizzano *software* e algoritmici per leggere le notizie, analizzare i dati e selezionare i titoli.

---

[5] Acronimo di New York Stock Exchange, la principale borsa statunitense fondata nel 1792

BlackRock, la più grande società di gestione del risparmio al mondo, ha creato un *business* significativo creando e offrendo ai suoi clienti istituzionali un *software* – Aladdin – per la gestione del rischio e l'allocazione degli investimenti[6].
In generale, sempre più aziende, utilizzano esclusivamente sistemi algoritmici per gestione le attività degli investitori, rinunciando completamente al modello tradizionale del consulente finanziario.

Quanto poi alle strategie di negoziazione algoritmica, l'utilizzo di potenti sistemi di *hardware* e sofisticati *software* di *trading* e un atteggiamento normativo e regolamentare particolarmente propenso al progresso tecnologico hanno consentito l'affermazione e l'espansione del fenomeno del *trading* algoritmico ad alta frequenza (o *high frequency trading, hft*).

Uno dei primi impulsi alla nascita dell'*hft* è stato offerto dalla decisione con cui la Securities and Exchange Commission ha permesso, all'inizio degli anni '90, l'utilizzo degli Electronic Communications Networks (ECN)[7] come sistema di *trading* alternativo rispetto ai mercati regolamentati. Gli ECN, usando la tecnologia computerizzata, hanno reso possibile usufruire di un mercato alternativo dove chi vende e chi compra si incontra in maniera "automatica", senza passare attraverso i servizi offerti dai *broker-dealer* (come invece avveniva sui tradizionali mercati regolamentati)[8].

---

[6] Aladdin, sebbene non sia propriamente un sistema di intelligenza artifciale, utilizza per i fini sopracitati forme di tecnologie estremamente avanzata. Cfr. B. HOPE, *How Computers Trawl a Sea of Data for Stock Picks*, in Wall street Journal, 2015. Sul punto anche, T. C. W. LIN, *The New Market Manipulation*, in Emory Law Journal, vol. 66, 2017, p. 1253: "During the financial crisis of 2008, BlackRock, using Aladdin, assisted the federal government with its critical and thorny decisions relating to the bailouts of distressed firms like AIG, Bear Stearns, and Citigroup".

[7] Una rete elettronica estranea ai mercati regolamentati che consente gli scambi di strumenti finanziari garantendo la *best execution*. Nel sistema regolamentare comunitario gli ECN corrispondono approssimativamente agli MTF (*Multilateral Trading Facility*) disciplinati dalla MiFID.

[8] Cfr. A. PUORRO, *High frequency trading: una panoramica*, in *Questioni di Economia e Finanza* n. 198, p. 9. Nei primi tempi, la struttura degli ECN era, tuttavia, nettamente separata dai mercati regolamentati, dove gli ordini di contrattazione inviati agli ECN non potevano essere trasmessi (c.d. *chinese wall*). Se su un ECN non era presente il miglior prezzo di acquisto o vendita (presente invece su altro ECN o sui mercati regolamentari), l'operazione di acquisto o vendita sugli ECN non sarebbe stata vantaggiosa quanto quella che si sarebbe potuta compiere sui mercati regolamentati. La potenziale presenza di prezzi diversi per gli stessi strumenti finanziari aumentava la possibilità di arbitraggi, con il rischio che questo sistema danneggiasse i *trader* ignari di quale fosse il miglior prezzo presente sul mercato. Ciò determinava l'impossibilità di fatto di operare in modo sufficientemente rapido da sfruttare le differenze di prezzo degli stessi strumenti finanziari fra ECN e mercati regolamentati. A. PUORRO, *High frequency trading*, *op. cit.*, p. 7 "l'arbitraggio, però, avveniva sistematicamente ai danni dei *trader* che non potevano

Un ulteriore atto della SEC che ha stimolato, seppur indirettamente, lo sviluppo dei sistemi di negoziazione ad alta frequenza è poi la "National Market System Regulation"[9] del 2005 e in particolare due norme: la "Sub Penny Rule" (o Rule 611)[10] e la "Order Protection Rule" (o "Rule 611)[11].

La prima – "Sub Penny Rule" – ha imposto a tutti i mercati presenti sul territorio USA di utilizzare il sistema decimale per calcolare le quote dei prezzi dei titoli azionari superiori o uguali all'unità. Lo scopo della norma era ridurre a un centesimo di dollaro il *tick-size*[12] e di renderlo univoco, in modo tale da restringere lo *spread bid-ask*. Ciò ha aperto alla possibilità di ottenere guadagni marginali unitariamente minuscoli per la singola operazione, ma cumulativamente rilevanti per gli operatori in grado di processare numerosissime operazioni in tempi ridotti e dunque ha spinto gli operatori a sviluppare sistemi in grado di ridurre i tempi di esecuzione delle operazioni per accumulare maggiori profitti[13].

---

conoscere il miglior prezzo presente sul mercato, in quanto gli arbitraggisti compravano (vendevano) dal *trader* "non informato" e vendevano (compravano) al prezzo migliore presente sul mercato. […] Per evitare tale sistematico svantaggio per alcune categorie di *trader*, la SEC è intervenuta nel 1997 inserendo l'obbligo del "Limit Order Display" con il quale, allo scopo di migliorare la trasparenza del mercato, ha imposto ai Market Maker di mostrare a tutti i *trader* quale fosse il miglior prezzo di acquisto e vendita (National Best Bid Offer, NBBO) presente in qualsiasi momento sull'intero mercato (ECN compresi)".

[9] http://www.sec.gov/rules/final/34-51808.pdf

[10] http://www.sec.gov/divisions/marketreg/subpenny612faq.htm

[11] http://www.sec.gov/divisions/marketreg/nmsfaq610-11.htm

[12] "Per *tick size* si intende l'incremento minimo a cui può essere soggetto il prezzo di azioni, contratti *future* o altri strumenti negoziati in un *book* di negoziazione. I *tick size* possono essere gli stessi per tutti gli strumenti finanziari della medesima asset class oppure differire a seconda del prezzo degli strumenti finanziari in modo che a livelli di prezzo più alti corrispondano *tick size* più ampi. Solitamente, anche la liquidità del mercato ha un impatto sui *tick size*, per cui a strumenti finanziari più liquidi corrispondono *tick size* più piccoli. Nel tempo si è osservata una tendenza alla progressiva riduzione dei *tick size* adottati per le azioni dalle *trading venue*, che ha favorito strategie di esecuzione congeniali agli *hft*r quali, ad esempio l'immissione di ordini mirati a verificare la profondità (*depth*) del *book* di negoziazione, ovvero il "saltare la fila" per posizionarsi nella parte alta del book stesso. Con *tick size* più sottili, infatti, si riduce il costo di siffatte strategie a svantaggio degli investitori tradizionali più inclini a negoziazioni '*queue-oriented*" così V. CAIVANO–S. CICCARELLI–G. DI STEFANO–M. FRATINI– G. GASPARRI–M. GILIBERTI–N. LINCIANO–I. TAROLA, *Il* trading *ad alta frequenza. Caratteristiche, effetti, questioni di* policy, in *Consob Discussion Papers n.5*, 2012, p. 11.

[13] A. PUORRO, *High frequency trading*, *op. cit.*, p. 15. Nello stesso senso: S. ALVARO–M. VENTORUZZO, «High-Frequency Trading»: *note per una discussione*, in Banca impresa e società, 2016, vol. 35, issue 3, p. 424 secondo do cui la "decimalizzazione", ossia la riduzione del *tick* di negoziazione, che rappresenta il minimo salto di prezzo che gli strumenti quotati possono compiere hanno favorito lo sviluppo delle strategie *hft*, rendendo possibili guadagni marginali unitariamente minuscoli ma cumulativamente rilevanti per operatori in grado di processare

La seconda norma –"Order Protection Rule" –, invece, ha imposto la negoziazione al "National Best Bid Offer" (o "NBBO") di ogni ordine immesso sul mercato o su un ECN, prevedendo che se l'ECN o il mercato regolamentato che riceve l'ordine non è in grado di offrire il miglior prezzo, deve obbligatoriamente trasferirlo per l'esecuzione sul mercato in cui è presente il "NBBO".
Disposizioni analoghe sono state emanate in ambito europeo con la Direttiva MiFID I[14], che ha rimosso l'obbligo di concentrazione degli scambi azionari solo sui mercati regolamentati (e permesso quindi lo sviluppo delle "Multilateral Trading Facilities", o "MTF")[15] e previsto l'obbligo della "Best Exectuion"[16].
Queste previsioni, statunitensi ed europee[17], insieme alla tendenza alla frammentazione dei mercati in atto favorita dallo sviluppo di MTF – su cui vengono quotati strumenti finanziari presenti anche sui mercati regolamentati –

---

numerosissime operazioni in tempi record". Gli Autori riportano come negli USA a partire dai primi anni duemila, "le borse abbandonarono le quotazioni in quarti, passando da un *tick* minimo di 1/16 di dollaro a $0.01 e riducendo quasi immediatamente di un sesto la differenza tra prezzi denaro e lettera".

[14] Direttiva 2014/65/UE del Parlamento europeo e del Consiglio del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la Direttiva 2002/92/CE e la Direttiva 2011/61/UE.

[15] Si tratta di un'alternativa alle borse valori tradizionali in cui viene effettuato un mercato di titoli, tipicamente utilizzando sistemi elettronici. Il concetto è stato introdotto dalla Direttiva MiFID I. L'articolo 4 par. 15 della Direttiva descrive il sistema multilaterale di negoziazione come un sistema "gestito da un'impresa di investimento o da un gestore del mercato che consente l'incontro - al suo interno ed in base a regole non discrezionali - di interessi multipli di acquisto e di vendita di terzi relativi a strumenti finanziari, in modo da dare luogo a contratti ai sensi delle disposizioni del titolo II". Ai fini della Direttiva, il termine "regole non discrezionali" significa che "le regole non lasciano all'impresa di investimento che gestisce un sistema multilaterale di negoziazione alcuna discrezionalità su come possano interagire gli interessi. Le definizioni prescrivono che gli interessi si incontrino in modo tale da dare luogo ad un contratto, il che significa che l'esecuzione ha luogo in base alle regole del sistema o tramite i suoi protocolli o le sue procedure operative interne" (Considerando 6). Il sistema multilaterale di negoziazione può essere gestito da un operatore di mercato o da un'impresa di investimento, mentre la gestione di un mercato regolamentato non è considerata un servizio di investimento ed è svolta esclusivamente da operatori di mercato autorizzati.

[16] Considerando 33 Direttiva 2004/39/CE: "È necessario imporre effettivamente alle imprese di investimento un obbligo di esecuzione alle condizioni migliori in modo da garantire che esse eseguano gli ordini alle condizioni più favorevoli per il cliente. Questo obbligo dovrebbe applicarsi alle imprese di investimento che hanno obblighi di natura contrattuale o derivanti da un rapporto di intermediazione nei confronti del cliente".

[17] S. ALVARO–M. VENTORUZZO, «High-Frequency Trading*»: note*, *op. cit.,* pp. 422-423, sottolineano le differenze fra l'intervento del legislatore statunitense e quello europeo. Gli Autori sostengono che, il NMS emanato negli USA nel 2005, nel prevedere l'obbligo di negoziazione e esecuzione delle operazioni alla "National Best Bid Offer", ha previso anche - proprio al fine di

hanno indotto gli operatori a cercare un'infrastruttura tecnologica in grado di stare al passo con le esigenze di contrattazione al miglior prezzo presente su ciascun mercato.

Infine, vi è un terzo fattore che ha condizionato e favorito lo sviluppo dell'*hft*: l'apertura al c.d. accesso diretto al mercato[18] da parte del *buy side* dell'industria finanziaria[19]. Si tratta, in pratica, della possibilità per l'impresa di investimento di "stipulare con il proprio *broker* un contratto che non solo consenta l'invio dei propri ordini al mercato senza intervento di quest'ultimo, sebbene utilizzando le sue stesse infrastrutture informatiche; bensì anche di trasmetterli

---

calcolare le migliori condizioni esistenti sul mercato - un obbligo dei gestori di mercati e altre piattaforme di scambio di inviare in tempo reale le proprie quotazioni a un sistema informatico centralizzato. Ciò ha imposto alle diverse piazze la creazione di un collegamento in modo che "ciascun ordine venga automaticamente deviato verso il luogo di negoziazione che offre il NBBO". Di qui, l'accesa competizione tra gestori di sistemi di scambi per offrire le migliori condizioni, che attraggono ordini e generano volumi.

Lo stesso sistema integrato di scambio di informazioni e ordini tra le borse e i sistemi di scambio alternativi non è stato previsto, sottolineano gli Autori, dal il legislatore europeo. La Direttiva MiFID si è infatti limitata a prevedere la mera la regola "Best Exectuion", senza riprodurre una forma di "esternalizzazione ai mercati" del rispetto delle migliori condizioni possibili.

Per questa ragione, gli Autori evidenziamo come "sebbene su entrambi i lati dell'Atlantico queste previsioni hanno creato maggiore competizione fra borse e piattaforme di scambio, gli automatismi previsti dal sistema americano, hanno reso più rilevante, per i gestori dei mercati, attrarre ordini, e quindi hanno dato maggiore centralità all'*hft*, come dimostrato dai volumi di negoziazioni ad alta frequenza che, pur significativi sia in USA che in Europa, sono superiori nel primo sistema".

[18] Si fa riferimento ai concetti di S*ponsored Access* (SA) e di *direct market access* (DMA), che rappresentano un sottoinsieme del D*irect Electronic Access* (DEA), ovvero di accesso diretto al mercato. Come chiariscono V. CAIVANO–S. CICCARELLI–G. DI STEFANO–M. FRATINI– G. GASPARRI–M. GILIBERTI–N. LINCIANO–I. TAROLA, *Il* trading *ad alta frequenza*, *op. cit.*, p. 11, "con il DMA i soggetti (intermediari e non) possono accedere al mercato senza diventare membri dello stesso, utilizzando le infrastrutture e i sistemi messi a disposizione da un partecipante al mercato e il codice identificativo di negoziazione di quest'ultimo. […] In modo analogo, lo Sponsored Access consente l'accesso diretto alla piattaforma di negoziazione, senza tuttavia passare per l'infrastruttura e il sistema messo a disposizione dal membro del mercato, bensì solo utilizzandone il codice identificativo. In generale, il Direct Electronic Access offre ai soggetti che se ne avvalgono vantaggi analoghi a quelli della membership, ma con minori costi anche in termini di adempimenti legali. Consente inoltre di mantenere l'anonimato nei confronti del mercato e degli altri partecipanti e, in particolare, di gestire la connessione con la piattaforma in modo del tutto autonomo rispetto al sistema di negoziazione del soggetto membro del mercato (intermediario e non), eventualmente ottenendo risultati migliori in termini di latenza".

[19] Così S. ALVARO–M. VENTORUZZO, *«High-Frequency Trading»: note*, *op. cit.,* p. 424, nt. 18: "per «sell side» si intendono i soggetti autorizzati alla negoziazione su mercati regolamentati, quelli che negli USA si chiamano «brokers», e che offrono i propri servizi di negoziazione per conto terzi al «buy side», categoria ampia che può andare da sofisticati hedge funds a giganteschi fondi pensione, da speculatori individuali a banche che non hanno accesso diretto a un particolare mercato sul quale vogliono operare".

direttamente al mercato usando le credenziali di accesso dell'intermediario finanziario, senza che l'ordine transiti per i suoi sistemi"[20]. Riducendo i passaggi, si sono velocizzate sensibilmente le operazioni.

L'insieme di questi fattori ha quindi favorito lo sviluppo di un sistema di avanzato livello tecnologico, in cui le 'macchine' agiscono, insieme all'essere umano, come attori principali[21]. In ambito finanziario come in altri settori, l'automazione computerizzata e l'intelligenza artificiale stanno acquisendo un ruolo sempre più rilevante e complementare all'intelligenza e alla capacità analitica umana, mutando profondamente i meccanismi di funzionamento dei mercati[22].

1.1. La 'rivoluzione algoritmica'

L'evoluzione che ha interessato le piattaforme di investimento ha riguardato il *trading* algoritmico, l'*high frequency trading*, fino ad arrivare ai sistemi di intelligenza artificiale.

Si tratta di una vera e propria 'rivoluzione algoritmica'[23] che, solo negli ultimi decenni, ha plasmato l'architettura e il funzionamento dei mercati finanziari globali e continuerà a farlo in modo sempre più pervasivo nel futuro. Infatti, l'industria finanziaria sta attualmente vivendo questa profonda trasformazione sostenuta dall'intelligenza artificiale, in particolare per quanto attiene alla

---

[20] Così S. ALVARO–M. VENTORUZZO, «*High-Frequency Trading*»: *note*, *op. cit.,* p. 424.

[21] Cfr. T.C.W. LIN, *The new Investor*, in UCLA Law Review, 2013, vol. 60, p. 681.

[22] In questo senso T.C.W. LIN, *The New Market Manipulation*, op*. cit.*, 2017, p. 1255, nonché A. AZZUTTI–W.G. RINGE–H.S. STIEHL, *Regulating AI Trading from an AI Life Cycle Perspective*, in N. Remolina–A. Gurrea-Martinez (eds.), Artificial Intelligence in Finance: Challenges, Opportunities and Regulatory Developments, Edward Elgar, 2023, pp. 198-243 e ID, *Machine Learning, Market Manipulation, and Collusion on Capital Markets: Why the "Black Box" Matters*, in University of Pennsylvania Journal of International Law, vol. 43, issue 1, 2021, p. 84 secondo cui la "rivoluzione algoritmica" ha plasmato l'architettura e il funzionamento dei mercati globali, portando a ritenere che gli algoritmi continueranno a guadagnare un ruolo sempre più pervasivo. Nella finanza globale, infatti, già allo stato attuale, gli algoritmi contribuiscono a condurre, gestire e monitorare le attività di *trading*, talvolta causando anche interruzioni al corretto funzionamento dei mercati. Per questa ragione, gli Autori ritengono particolarmente apprezzabile il fatto che l'innovazione tecnologica finanziaria sia stata supportata dalla regolamentazione europea per favorire lo sviluppo di mercati più efficienti e favorire la concorrenza fra i partecipanti.

[23] L'espressione è di A. AZZUTTI–W.G. RINGE–H.S. STIEHL, *Regulating AI Trading*, *op. cit.*, pp. 198-243. Come sottolinea F. CONSULICH, Flash offenders*. Le prospettive di* accountability *penale nel contrasto alle intelligenze artificiali devianti*, in Riv. It. Dir. Proc. Pen., 2022, fasc. 3, p. 1018, "quello dei mercati finanziari è certamente il campo che più di ogni altro ha sperimentato le sfide dell'intelligenza artificiale. […] Le transazioni sono oggi per lo più compiute da operatori non fisici e i soggetti meno reattivi ai cambiamenti tecnologici in corso […] sono esposti alle ingiurie arrecate loro dai famigerati algoritmi per la negoziazione ad alta frequenza […]".

gestione e al monitoraggio delle attività di *trading*. Per questo motivo, l'evoluzione tecnologica in ambito finanziario è stata generalmente supportata anche dai legislatori, al fine di favorire la concorrenza tra i partecipanti al mercato su diversi livelli, con l'obiettivo di sostenere lo sviluppo di mercati più efficienti e liquidi. Allo stesso tempo, proprio le strategie algoritmiche sviluppate negli ultimi anni per adeguare le esigenze degli operatori alla struttura di mercato hanno suscitato grande interesse della letteratura specialistica[24].

Gli strumenti tecnologici che fanno parte di questa rivoluzione hanno specifiche caratteristiche e si distinguono per differenti livelli di autonomia rispetto all'agire umano, nonché vari gradi di capacità di autoapprendimento e di opacità nei meccanismi operativi.

Elemento comune è che ciascuna di queste tecnologie può – oltre ai benefici già elencati – costituire una nuova fonte di rischio per i mercati e, nello specifico, facilitare (nuove) forme di abusi di mercato. Occorre dunque analizzarle in modo compiuto, al fine di comprendere la capacità dell'attuale sistema di tutelare efficacemente l'integrità, bene giuridico attorno al quale sono costruite le fattispecie penali in materia finanziaria.

Nell'esplorare le possibili implicazioni sul piano penalistico del ricorso al *trading* algoritmico (anche basato su intelligenza artificiale), si volgerà quindi lo sguardo agli strumenti attualmente più utilizzati nella prassi finanziaria.

L'obiettivo è superare la genericità del dibattito sul ruolo degli algoritmi in questo settore, riconoscendo la diversità delle funzioni svolte dagli algoritmi di *trading* e, di conseguenza, individuare le specifiche tipologie di rischio e pericolosità di cui ciascuna di esse è foriera.

2. Il trading algoritmico

'Trading algoritmico' è un termine generico usato per descrivere tutte le strategie in cui gli ordini sono inviati al mercato secondo un insieme pre-programmato di regole. In altre parole, è a un processo che utilizza istruzioni di *trading* automatizzate, programmato per tenere conto di variabili come il prezzo, la tempistica e il volume. Le decisioni che riguardano il se, il quando e a che prezzo inviare l'ordine sono definite dall'algoritmo. Tipicamente il *trading*

[24] C.L. DUNIS–P.W. MIDDLETON–A.KARATHANASOPOLOUS–K.A. THEOFILATOS, *Artificial Intelligence in Financial Markets*, Palgrave Macmillan, 2016.

algoritmico coinvolge funzioni quali l'apprendimento, la progettazione dinamica, il ragionamento e i processi decisionali[25].

Si tratta, più precisamente, di una forma di "negoziazione di strumenti finanziari in cui un algoritmo informatizzato determina automaticamente i parametri individuali degli ordini (come, ad esempio, se avviare l'ordine), i tempi, il prezzo o la quantità dell'ordine o come gestire l'ordine dopo la sua presentazione, con intervento umano minimo o nullo"[26]. La negoziazione algoritmica 'classica'[27] si basa su sistemi di tipo deterministico (o *rule-based*) [28] e agisce tramite formule complesse, combinate con modelli matematici e supervisione umana, per

---

[25] Da non confondere con gli algoritmi 'di esecuzione', che sono usati solo per eseguire gli ordini, il *trading* algoritmico ha invece l'obiettivo di automatizzare determinate strategie e l'esecuzione automatica dell'ordine è solo una delle componenti dell'algoritmo. L'algoritmo di *trading* è programmato per prende la decisione di investimento quando si realizzano determinate condizioni.

[26] La definizione è quella contenuta nell'art. 4 par. 39 Direttiva 2014/65/UE del Parlamento europeo e del Consiglio del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la Direttiva 2002/92/CE e la Direttiva 2011/61/UE (c.d. MiFID II).

Nell'affrontare il fenomeno del *trading* algoritmico, MiFID II utilizza evidentemente un proprio vocabolario, che tiene conto della necessità di fornire un sistema completo di regolamentazione dei servizi di investimento. Particolarmente pregevole è lo sforzo di fornire una distinzione di base per il trading automatizzato, specificamente tra *trading* algoritmico e *hft*. Le due definizioni sono collegate, in modo che la seconda (*hft*) sia definita come un caso speciale della prima (*trading* algoritmico), delineata in termini più generali.

La nozione di citata è poi ulteriormente specificata all'articolo 18 del regolamento delegato (UE) 2017/5654 della Commissione, che stabilisce che "[...] un sistema è considerato privo di intervento umano o limitato se, per qualsiasi processo di generazione di ordini o quotazioni o qualsiasi processo di ottimizzazione dell'esecuzione degli ordini, un sistema automatizzato prende decisioni in una qualsiasi delle fasi di avvio, generazione, instradamento o esecuzione di ordini o quotazioni secondo parametri predeterminati" (Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive). ALVARO-VENTORUZZO, «High-Frequency Trading»: *note*, *op. cit.*, pp. 417-444 definiscono il *trading algoritmico* come "un insieme di hardware e software […] utilizzati da negoziatori professionali, per conto proprio o di terzi, in grado di osservare e reagire a informazioni di mercato in tempo reale, assumendo decisioni di negoziazione secondo algoritmi predefiniti – seppur in alcuni casi capaci di «evolvere» al cambiare delle condizioni – e inviando e/o gestendo ordini senza, o con minimo, intervento umano. Questi sistemi possono avere diverse finalità, ad esempio quella di minimizzare l'impatto di ordini significativi suddividendoli in numerosi piccoli ordini da piazzare su mercati diversi, e possono prevedere periodi di possesso degli strumenti finanziari anche prolungati".

[27] Utilizziamo questa espressione per riferirci al *trading* algoritmico non basato su sistemi di intelligenza artificiale.

[28] Rientra, ad esempio, nell'ambito del *trading* algoritmico il c.d. *systemic trading*, ossia qualsiasi strategia di *trading* che adotta un approccio sistematico all'attività di investimento, che basa la propria strategia sulla replica delle azioni precedentemente eseguite da *trader* non algoritmici.

prendere decisioni di acquisto o vendita di titoli finanziari in borsa[29]. Di conseguenza, è strettamente dipendente – e in parte anche limitato – dalla conoscenza e dalle supposizioni dei programmatori. Benché le operazioni di *trading* vengano compiute in modo automatizzato, le decisioni di *trading* sono prese dall'essere umano che impartisce le istruzioni all'algoritmo[30]. Proprio per questo, le strategie che un algoritmo di *trading* 'classico' è in grado di porre in essere sono predefinite e limitate.

Dunque, il *trading* algoritmico si caratterizza per automazione e velocità, nel senso che dal momento che le operazioni sui mercati vengono eseguite automaticamente, è possibile analizzare e rispondere alle condizioni di mercato in frazioni di secondo, molto più velocemente di quanto possa fare un *trader* umano.

Le caratteristiche sin qui elencate conferiscono maggiore efficienza alle operazioni (perché eseguite in modo molto più rapido e preciso) rispetto a quelle eseguite tramite *trading* 'manuale', capacità di gestione di grandi quantità di dati in tempo reale e la possibilità di eseguire *backtest*[31]. A ciò si aggiunge la capacità di inserire contemporaneamente ordini di acquisto e di vendita per catturare lo spread *bid-ask* (*market making*), sfruttare le inefficienze temporanee di prezzo tra diversi mercati o strumenti finanziari (arbitraggio statistico), analizzare i *trend* di mercato e compiere operazioni che sfruttino la direzione *trend* e infine analizzare le notizie finanziarie e fare *trading* basandosi sulle reazioni del mercato.

Per comprendere la portata innovativa degli strumenti di cui di discute, occorre considerare che, generalmente, nella fase esecuzione del *trade*, i *dealer* eseguono i propri ordini tramite un *order book* centralizzato che elenca gli ordini di acquisto e vendita per uno specifico titolo e li classifica in base al prezzo e al

---

[29] Cfr. A. DAVOLA, *Algoritmi decisionali e trasparenza bancaria. Il paradigma dell'inerenza nella regolamentazione delle tecnologie emergenti*, Milano, Utet, 2020, p. 70 parla di "algoritmi di tipo ingegneristico […] funzionali all'elaborazione di nuove strategie o modalità di investimento nei mercati finanziari".

[30] Cfr. P. LUCANTONI, *L'«high frequency trading» nel prisma della vigilanza algoritmica del mercato*, in Analisi Giuridica dell'Economia, Studi e discussioni sul diritto dell'impresa, 2019, fasc. 1, p. 300, "il *trader* (*rectius* l'essere umano che sta dietro la macchina) imposta una serie di regole che stabiliscono *a priori* le reazioni del *trader*-macchina alla ricezione di una determinata informazione. Grazie a queste regole, il programma di *trading* agisce inoltrano e/o ritirando ordini al ricorrere delle condizioni prefissate. […] L'attività decisionale umana funge da guida e indirizzo per i compiti e la serie di azioni che verranno poi svolti in concreto dal programma".

[31] Le strategie possono essere testate sui dati storici per verificarne l'efficacia prima di essere eseguite nel mercato reale.

momento di arrivo dell'ordine (generalmente su base *first-in-first-out*). Gli algoritmi di *trading* vengono progettati proprio in modo da essere in grado di sfruttare la presenza di *order book* centralizzati e la liquidità dei mercati, nonché comprendere quale sia il numero di ordini di acquisto e vendita a ciascun prezzo per un determinato titolo[32].

L'azione del *trader* algoritmico può coinvolgere cinque fasi: accesso/pulizia dei dati[33], analisi *pre-trade*[34]: creazione di segnali di *trading*, esecuzione del trade e gestione post-*trade*[35]: Di queste fasi, solo le prime due sono propriamente automatizzate, mentre quelle successive sono di regola supervisionate dagli esseri umani.

Dal punto di vista operativo, i sistemi di *trading* algoritmico richiedono quindi un'infrastruttura adeguata a gestire enormi quantità di dati in tempo reale[36] e l'accumulo di dati storici dettagliati sulla base dei quali eseguire l'analisi *pre-trade* e le fasi successive.

Lo spettro delle strategie poste in essere tramite algoritmi di *trading*, come si vedrà, è assai ampio e, pur non essendo nuove al contesto degli investimenti, dimostra come il ricorso a sistemi di negoziazione algoritmica non fa altro che agevolare, velocizzare, rendere più efficienti strategie ben realizzabili anche con tecnologie pre algoritmiche.

Il fenomeno del ricorso a sistemi di *trading* algoritmico è particolarmente rilevante: si pensi solo al fatto che nel 2019, l'80% degli scambi di obbligazioni in ambito europeo è avvenuto tramite sistemi algoritmici (diversi dall'*hft*)[37]. Nell'ultimo

---

[32] Cfr P. TRELEAVEN–M. GALAS–V. LALCHAND, *Algorithmic trading review*, in *Communication of the ACM, 2013, vol. 56*, issue 11, pp 76-85.

[33] Acquisizione e "pulizia" dei dati (finanziari, economici, ecc) che guidano l'algoritmo.

[34] Analisi delle proprietà degli *asset* per identificare opportunità di *trading* utilizzando dati di mercato o notizie finanziarie (*data analysis*).

[35] Analisi dei risultati dell'attività di *trading*, ad esempio della differenza tra il prezzo quando è stata presa la decisione di acquisto/vendita e il prezzo di esecuzione finale.

[36] Ad esempio i prezzi di apertura, massimi, minimi e chiusura di un titolo per ogni giorno di negoziazione o relativi a periodi di tempo più lunghi. Tali dati permettono di condurre analisi dettagliate e identificare pattern, tendenze e comportamenti nel mercato finanziario.

[37] ESMA, *Consultation Paper. Mifid II/MiFIR review report on Algorithmic Trading*, 2021 chiarisce che, fino alla metà del 2019, nel *trading* in obbligazioni non si registrava la presenza di strumenti algoritmici; nel terzo trimestre del 2019, invece, il *trading* algoritmico ha rappresentato circa l'80 per cento del volume. Per i derivati, il rapporto tra *trading* algoritmico e non algoritmico è rimasto stabile fino al secondo trimestre del 2019; dopo quel periodo, il *trading* algoritmico (non *hft*) ha iniziato ad aumentare. A partire dal 2018, il *trading* algoritmico ha conosciuto una crescita significativa nel mercato azionario europeo, con un incremento stimato tra il 50% e il 70%.

In ambito nazionale, invece, le operazioni riconducibili al *trading* ad alta frequenza (*hft*) sul Mercato Telematico Azionario (MTA) hanno rappresentato circa il 30% del totale degli scambi tra il 2016 e il 2019, registrando una flessione al 26% nell'ultimo anno di riferimento. Sul punto, CONSOB, *Relazione per l'anno 2019*, 31 marzo 2020.

Inoltre, CONSOB, *Relazione per l'anno 2018*, Roma, 2019, p. 65: "Nel corso del 2018, il 32 per cento circa dei controvalori scambiati sull'MTA è riconducibile a operatori registrati come *high frequency traders* (*hftrs*), prevalentemente operatori esteri, che utilizzano tecniche di *high frequency trading* in senso stretto (ossia basate su algoritmi e quindi appartenenti alla famiglia più ampia del *trading* algoritmico ma centrate sulla velocità di acquisizione ed elaborazione delle informazioni di mercato e di reazione a tali informazioni). Il dato tuttavia sale a oltre il 63 per cento se riferito a soggetti registrati ai sensi delle nuove definizioni previste dalla Direttiva 2014/65/UE (MiFID II) e dal Regolamento delegato (UE) n. 565/2017 e che nel corso dell'anno hanno trasmesso ordini mediante algoritmi. Il numero maggiore di operatori che effettuano *hft* si rileva principalmente sui mercati IDEM, MTA ed EtfPlus, mentre la loro presenza risulta meno significativa sul MOT e su EuroTLX".

Sul punto, V. CAIVANO–S. CICCARELLI–G. DI STEFANO–M. FRATINI– G. GASPARRI–M. GILIBERTI–N. LINCIANO–I. TAROLA, *Il* trading *ad alta frequenza*, *op. cit.*, p. 13 riportano una indagine ESMA, secondo cui, nei primi mesi del 2010, i paesi meno interessati dal *trading* ad alta velocità sembrano essere quelli nordici, con una quota di scambi attribuibili agli *hft*r pari al 13% per Nasdaq OMX a fronte del 40% registrato per le piattaforme Chi-X e Deutsche Boerse.

In merito, CONSOB, *Relazione per l'anno 2015*, Roma, 2016, p. 66: "L'utilizzo di tecnologia ad alta frequenza (hft) per l'esecuzione di negoziazioni ha di recente conosciuto uno sviluppo significativo anche sui mercati italiani, stimolando numerose riflessioni circa i possibili effetti sull'ordinato svolgimento degli scambi e sulla stabilità, liquidità e volatilità dei mercati.

Il monitoraggio del fenomeno si fonda anzitutto dalla rilevazione della sua effettiva diffusione. I dati relativi alle quote di mercato degli operatori classificati come *high frequency traders* (*hfts*), in termini di incidenza del controvalore scambiato sul totale, evidenziano una crescita non omogenea tra i diversi mercati organizzati e gestiti da Borsa Italiana.

L'attività di negoziazione automatizzata ad alta frequenza si è diffusa in maniera significativa sui mercati MTA, IDEM e ETFplus, mentre sul MOT la quota di mercato degli *hft*rs è rimasta sostanzialmente stabile. In particolare, le negoziazioni riconducibili a strategie HFT hanno sfiorato il 29 per cento circa del totale sul mercato azionario a pronti, il 44 per cento circa degli scambi di *futures* sull'indice Ftse Mib (il dato sale al 69 per cento considerando i *mini futures*, introdotti inizialmente per avvicinare la clientela retail a strumenti derivati standardizzati).

Infine, per quanto riguarda gli altri mercati, nel corso del 2015 va sottolineato che circa la metà degli scambi di *exchange traded products* (Etf) è avvenuta in contropartita a operatori *hftrs*, mentre l'incidenza è pari al 20 per cento circa sul mercato obbligazionario MOT".

Per quanto riguarda il passato, S. ALVARO–M. VENTORUZZO, «High-Frequency Trading*»: note*, *op. cit.,* p. 418 riportano i seguenti dati: "secondo uno studio del 2011, la quota di operazioni basate su queste tecniche nell'ambito della negoziazione sulle borse valori variava, a seconda dei mercati, tra il 19 e il 40% in Europa, e tra il 40 e il 70% negli USA. Inferiore, ma in crescita, la quota nei paesi asiatici, attestata secondo alcune stime intorno al 10%). Inferiore, ma in crescita, la quota nei paesi asiatici, attestata secondo alcune stime intorno al 10%".

Secondo altri studi, anch'essi riportati da S. ALVARO–M. VENTORUZZO, «High-Frequency Trading*»: note*, *op. cit.,* p. 418 nel 2012, negli Stati Uniti gli scambi di azioni effettuati mediante l'*hft* ha raggiunto il 51% del totale (nel 2009 era pari al 61%), il 48,5% sull'intero exchange traded volume ed oltre il 70% del numero delle transazioni in derivati. Mentre, in Unione Europea lo scambio di azioni tramite *hft* aveva raggiunto il 35% ed il 39% del valore degli scambi. Nello stesso periodo,

decennio il numero di partecipanti al mercato che operano tramite tecniche di negoziazione algoritmica è aumentato in modo sensibile[38]. Molti partecipanti al mercato si avvalgono ormai da tempo della negoziazione algoritmica, sia nei mercati azionari che nei mercati delle materie prime. Ciò ha portato – come già anticipato – a cambiamenti significativi nelle macrostrutture e nelle microstrutture del mercato: un mutamento che, come si vedrà, è stato supportato anche della legislazione dell'UE[39].

D'altronde, il diffuso uso del *trading* algoritmico non può stupire se si considerano i vantaggi che esso comporta: la solidità delle basi informatiche, la velocità di esecuzione e la diversificazione del rischio[40].

3. L'*high frequency trading*

Un sottoinsieme specifico della negoziazione algoritmica è costituito dalla negoziazione algoritmica ad alta frequenza[41].

Si tratta, in via di prima approssimazione, di sistemi che consentono di realizzare un numero elevato di negoziazioni in brevissimo tempo e che

---

"il peso dell'*hft* rispetto al totale degli scambi in azioni era pari al 28% in Giappone, al 20% in Australia, al 18% in Canada, al 12% in Asia e al 6% in Brasile. Sul mercato di Singapore la soglia era di circa il 30% del *derivatives trading* nel 2013. Nello stesso anno, Hong Kong registrava un 20% di scambi tramite *hft*, e in Australia si oscillava tra il 22 e il 27% giornaliero".

[38] S. ALVARO–M. VENTORUZZO, «High-Frequency Trading*»: note*, *op. cit.,* p. 420 segnalano che gli operatori si avvalgono di *hft* "direttamente (tramite infrastrutture e algoritmi di proprietà) o indirettamente (appoggiandosi a fornitori di servizi), la lista include soggetti diversi ed eterogenei. Accanto a investitori istituzionali come fondi pensione, fondi comuni e hedge funds, vi sono anche operatori specializzati, tra i quali spiccano ad esempio *Automated Trading Desk*, acquistata da Citigroup nel 2007; o società come KCG Holdings, un market maker basato a Chicago e risultante dalla fusione tra GETCO LLC e Knight Capital Group, un altro operatore *hft* che, dopo un errore di negoziazione costato oltre 450 milioni di dollari, è stato assorbito nel gruppo nel 2012. Altri nomi noti sono Chicago Trading, Citadel, Timber Hill, Tradebot e Virtu Financial".

[39] Adeguamento di cui si darà atto *infra*. In questo senso anche S. ALVARO–M. VENTORUZZO, «High-Frequency Trading*»: note*, *op. cit.*, p. 422 sostengono che lo sviluppo del *trading* algoritmico e del *hft* sia in buona parte frutto della decisione dei legislatori dei Paesi avanzati di favorire la creazione di diverse borse e sistemi di scambio fra loro, perché considerato un approccio più favorevole all'efficienza e l'equità del mercato rispetto al modello tradizionale dominato dall'obbligo di concentrazione degli scambi.

[40] Come notano Z. ZHANG–S. ZOHREN–S. ROBERTS, *Deep Reinforcement Learning for Trading*, in The Journal of Financial Data Science, 2020, vol. 2, issue 2, pp. 25-40 si tratta di vantaggi che dipendono dall'applicazione di modelli matematici e statistici.

[41] La negoziazione algoritmica è una delle strategie tipiche di *trading* algoritmico.

garantisce profitto sfruttando arbitraggi fra diversi mercati o la riduzione dell'intervallo temporale tra ordine ed esecuzione[42].

3.1. Definizioni

La definizione di questa attività è stata a lungo discussa. Nel corso degli ultimi anni la letteratura e le analisi empiriche hanno proposto e adottato molteplici definizioni, più o meno ampie[43].

È stata descritta come una "vasta gamma di strategie di negoziazione altamente competitive utilizzate dagli intermediari del mercato dei valori mobiliari che utilizzano un sistema automatizzato di negoziazione algoritmica e computer ultra-veloci per detenere titoli per una frazione di secondo e quindi operare per catturare lo *spread*"[44]. Oppure, più genericamente, come "la strategia utilizzata di *trader* professionisti che agiscono in proprio e che si impegnano in strategie che generano un gran numero di operazioni su base giornaliera. I *trader* possono essere organizzati in vari modi, come società di negoziazione per conto proprio, come *desk* di negoziazione per conto proprio di un *broker-dealer* multiservizi o come *hedge fund*"[45]. O ancora, come "negoziazioni per conto proprio, basate su algoritmi programmati a leggere informazioni rilevanti, ad esempio circa differenze di prezzo tra piazze di scambio, ed effettuare un elevatissimo numero di ordini e transazioni su strumenti liquidi con periodi di possesso brevissimi, nell'ordine di frazioni di secondo, senza detenere una posizione alla chiusura della giornata borsistica (c.d*. flat position*)"[46]. E, infine, "una tipologia di *trading* completamente automatizzato (della famiglia del *trading* algoritmico) in grado di

---

[42] Così G. RUTA, *I.A. nei reati economici e finanziari*, in Intelligenza artificiale e giurisdizione penale, Atti del Workshop della Fondazione Vittorio Occorsio, Università Mercatorum, Roma, 19 novembre 2021, pp. 58-75.

[43] V. CAIVANO–S. CICCARELLI–G. DI STEFANO–M. FRATINI– G. GASPARRI–M. GILIBERTI–N. LINCIANO–I. TAROLA, *Il* trading *ad alta frequenza*, *op. cit.*, pp. 9-10 nonché U.S. SECURITIES AND EXCHANGE COMMISSION, *Concept Release on Equity Market Structure*, in Exchange Act Release No. 34-61,358, 75 Fed. Reg. vol. 75, n. 13, p. 3607 "The lack of a clear definition of *hft*, however, complicates the Commission's broader review of market structure issues. The lack of clarity may, for example, contribute to the widely varying estimates of hft volume in today's equity markets. Although the term itself clearly implies a large volume of trades, some concerns that have been raised about particular strategies used by proprietary firms may not necessarily involve a large number of trades. Indeed, any particular proprietary firm may simultaneously be employing many different strategies, some of which generate a large number of trades and some that do not".

[44] IOSCO, *Principles for Dark Liquidity. Final Report 06/11,* 2011 (traduzione nostra).

[45] Così U.S. SECURITIES AND EXCHANGE COMMISSION, *Concept Release on Equity Market*, *op. cit.*, p. 3606 (traduzione nostra).

[46] S. ALVARO–M. VENTORUZZO, «High-Frequency Trading*»: note*, *op. cit.,* p. 421.

eseguire una moltitudine di calcoli in pochissimo tempo; dispone di un collegamento con il mercato estremamente rapido, analizza dati *tick-by-tick* avvalendosi di infrastrutture tecnologiche e informatiche in grado di eseguire operazioni in un arco temporale di pochi millisecondi. Un sistema ad alta frequenza è progettato in modo tale da eseguire le proprie strategie in maniera autonoma, analizzando il mercato e trasmettendo migliaia di messaggi di acquisto e vendita al secondo e inserendo contestualmente ordini di esecuzione, di cancellazione o di sostituzione che si adattano immediatamente al flusso informativo disponibile. L'obiettivo principale di un sistema ad alta frequenza è di identificare e trarre vantaggio da rapidi sbilanciamenti di liquidità o da inefficienze dei prezzi di brevissima durata; solitamente chiude la giornata di contrattazioni *flat"*[47].

Anche il legislatore europeo – nel Considerando 61 della Direttiva MiFID II[48] – definisce l'*high frequency trading* come sottoinsieme specifico della negoziazione algoritmica, capace di analizzare dati o segnali del mercato a velocità elevata per poi inviare o aggiornare un gran numero di ordini entro un tempo brevissimo in risposta all'analisi. La gestione degli ordini avviene in modo automatizzato, senza intervento umano, tanto che la creazione e la liquidazione delle posizioni avviene in tempi estremamente ridotti a fronte di elevato rapporto infragiornaliero di ordini/operazioni. Gli *high frequency trader* tipicamente chiudono "il giorno di negoziazione in una posizione *flat*, o prossima a essa"[49].

Ciò che emerge dalle diverse definizioni, è che questa tecnica di negoziazione algoritmica si caratterizza innanzitutto per il fatto che l'inizializzazione, la generazione, la trasmissione e l'esecuzione degli ordini di negoziazione vengono gestiti dalla macchina, senza intervento umano[50].

Altra caratteristica fondamentale è la velocità con cui operano. Infatti, le infrastrutture su cui si basa l'*high frequency trading* riducono al minimo le latenze

---

[47] Cfr. F.J. FABOZZI–S.M. FOCARDI–C. JONA, *High Frequency Trading: Methodologies and Market Impact, Review of future markets*, vol. 19, 2010, pp. 7-38, definizione citata anche da A. PUORRO, *High frequency trading*, *op. cit.*, p. 9.

[48] Direttiva 2014/65/UE del Parlamento europeo e del Consiglio del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la Direttiva 2002/92/CE e la Direttiva 2011/61/UE.

[49] Così il Considerando 61 della Direttiva 2014/65/UE.

[50] Art. 40 par 1 (40) MiFID II. P. LUCANTONI, *L'«high frequency trading»*, *op. cit.*, p. 298 sottolinea come la negoziazione algoritmica ad alta frequenza abbia in comune con il *trading* algoritmico la 'programmabilità', ossia l'agire in maniera molto rapida agli stimoli individuati dal relativo programmatore.

di rete[51] e le informazioni sono veicolate ad una velocità altissima grazie a servizi di c.d. *co-location, proximity*[52] e *feed* di dati diretti offerti dalle borse e da altri soggetti[53].

Hardware e *software* su cui l'*hft* si basa garantiscono una capacità di calcolo estremamente sofisticata, capace di leggere informazioni rilevanti (ad esempio differenze di prezzo fra piazze di scambio) e effettuare un elevatissimo numero di ordini e transazioni a velocità quasi incommensurabili[54]. L'*high frequency trader*, infatti, è in grado di immettere migliaia di ordini al secondo[55].

Per questa ragione è in grado di far seguire all'immissione di ordini numerose cancellazioni o modifiche, al fine di adeguare la strategia alle nuove condizioni di mercato, che vengono elaborate dagli algoritmi in tempo reale sulla base delle

---

[51] Art. 4 par. 1 (40) Direttiva 2014/65/UE (MiFID II). Sul punto anche U.S. SECURITIES AND EXCHANGE COMMISSION, *Concept Release on Equity Market*, *op. cit.*, p. 3606 "characteristics often attributed to proprietary firms engaged in hft are: the use of extraordinarily highspeed and sophisticated computer programs for generating, routing, and executing orders [...]"

[52] Cfr. le definizioni di V. CAIVANO–S. CICCARELLI–G. DI STEFANO–M. FRATINI– G. GASPARRI–M. GILIBERTI–N. LINCIANO–I. TAROLA, *Il* trading *ad alta frequenza*, *op. cit.*, p. 10; nonché F. CONSULICH, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca borsa e titoli di credito*, 2018, fasc. 2, p. 199: gli hardware sono "scientemente posti in prossimità del server dei mercati finanziari presso i quali tali programmi algoritmici operano, sicché lo spazio che l'impulso elettrico deve percorrere per giungere a destinazione è ridottissimo (colocation)".

[53] S. ALVARO–M. VENTORUZZO, «High-Frequency Trading»*: note*, *op. cit.,* p. 421, nt. 14 riportano un significativo passaggio del libro best seller di M. Lewis, Flash Boys: A Wall Street Revolt, New York-London, Norton, 2014, secondo cui "alcuni anni fa la società Spread Networks ha investito trecento milioni di dollari per installare un cavo di fibra ottica il quanto più diritto possibile tra la borsa mercantile di Chicago e il data center del Nasdaq in New Jersey, al fine di ottenere un vantaggio temporale nella trasmissione delle informazioni di circa due millisecondi, arrivando intorno ai 13. I concorrenti, come Tradeworx e McKay, stanno tuttavia passando a sistemi di trasmissione aerea, in quanto il minor indice di rifrazione dell'aria rispetto al vetro consentirebbe di avvicinarsi ulteriormente al compiere il percorso alla velocità della luce, ossia circa 9 millisecondi rispetto ai 7.5 che impiega la luce".

[54] V. CAIVANO–S. CICCARELLI–G. DI STEFANO–M. FRATINI–G. GASPARRI–M. GILIBERTI–N. LINCIANO–I. TAROLA, *Il* trading *ad alta frequenza*, *op. cit.*, p. 8. Come notano, S. ALVARO–M. VENTORUZZO, «High-Frequency Trading»*: note*, *op. cit.,* p. 422 si tratta di un elemento di fondamentale importanza perché "il prezzo di talune azioni può cambiare oltre 10.000 volte in un minuto secondo: per intendersi, nel tempo che il lettore impiega per scorrere le parole da qui al prossimo punto, un *high frequency trader* compie migliaia di operazioni". Nonché, U.S. SECURITIES AND EXCHANGE COMMISSION, *Concept Release on Equity Market*, *op. cit.*, p. 3606 "Structure characteristics often attributed to proprietary firms engaged in hft are: è [...] the submission of numerous orders that are cancelled shortly after submission".

[55] FINANCIAL INDUSTRY REGULATORY AUTHORITY, *Getting Up to Speed on High-Frequency Trading*, 25 novembre 2015, https://www.finra.org/investors/insights/getting-speed-high-frequency-trading. Nonché V. CAIVANO–S. CICCARELLI–G. DI STEFANO–M. FRATINI– G. GASPARRI–M. GILIBERTI–N. LINCIANO–I. TAROLA, *Il* trading *ad alta frequenza*, *op. cit.*, p. 8.

informazioni derivanti dagli ordini presenti sul *book*, con ridotti *order-to-trade ratio*[56]. Il tempo che intercorre tra la decisione di compiere un'operazione finanziaria e la sua compiuta esecuzione sul mercato è minimo[57].

Di conseguenza, i sistemi di negoziazione algoritmica ad alta frequenza sono soliti assumere posizioni "lunghe" o "corte" su un titolo per periodi normalmente non superiori a una seduta di borsa[58], fattore che determina un rapido *turnover* dei titoli all'interno del portafoglio[59].

Gli *high frequency trader* effettuano *trading* prevalentemente in conto proprio e mostrano una generale, sebbene non esclusiva, preferenza per gli strumenti finanziari più liquidi. L'operatività di un *high frequency trader* richiede infatti la possibilità di uscire da una determinata posizione con un'elevata velocità. "Gli strumenti più liquidi sono quelli dai quali è possibile disinvestire rapidamente poiché hanno un mercato in grado di assorbire e soddisfare ordini per importi significativi. Tali strumenti, inoltre, sono quelli per i quali risultano particolarmente efficaci le tecniche statistiche sottostanti agli algoritmi utilizzati dagli *high frequency trader*"[60].

Tutte queste caratteristiche agevolano una pluralità eterogena di strategie[61], accomunate dalla necessità di operare più velocemente degli altri operatori, dalla capacità di influenzare gli andamenti di mercato e dalla tendenza ad avere portafogli non esposti al 'rischio mercato'.

---

[56] L'*order-to-trade ratio* (OTR) descrive il rapporto tra l'immissione, la modifica e la cancellazione di ordini/quote e le operazioni eseguite.

[57] F. CONSULICH, *Il nastro di Möbius*, *op.cit.*, p. 199 "i *trader*s algoritmici sono in grado di aggredire finestre di investimento che durano poche frazioni di secondo, poiché riducono al minimo possibile i cd. periodi di latenza, ovvero il lasso temporale che intercorre tra la decisione di compiere un'operazione finanziaria e la sua compiuta esecuzione sul mercato. La capacità, propria degli *hft*, di annullare quasi del tutto il periodo necessario a tradurre un'idea economica in un dato di realtà è denominata cd. bassa latenza (cd. low latency)".

[58] Le posizioni sono generalmente chiuse a fine giornata. Nel corso di una sessione, il periodo medio di detenzione degli strumenti varia da alcuni secondi a diversi minuti. Cfr. SEC *op cit.,* 2010, "Structure characteristics often attributed to proprietary firms engaged in hft are: [...] ending the trading day in as close to a flat position as possible (that is, not carrying significant, unhedged positions overnight).

[59] U.S. SECURITIES AND EXCHANGE COMMISSION, *Concept Release on Equity Market*, *op. cit.*, p. 3606 "Structure characteristics often attributed to proprietary firms engaged in hft are: [...] very short time-frames for establishing and liquidating positions".

[60] V. CAIVANO–S. CICCARELLI–G. DI STEFANO–M. FRATINI– G. GASPARRI–M. GILIBERTI–N. LINCIANO–I. TAROLA, *Il* trading *ad alta frequenza*, *op. cit.*, p. 8.

[61] Tutte le strategie sono caratterizzate dalla forte reattività agli stimoli del mercato.

3.2 Le strategie di high frequency trading

Le strategie adottate dagli *high frequency trader* più di frequente non sono di per sé abusive e possono essere descritte – seppur sinteticamente – come segue. Come si vedrà, alcune di queste possono, a determinate condizioni che si chiariranno, assumere rilevanza penale.

3.2.1. Il market making

In primo luogo, il *market making*, che consiste nel fornire liquidità agli strumenti negoziati sulle varie piattaforme, attraverso la disponibilità continua a negoziare tali strumenti, pubblicando continuamente prezzi di acquisto (*bid*) e vendita (*ask*) per uno strumento finanziario. Il guadagno deriva dalla differenza tra il prezzo di acquisto e il prezzo di vendita (*bid-ask spread*)[62]. Gli *high frequency trader* che agiscono da *market maker* utilizzano gli algoritmi per calcolare prezzi *bid* e *ask* tali da conseguire profitti sulla base di arbitraggi tra i *bid-ask spread* che si formano sulle diverse sedi di negoziazione.

3.2.2. Il tick trading

In secondo luogo, il *tick trading,* un insieme di tecniche utilizzate per identificare un importante ordine immesso sul mercato e che è stato suddiviso in piccoli ordini in modo da evitare tensioni sul prezzo[63]. L'algoritmo è in grado di

---

[62] Il *market maker* svolge un ruolo fondamentale nel mercato: si tratta infatti di intermediari che offrono liquidità agli altri partecipanti al mercato, esponendo in modo continuativo proposte di acquisto (*bid*) o vendita (*ask*) su un dato strumento finanziario e aumentando il proprio guadagno all'aumentare nel numero delle transazioni effettuate. Cfr. la definizione di V. CAIVANO–S. CICCARELLI–G. DI STEFANO–M. FRATINI– G. GASPARRI–M. GILIBERTI–N. LINCIANO–I. TAROLA, *Il* trading *ad alta frequenza*, *op. cit.*, p. 9.
Per chiarire: il *market maker* pubblica un prezzo di acquisto (*bid*) e un prezzo di vendita (*ask*) per uno strumento finanziario (ad esempio un *bid* di 100 euro e un *ask* di 102 euro per una stessa azione). Se un investitore vuole vendere l'azione, il *market maker* la comprerà al prezzo *bid* di 100 euro. Se un investitore vuole comprare l'azione, il *market maker* la venderà al prezzo *ask* di 102 euro. La differenza tra il prezzo di vendita e il prezzo di acquisto (*bid-ask spread*), in questo caso 2 euro, rappresenta il guadagno del *market maker*. Questo *spread* 'compensa' il *market maker* per il rischio assunto e per aver fornito liquidità.

[63] Si prenda ad esempio l'azione XYZ, il cui prezzo corrente è 50,00 euro e il tick 0,01 euro (e le commissioni per operazioni: 0,005 euro per azione). Il *tick trader* segue costantemente il flusso degli ordini e il libro degli ordini per l'azione XYZ e nota che il prezzo dell'azione XYZ si sta muovendo tra 50,00 e 50,01 euro in un breve intervallo di tempo. Piazza quindi un ordine di acquisto a 50,00 euro per 1000 azioni. Quando l'ordine di acquisto viene eseguito, il *trader* piazza immediatamente un ordine di vendita a 50,01 euro per le stesse 1000 azioni. L'ordine di vendita

individuare tutti i singoli ordini e prevedere incrementi o decrementi del prezzo complessivo, man mano che le frazioni di ordini arrivano sul mercato e anticipare altri operatori[64].

3.2.3. L'arbitraggio

In terzo luogo, l'arbitraggio, ossia l'acquisto o la vendita di un bene o un'attività finanziaria e l'esecuzione contemporanea di una operazione di segno opposto sullo stesso strumento, negoziato su un mercato diverso dal precedente[65] oppure su titoli con identico *payout*[66]. La logica alla base dell'arbitraggio è quella di sfruttare le differenze di prezzo al fine di ottenere un profitto. L'operazione è ovviamente possibile se il guadagno che si ottiene supera

---

viene eseguito quando il prezzo raggiunge 50,01 euro. Se si tiene conto che il prezzo di acquisto era pari a 50,00 euro, mentre il prezzo di vendita a 50,01 euro, il profitto lordo per azione è quindi: 50,01 - 50,00 = 0,01 euro; mentre il profitto lordo totale: 0,01 euro x 1000 azioni = 10,00 euro. A queste si aggiungono 10 euro di commissioni totali (0,005 euro x 1000 azioni x 2 (acquisto e vendita). Il profitto netto è invece pari a 0,00 euro (profitto lordo - commissioni = 10,00 euro - 10,00 euro). Il profitto netto è zero a causa delle commissioni. Tuttavia, se il *trader* riuscisse a ridurre le commissioni o aumentare leggermente il margine tra il prezzo di acquisto e vendita (ad esempio, comprando a 50,00 euro e vendendo a 50,02 euro), il profitto netto aumenterebbe.

[64] P. LUCANTONI, *L'«high frequency trading»*, *op. cit.*, p. 298 "per impedire che la negoziazione ad alta frequenza rappresenti un vantaggio competitivo sul mercato è stato introdotto l'obbligo, per le sedi di negoziazione di indicare: i) i tick di negoziazione, intesi come incrementi minimi cui può essere soggetto il prezzo degli strumenti negoziati (art 65 sexies c. 5 lett. d tuf) e ii) l'order to trade ratio, ovvero il limite al rapporto massimo tra odrini non eseguiti e operazioni (art. 65 sexies c. 5 lett. f tuf)".

[65] Un esempio: Alfa è quotata sia alla Borsa di Toronto (TSX) che alla Borsa di New York (NYSE). Le azioni di Alfa sono quotate 63,50 dollari CAD sul TSX e 47,00 dollari USD sul NYSE. Si supponga che il tasso di cambio USD/CAD sia di 1,37 dollari, il che significa che un dollaro USA equivale a 1,37 dollari CAD. Se si usasse il tasso di cambio menzionato, l'azione da 47 dollari USA dovrebbe corrispondere a 64,39 dollari CAD sul TSX. Ma non è così: il prezzo attuale della borsa di Toronto è inferiore. In queste circostanze, un *trader* può acquistare azioni Alfa sul TSX a 63,50 dollari CAD e contemporaneamente vendere lo stesso titolo sul NYSE a 47,00 dollari USD. Tenendo conto del tasso di cambio, il valore equivalente di ciascuna azione dovrebbe essere di 64,39 dollari CAD. In definitiva, il *trader* ha ottenuto un profitto di 0,89 dollari per azione (64,39 dollari - 63,50 dollari) per questa transazione.

[66] Un esempio di *payout* identico che crea occasione di arbitraggio. Si considerino due obbligazioni diverse, emesse da due aziende diverse, con caratteristiche diverse, che promettono di pagare esattamente la stessa somma di denaro alla stessa data nel futuro (100 euro fra un anno). Sebbene le obbligazioni siano emesse da aziende diverse, dopo un anno pagano entrambe 100 euro: hanno lo stesso *payout*. L'opportunità di arbitraggio si crea se, al momento dell'acquisto, le due obbligazioni hanno prezzi diversi (ad esempio, l'obbligazione A costa 95 euro e l'obbligazione B 93 euro. Si può cioè sfruttare tale differenza di prezzo comprando l'obbligazione B a 93 euro e vendere (o vendere allo scoperto) l'obbligazione A a 95 euro. Alla fine del periodo, quando entrambe pagheranno 100 euro, il profitto deriva dalla differenza di prezzo al momento dell'acquisto, cioè 2 euro per ogni coppia di obbligazioni scambiate.

i costi per il trasferimento del bene da un mercato all'altro. L'opportunità di effettuare operazioni di arbitraggio si presenta ogni volta che una stessa attività è contrattata su due mercati diversi a prezzi diversi o, nel caso in cui due attività siano perfettamente sostituibili tra loro, con identico *payout*. Questa operazione è agevolata dalla capacità degli algoritmi di reagire in millisecondi a differenze di prezzo anche minuscole tra strumenti e indici finanziari, valute o *commodities* negoziati su piazze diverse.

3.2.4. La liquidity detection

In quarto luogo, la *liquidity detection*, strategia basata sull'osservazione dell'operatività di altri partecipanti al mercato in modo da inferirne le strategie sottostanti e agire di conseguenza[67]. La strategia di *liquidity detection* effettuata tramite algoritmi di *trading* consente di sondare il mercato con piccoli ordini per capire quanta liquidità è disponibile senza far salire il prezzo del titolo.

3.2.5. Lo smoking *e lo* spoofing

La quinta strategia rilevante è lo *smoking*, tecnica di *trading* che cerca di 'testare' la profondità del mercato e scoprire la presenza di ordini di grandi dimensioni, che hanno la capacità di far muovere il mercato. Questa strategia sfrutta piccole variazioni di prezzo per ottenere profitti rapidi, immettendo molti ordini allettanti ('ordini civetta') con l'obiettivo di attrarre il maggior numero di *slow trader* per poi modificare questi ordini molto velocemente tramite l'inserimento di

---

[67] Si pensi ad un fondo di investimento che ha intenzione di acquistare 100.000 azioni di Alfa, senza far aumentare eccessivamente il prezzo. L'algoritmo di *trading* rileva la liquidità disponibile nel mercato, per eseguire l'acquisto in modo efficiente.
Innanzitutto esegue piccoli ordini di prova per sondare la profondità del mercato senza rivelare l'intera intenzione di acquisto.
In un secondo momento, l'algoritmo inizia a piazzare piccoli ordini di acquisto, ad esempio 100 azioni per volta, a intervalli regolari e a diversi livelli di prezzo. Monitora attentamente la reazione del mercato a questi ordini: se l'ordine viene eseguito immediatamente senza muovere il prezzo, l'algoritmo deduce che c'è una buona disponibilità di azioni a quel livello di prezzo. Se l'ordine impiega più tempo a essere eseguito o se il prezzo inizia a salire, l'algoritmo deduce che la liquidità è minore a quel livello di prezzo.
Successivamente, l'algoritmo raccoglie i dati dagli ordini di prova per creare un profilo della liquidità del mercato. Ad esempio, può determinare che ci sono molte azioni disponibili a 63,50 dollari, ma poche a 63,40 dollari.
Utilizzando le informazioni raccolte, l'algoritmo decide come piazzare i grandi ordini in modo da minimizzare l'impatto sul mercato, ad esempio distinguendo gli ordini nel tempo e a vari livelli di prezzo per evitare di muovere troppo il mercato (potrebbe comprare 10.000 azioni a 63,50 dollari, aspettare del tempo e comprare altre 10.000 azioni a 63,55 dollari, e così via).

condizioni meno favorevoli, prima che le controparti possano accorgersi della modifica[68].

Un principio per certi versi simile sta alla base dello *spoofing*, che sfrutta l'immissione di una serie di ordini di vendita 'fasulli' aventi il solo scopo di simulare una fase di ribasso del mercato, i quali tuttavia vengono cancellati prima di essere eseguiti[69].

Gli esempi citati rendono evidente come la maggiore efficacia delle strategie dipenda dalla maggiore velocità di questo tipo di *trader*, rispetto a quella dei partecipanti al mercato che non si servono degli algoritmi ad alta frequenza (i c.d. *slow trader*).

Infatti, sebbene spesso i margini di profitto per la singola transazione singola transazione siano esigui, è proprio grazie agli elevati volumi di negoziazioni

---

[68] Il *trader hft* invia un gran numero di piccoli ordini di acquisto o vendita su vari strumenti finanziari. Questi ordini sono spesso inseriti e cancellati rapidamente. Successivamente, si osserva come il mercato reagisce a questi ordini. Se un piccolo ordine provoca una grande reazione (ad esempio, un rapido aumento o diminuzione del prezzo), il *trader* potrebbe dedurre che ci sono grandi ordini nascosti (non visibili) in attesa di essere eseguiti. Una volta identificata la presenza di ordini di grandi dimensioni, il *trader* può decidere di sfruttare questa informazione (*i.e.* piazzare ordini più grandi per approfittare del supposto movimento del prezzo).

Un esempio pratico: il *trader hft* invia un ordine di acquisto di 100 azioni di una società a 10,00 euro per azione. Subito dopo, inserisce un altro ordine di vendita di 100 azioni a 10,05 euro per azione. Se il primo ordine di acquisto viene eseguito immediatamente e il prezzo inizia a salire, il *trader* potrebbe intuire che ci sono grandi ordini di acquisto in attesa. Analogamente, se l'ordine di vendita viene eseguito subito e il prezzo inizia a scendere, potrebbe dedurre che ci sono grandi ordini di vendita.

Nel primo caso (grandi ordini di acquisto), potrebbe decidere di acquistare un numero maggiore di azioni prima che il prezzo salga ulteriormente. Viceversa, se ci sono grandi ordini di vendita, potrebbe vendere rapidamente le azioni che possiede prima che il prezzo scenda.

[69] In buona sostanza, il *trader* piazza grandi ordini di acquisto o vendita che non ha intenzione di eseguire. Questi ordini sono visibili nel book degli ordini e creano l'apparenza di una forte domanda o offerta. Il mercato, di fronte a questi grandi volumi è indotto a pensare che il prezzo del titolo stia per salire (se ci sono grandi ordini di acquisto) o scendere (se ci sono grandi ordini di vendita) e dunque a piazzare ordini veri seguendo la tendenza solo apparente. Mentre gli altri partecipanti reagiscono agli ordini falsi, il *trader hft* inserisce ed esegue ordini veri dall'altro lato del mercato (ad esempio, se ha piazzato ordini falsi di acquisto, potrebbe vendere il titolo a un prezzo più alto). Poco prima che gli ordini falsi vengano eseguiti, il *trader* li cancella. In questo modo, evita di acquistare o vendere realmente grandi quantità di titoli.

Un esempio pratico: si immagini che un *trader* voglia vendere azioni di una società. Piazza un grande ordine di acquisto di 10.000 azioni a 10,00 euro per azione. Questo crea l'apparenza di una forte domanda, che induce il mercato a immaginare che il prezzo dell'azione stia crescendo e, dunque, fa sì che gli altri *trader* immettano ordini di acquisto, facendo salire effettivamente il prezzo. Mentre il prezzo sale, il *trader hft* vende le sue azioni a un prezzo più alto, ad esempio a 10,05 euro per azione. Prima che l'ordine di acquisto di 10.000 azioni venga eseguito, il *trader* lo cancella, traendo profitto.

operate in un'unità di tempo che la strategia è foriera di profitto: numerosi scambi e transazioni del valore di milioni di dollari avvengono a velocità misurabili in millisecondi.

Oggi, i numeri del *trading* ad alta frequenza, per volumi di scambi e valore in dollari, si aggirano sulle centinaia di miliardi al giorno[70]. Il fenomeno è in continua espansione.

Negli ultimi anni, si stima che il *trading* ad alta frequenza abbia rappresentato, nel 2018 la quota di scambi azionari effettuata tramite operatori algoritmici in Europa ha subito un incremento del 50-70%, a fronte dell'incremento annuo del 20% registrato nel 2011. A seconda delle rilevazioni, e soprattutto al variare del periodo storico e del mercato considerato, le percentuali mutano, ma tutte le analisi sono concordi nell'evidenziare la poderosa colonizzazione degli scambi da parte degli operatori algoritmici[71].

3.3. L'impatto *dell'high frequency trading* sui mercati: i benefici

Considerata l'importanza del fenomeno, l'impatto dell'uso di algoritmi nell'esecuzione delle operazioni sugli strumenti finanziari è da tempo uno degli argomenti più discussi nel settore finanziario.

Come indicato nel Considerando 62 della Direttiva MiFID II, "il progresso tecnico ha reso possibile la negoziazione ad alta frequenza e l'evoluzione dei modelli commerciali. L'utilizzo della tecnologia di negoziazione ha aumentato la velocità, la capacità e la complessità delle modalità di negoziazione degli investitori. Esso ha inoltre consentito ai partecipanti ai mercati di facilitare l'accesso elettronico diretto ai mercati per i loro clienti mediante l'utilizzo dei loro sistemi di negoziazione, l'accesso diretto ai mercati o l'accesso sponsorizzato.

In generale, la tecnologia di negoziazione ha apportato vantaggi al mercato e ai partecipanti al mercato, come una più ampia partecipazione ai mercati, un aumento di liquidità, differenziali più ridotti, minore volatilità a breve termine e i mezzi per ottenere una migliore esecuzione degli ordini per i clienti".

Secondo la dottrina, il mercato ha beneficiato dell'avvento del *trading* ad alta frequenza sotto numerosi profili.

Un primo aspetto riguarda il ruolo degli *high frequency trader* come *market maker*: poiché essi guadagnano solo se scambiano continuamente volumi massicci, gli *hft* di fatto forniscono liquidità ai mercati e offrono quindi la certezza

---

[70] T.C.W. LIN, *The New Market Manipulation*, op*. cit.*, 2017, p. 1273.

[71] F. CONSULICH, *Il nastro di Möbius*, *op. cit.*, p. 197.

di trovare tanti ordini quanti sono gli investitori disposti a negoziare, anche per i prodotti meno scambiati e per le sedi di negoziazione alternative[72]. Tanto è vero che, secondo i primi studi sull'impatto del *trading* ad alta frequenza sui mercati, gli *hft* sembrano aumentare l'efficienza dei mercati e a diminuire la volatilità[73].
È stato poi sottolineato come l'avvento del *trading ad alta frequenza* abbia avuto un impatto positivo sulla velocità di esecuzione degli ordini, che è aumentata, permettendo una migliore è più rapida esecuzione degli ordini.
Un altro beneficio della concorrenza esercitata dalle imprese di *hft* è la riduzione dei costi di transazione per tutti i partecipanti al mercato.
Nel complesso, quindi, si può affermare che, secondo la prevalente dottrina, l'impatto del *trading* algoritmico ad alta frequenza sia positivo[74].

3.4. L'impatto *dell'high frequency trading* sui mercati: i rischi

Ciò non toglie che rimangano tuttora alcune perplessità soprattutto sul legame fra *trading* algoritmico – in generale, ma specialmente quello ad alta frequenza – e perturbazioni del mercato, sia volontarie che derivanti da malfunzionamenti dei sistemi[75].

---

[72] Sul punto, si vedano D. LEIS, *High Frequency Trading*, *op. cit*. p. 4.; Come sottolineano G. STRAMPELLI–G. BALP, *Preserving Capital Markets Efficiency in the High-Frequency Trading Era*, in Bocconi Legal Studies Research Paper, 2018, p. 6 non è mancato però chi ha notato che poiché gli *hft* forniscono liquidità come prodotto del loro tentativo di ottenere profitti dall'attività di *trading*, rimane da capire se essi forniscono liquidità preziosa o - come ha osservato la SEC - liquidità fantasma che scompare quando è più necessaria per gli investitori a lungo termine e gli altri partecipanti al mercato. Gli autori sposano la tesi della dottrina che ritiene più accurata la descrizione del ruolo di fornitori di liquidità degli operatori ad alta frequenza secondo cui essi servono come intermediari infragiornalieri e trasmettono rapidamente gli squilibri dagli investitori istituzionali agli altri partecipanti al mercato. Secondo gli Autori, considerando che la maggior parte delle contrattazioni (in particolare, i grandi ordini di investitori istituzionali passivi) avviene poco prima della chiusura delle borse, l'effetto benefico della liquidità infragiornaliera da parte dell'*hft* potrebbe probabilmente non incidere sugli investitori istituzionali quanto la fornitura di liquidità intergiornaliera.

[73] J. A. BROGAARD, *High Frequency Trading and its Impact on Market Quality*. in Northwestern University Kellogg School of Management Working Paper n. 66, pp. 1-75. Nello stesso senso: G. STRAMPELLI–G. BALP, *Preserving capital markets*, *op. cit.*, p. 8.

[74] Sul punto si rinvia all'approfondimento di O. COSME JR., *Regulating High-Frequency Trading: The Case for Individual Criminal Liability*, The Journal of Criminal Law and Criminology, 2019, vol. 109, issue 2, pp. 365-394 nonché S. ALVARO–M. VENTORUZZO, «High-Frequency Trading*»: note*, *op. cit.,* pp. 420 ss. e A. DAVOLA, *Algoritmi decisionali,* 2020, *op. cit.*, pp. 18-22.

[75] Qui il riferimento è agli episodi di *flash crash*, occorsi – ad esempio – nel 2022 e nel 2010.

Sempre maggiore attenzione è stata riservata - anche dalle autorità di vigilanza - alle ripercussioni derivanti dall'incremento della velocità operativa dei partecipanti al mercato (in termini di immissione, modifica e cancellazione degli ordini). In particolare, ci si è concentrati sul rischio sistemico connesso ad eventi *shock*, sulla qualità del mercato (in termini di efficienza informativa dei prezzi, volatilità e liquidità) e, più in generale, sull'integrità del mercato[76].

Come si vedrà, lo stesso legislatore europeo ha sottolineato il rischio di "sovraccarico dei sistemi nelle sedi di negoziazione a causa del gran numero di ordini, i rischi che la negoziazione algoritmica generi ordini erronei o doppi o che comunque non funzioni correttamente e crei così un mercato disordinato e il

---

Il primo, più recente, avvenuto il 3 maggio 2022, ha interessato le principali borse europee. Sul punto, B. ELDER, *That Citi flash crash revisited*, in Financial Times, 3 maggio 2022, https://www.ft.com/content/3089d32b-1535-4f13-9411-c31b12486e4d.

Il secondo, invece, risale al 6 maggio 2010, durante il quale il mercato azionario americano ha vissuto una sessione di *trading* caratterizzata da una volatilità senza precedenti. La giornata si aprì alle 9.30 in un contesto di forte instabilità e di tendenza al ribasso, dovuta tra l'altro alle notizie sui disordini sociali in Grecia (dovute alle azioni di governo e Unione Europea sul debito del Paese). Per le prime ore i mercati si sono mossi come nella maggior parte delle sessioni di *trading* ordinarie. Improvvisamente alle 14.40 il Dow Jones scese del circa 10% in meno di cinque minuti, causando forti perdite anche negli altri indici e determinando una volatilità protrattasi per venti minuti. Nell'arco di meno di trenta minuti di estrema volatilità, circa 1.000 miliardi di dollari di valore di mercato "scomparvero" dal mercato azionario statunitensi, centinaia di titoli vennero scambiati a prezzi assurdi, che andavano da un centesimo per azione a 100.000 dollari per azione. Dopo il precipitoso declino, il mercato ha recuperato a recuperare gran parte delle perdite. Il tutto nel giro di meno di un'ora. I risultati di un'indagine della SEC e della CFTC chiarirono l'accaduto nei termini sintetizzati da S. ALVARO–M. VENTORUZZO, «High-Frequency Trading*»: note*, *op. cit.,* p. 428 "un operatore – verosimilmente un fondo comune che utilizzava *hft* ma, si noti, non un operatore «puro» *hft* – aveva immesso un importante ordine di vendita su *futures* sull'indice S&P 500; l'algoritmo che governava la transazione, tuttavia, non considerava il prezzo, ma solo il volume: in altre parole, non era programmato per fermarsi in caso di repentino declino del corso dello strumento. Gli algoritmi di altri operatori *hft* amplificarono l'effetto dell'ordine e i prezzi di mercato iniziarono a crollare. Caduti i prezzi, molti sistemi automatici bloccarono l'attività, essendo programmati per interromperla a fronte di un siffatto ribasso. Gli operatori «umani» che osservarono il fenomeno esitarono a fronte del crollo: i *market makers* ampliarono lo spread tra prezzo di acquisto e vendita per compensare il rischio, e molti *traders* non ebbero immediatamente il coraggio di tornare ad acquistare, temendo eventi catastrofici dei quali non erano a conoscenza. La crisi di liquidità che ne seguì fece il resto. Anche i *circuit breakers* contribuirono agli eventi: paradossalmente, i sistemi del NYSE disegnati per sospendere le quotazioni a fronte di eccessi di ribasso, in un sistema basato sull'interconnessione delle borse, ebbero l'effetto di dirottare ancora più ordini di vendita dal NYSE ad altri sistemi di scambio con diversi algoritmi, aumentando così la pressione dell'offerta su queste piazze". Sul punto: D. LEIS, *High Frequency Trading*, *op cit.* pp. 60-66; A. PUORRO*, High frequency trading*, *op. cit.*; T.C.W. LIN, *The New Market Manipulation*, op*. cit.*, 2017, pp. 1287-1293.

[76] V. CAIVANO–S. CICCARELLI–G. DI STEFANO–M. FRATINI–G. GASPARRI–M. GILIBERTI–N. LINCIANO–I. TAROLA, *Il* trading *ad alta frequenza*, *op. cit.*, pp. 17-24.

rischio che i sistemi di negoziazione algoritmica reagiscano in modo eccessivo ad altri eventi di mercato, esacerbando così la volatilità qualora preesista un problema di mercato"[77]. Per questa ragione nella Direttiva MiFID II si è esplicitata la necessità di sottoporre le tecniche di negoziazione algoritmica ad alta frequenza "a uno speciale controllo regolamentare"[78].

Ai rischi legati ai malfunzionamenti dei sistemi, si aggiunge poi il rischio che le capacità computazionali degli algoritmi di *hft* siano sfruttate per porre in essere strategie riconducibili alle fattispecie penali di abuso di mercato, come si dirà in seguito.

In definitiva, la pervasiva diffusione di sistemi algoritmici in ambito finanziario rischia di svelare nuove – o esacerbare esistenti – forme di vulnerabilità dei mercati.

4. Intelligenza artificiale e strategie di trading

Il *trading* algoritmico così come sinora descritto si basa principalmente su modelli matematici e statistici 'classici'. L'ulteriore evoluzione delle potenzialità di tali algoritmi si ha tramite l'integrazione, negli algoritmi di *trading*, di sistemi di intelligenza artificiale in senso stretto[79]. Mentre l'algoritmo di *trading* 'classico' è programmato per prendere la decisione di investimento al realizzarsi di condizioni individuate dall'esse umano; se l'algoritmo di *trading* integra sistemi di intelligenza artificiale, è la 'macchina' stessa a individuare le condizioni di *trading* favorevoli per l'investimento.

---

[77] Considerando 62 MiFID II.

[78] Considerando 62 MiFID II.

[79] Più correttamente si parla di 'algoritmi di *trading* basati sull'intelligenza artificiale", per riferirsi al fatto che gli algoritmi di *trading* operano sui mercati usando i risultati prodotti dai sistemi di intelligenza artificiale.

In un recente studio sull'uso dell'intelligenza da parte degli *hedge fund* negli Stati Uniti, si riporta che gli stessi *hedge fund* utilizzano termini diversi per denominare e definire i loro sistemi basati sull'intelligenza artificiale e che, sebbene rientrino tutti nella definizione di IA stabilita dal Congresso nel National Defense Authorization Act del 2019, diverse società non considerano queste tecnologie una vera e propria intelligenza aritificiale. Cfr. U.S. SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, *AI in the Real World. Hedge Funds' Use of Artificial Intelligence in Trading*, 2024, nonché A. AZZUTTI–W.G. RINGE–H.S. STIEHL, *Machine Learning, Market Manipulation*, *op. cit.*, p. 85 secondo cui grazie ai progressi simultanei compiuti nell'elaborazione ad alte prestazioni e nella comunicazione (ad es., *edge*/*cloud computing*) e nell'analisi dei b*ig data*, i metodi di *machine learning* consentono oggi agli algoritmi di *trading* di essere molto più flessibili rispetto a condizioni di mercato in continua evoluzione, sotto diversi livelli di autonomia. *Machine learning* e *big data* sono gli ingredienti fondamentali della maggior parte delle strategie di *trading* algoritmico innovative e all'avanguardia (traduzione nostra).

Sicché le diverse capacità dei sistemi di intelligenza artificiale – quali ad esempio la capacità predittiva – li rendono dei candidati naturale per l'applicazione al *trading*[80]. Ciò comporta tuttavia anche il rischio che siano essi anche in grado di ottimizzare o portare alla luce strategie ingannevoli e aggressive e potenzialmente penalmente rilevanti.

Proprio per questa ragione, è necessario innanzitutto definire cosa si intende con l'espressione – talvolta abusata – 'intelligenza artificiale'. Lo sforzo definitorio è rilevante, non solo a fini teorici[81], ma anche e soprattutto pratici. Come si vedrà, comprendere quando si è di fronte a un sistema di intelligenza artificiale e come tale sistema può essere qualificato permette di tracciare i confini della responsabilità penale per reati commessi da o tramite l'utilizzo di tali sistemi.

---

[80] Cfr. M. KEARNS–Y. NEVMYVAKA, *Machine Learning for Market Microstructure and High Frequency Trading*, in D. Easley–Lopez de Prado M.–O'Hara M. (eds.), High Frequency Trading, Risk Books, 2013, pp. 91-124.

Il *machine learning* nell'ambito del *fintech* è utilizzato, oltre che per il *trading*, anche per:

1) rilevamento e prevenzione delle frodi, tramite monitoraggio in tempo reale delle transazioni, identificazione di *pattern* o comportamenti insoliti. (Analizzando i dati storici delle transazioni, i sistemi basati su *machine learning* possono segnalare attività potenzialmente fraudolente con maggiore precisione rispetto ai sistemi tradizionali basati su regole);
2) *credit scoring* e gestione del rischio. I sistemi basati sul *machine learning* valutano la probabilità di insolvenza o morosità sulla base di dati diversi da quelli usati dai sistemi tradizionali (i.e. storia creditizia del singolo), come l'attività sui social media, la cronologia dei pagamenti e persino i modelli di utilizzo dello smartphone. L'ampia gamma di dati a cui possono attingere i sistemi basati su intelligenza artificiale consente quindi di prendere decisioni più informate e di gestire il rischio in modo più efficace;
3) fornitura servizi finanziari personalizzati, ad esempio *robo advisory* su investimenti e gestione del portafoglio, in base agli obiettivi finanziari, alla propensione al rischio e alle condizioni di mercato o la creazione di prodotti finanziari personalizzati servizio clienti e assistenza;
4) chatbot e assistenti virtuali per la gestione delle richieste dei clienti, elaborare le transazioni e fornire consulenza finanziaria. Questi sistemi sono in grado di gestire grandi volumi di domande, fornendo risposte immediate e liberando gli agenti umani per compiti più complessi.

[81] Il concetto di intelligenza artificiale affonda le radici nell'ambito scientifico, che adotta un linguaggio differente da quello tecnico giuridico. La 'traduzione' del concetto matematico in concetto giuridico è necessario, però, ai fini del presente lavoro, tenuto conto dei principi fondamentali che governano il diritto penale, primo fra tutti il principio di legalità e i suoi corollari. Cfr. A. GIANNINI, *Criminal behavior and accountability of artificial intelligence systems*, Eleven Publishers, Maastricht, 2023, pp. 25-44. Sulla necessità di una nozione di intelligenza artificiale "penalisticamente orientata", F. CONSULICH, Flash offenders, *op. cit.*, p. 1017; nonché B. FRAGASSO, *La responsabilità penale del produttore di sistemi di intelligenza artificiale,* in Dir. Pen. cont. Riv Trim., 2023, fasc. 1, pp. 26-45.

Nel linguaggio comune, il termine 'intelligenza artificiale' è usato talvolta in senso generico e atecnico per riferirsi a sistemi basati su algoritmi o sistemi automatizzati, spesso mancando di sottolinearne la differenza con i tradizionali sistemi *software* o dagli approcci di programmazione più semplici. Si tratta di un'impropria sineddoche non accettabile quando ci si riferisce a un ambito tecnico come quello oggetto del presente lavoro[82].

I tentativi di individuare una nozione univoca di IA sono innumerevoli e convergenti – per la maggior parte – su alcune caratteristiche tipiche: la capacità di percepire l'ambiente esterno, di elaborare informazioni (raccolta e interpretazione dei dati), il *decision-making* (inclusi ragionamento e apprendimento), l'esecuzione di azioni e compiti in modo adattivo (ossia in risposta ai cambiamenti nell'ambiente circostante) con un certo livello di autonomia e la facoltà di raggiungere obiettivi specifici[83].

Tra le tante definizioni, tuttavia, in questa sede pare opportuno fare riferimento al testo – di recente approvazione – del Regolamento sull'intelligenza artificiale (c.d. AI Act)[84]. A norma dell'art. 3, un sistema di intelligenza artificiale è "un sistema

---

[82] Come nota H. SURDEN, *Artificial Intelligence and Law: An Overview*, in Georgia State University Law Review, 2019, vol. 35, issue 4, p. 1308 si tratta, in altri termini, di una 'rappresentazione operativa' che descrive genericamente tutti quei programmi che compiono attività automatizzate con capacità cognitive analoghe – ma non identiche – a quelle dell'uomo. Sarebbe tuttavia errato pensare che le intelligenze artificiali producano i loro risultati usando una sorta di cognizione informatica di sintesi che eguaglia o supera il pensiero umano. "La realtà è che gli attuali sistemi di IA non sono assolutamente macchine intelligenti e pensanti in senso stretto" (traduzione nostra).

Sul punto, *ex multis*, C. BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. it. dir. proc. pen.*, 2019, fasc. 4, p. 1914 e J. KAPLAN, *Artificial Intelligence: What Everyone Needs to Know,* Oxford, 2016, p. 1.

[83] Un esempio di possibile variabile che la macchina deve prendere in considerazione: la società di *trading* Alfa vuole prevedere il prezzo dell'azione XYZ a 1 secondo da ora. La società ritiene che il volume attuale nel *book* degli ordini e la tendenza del prezzo negli ultimi 10 secondi contengano informazioni preziose su dove si dirigerà il prezzo nel secondo successivo. Il "volume nel book degli ordini" e la "tendenza del prezzo negli ultimi 10 secondi" sono le variabili del modello predittivo.

[84] Regolamento (Ue) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale). Pubblicato in Gazzetta Ufficiale dell'Unione europea il 12 luglio 2024 ed entrato in vigore l'1 agosto 2024. Testo disponibile al seguente link https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=OJ%3AL_202401689#d1e2918-1-1.

Le altre principali definizioni sono le seguenti.

automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali"[85].

Definzione IOSCO, *The use of artificial intelligence and machine learning by market intermediaries and asset managers. Final Report*, 2021 "la scienza e l'ingegneria di realizzare macchine intelligenti, o semplicemente lo studio dei metodi per far sì che i computer imitino le decisioni umane per risolvere problemi. L'IA include compiti come apprendimento, ragionamento, pianificazione, percezione, comprensione del linguaggio e robotica" (traduzione nostra).
Definzione del Financial Stability Board: "la teoria e lo sviluppo di sistemi informatici capaci di svolgere compiti che tradizionalmente richiedono intelligenza umana" (traduzione nostra).
Definizione contenuta nelle Linee guida dell'OCSE "l'intelligenza artificiale è un sistema basato su macchine che può, per un insieme dato di obiettivi definiti dall'uomo, fare previsioni, raccomandazioni o decisioni che influenzano ambienti reali o virtuali. I sistemi di IA sono progettati per operare con diversi livelli di autonomia" (traduzione nostra).
Definizione di McCarthy, che si riferisce all'intelligenza artificiale come la scienza e l'ingegneria di creare macchine intelligenti in particolare programmi informatici intelligenti.
A queste si aggiunge l'ampio studio sulle diverse definizioni di intelligenza artificiale condotto da P. RUSSELL–S.J. NORVIG, *Artificial Intelligence: A Modern Approach*, IV ed., London, Pearson, 2020 che, analizzando le diverse definizioni di intelligenza artificiale, le organizza in quattro categorie: sistemi che pensano come gli esseri mani, sistemi che operano come gli esseri umani, sistemi che pensano razionalmente, sistemi che agiscono razionalmente. Secondo gli Autori, un agente intelligente esegue le azioni migliori possibili in una situazione ed è razionale l'agente che "fa la cosa giusta".
Nell'ambito della legislazione americana, la principale nozione di intelligenza artificiale è contenuta nel National Artificial Intelligence Initiative Act del 2020, sec. 5002, n.3 un sistema basato su macchine in grado, per un determinato insieme di obiettivi definiti dall'uomo, di fare previsioni, raccomandazioni o decisioni che influenzano ambienti reali o virtuali. I sistemi di intelligenza artificiale utilizzano input basati sulla macchina e sull'uomo per a) percepire ambienti reali e virtuali; b) astrarre tali percezioni in modelli attraverso l'analisi in modo automatizzato; e c) utilizzare l'inferenza del modello per formulare opzioni di informazione o azione. (traduzione nostra, testo originale disponibile al link https://www.congress.gov/bill/116th-congress/house-bill/6216). A tale definizione rimanda, peraltro, anche il testo della proposta di Financial Artificial Intelligence Risk Reduction Act del 2024 (S.3554 – FAIRR Act, disponile al link https://www.congress.gov/116/bills/hr6216/BILLS-116hr6216ih.pdf).
Più, in generale, sulle diverse definizioni di 'intelligenza artificiale' fornite nel corso del tempo, si veda F. CONSULICH, Flash offenders, *op. cit.*, p. 1017.

[85] La Proposta di Regolamento del Parlamento Europeo e del Consiglio, nella versione del 6 dicembre 2022, si esprimeva invece in questi termini: è intelligenza artificiale "un sistema progettato per funzionare con elementi di autonomia e che, sulla base di dati e input forniti da machine e/o dall'uomo, deduce come raggiungere una determinate serie di obiettivi avvalendosi di approcci di apprendimento 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.

Si tratta di una definizione generica, capace di includere le diverse categorizzazioni elaborate in dottrina sulla base delle differenti capacità dei sistemi in questione[86]: IA 'deboli' e IA 'forti'[87] in base alle capacità e potenziali; oppure, a seconda del grado di autonomia del sistema rispetto all'intelligenza umana, IA assistita, aumentata o autonoma[88] e infine fra apprendimento supervisionato, non supervisionato e 'per rinforzo' (e la sottocategoria

Quanto al testo definitivo dell'AI Act, occorre rilevare che nel Considerando 12 si elencano le principali caratteristiche dei sistemi di intelligenza artificiale, che la distinguono dai tradizionali sistemi software o dagli approcci di programmazione più semplici. Innanzitutto la "capacità inferenziale. Tale capacità inferenziale si riferisce al processo di ottenimento degli output, quali previsioni, contenuti, raccomandazioni o decisioni, che possono influenzare gli ambienti fisici e virtuali e alla capacità dei sistemi di IA di ricavare modelli o algoritmi da input o dati. Le tecniche che consentono l'inferenza nella
costruzione di un sistema di IA comprendono approcci di apprendimento automatico che imparano dai dati come conseguire determinati obiettivi e approcci basati sulla logica e sulla conoscenza che traggono inferenze dalla conoscenza codificata o dalla rappresentazione simbolica del compito da risolvere. La capacità inferenziale di un sistema di IA trascende l'elaborazione di base dei dati e consente l'apprendimento, il ragionamento o la modellizzazione". Si evidenzia poi l'automazione, che "si riferisce al fatto che il funzionamento dei sistemi di IA prevede l'uso di macchine".
I sistemi di IA "possono operare in base a obiettivi espliciti definiti o a obiettivi impliciti. Gli obiettivi del sistema di IA possono essere diversi dalla finalità prevista del sistema di IA in un contesto specifico.
I sistemi di IA sono progettati per funzionare con livelli di autonomia variabili, il che significa che dispongono di un certo grado di autonomia di azione rispetto al coinvolgimento umano e di capacità di funzionare senza l'intervento umano.
L'adattabilità che un sistema di IA potrebbe presentare dopo la diffusione si riferisce alle capacità di autoapprendimento, che consentono al sistema di cambiare durante l'uso".

[86] Cfr. N. ABRIANI–G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale*, Bologna, 2021, pp. 21 ss., nonché I. SALVADORI, Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale, in Riv. it. Dir. proc. Pen., 2021, fasc. 1, p. 91. Per una panoramica dei diversi criteri classificatori delle i.a. si veda: O. POLLICINO – P. DUNN, *Intelligenza artificiale e democrazia*, Milano, Bocconi Univerisity Press, 2024, pp. 77-87

[87] Termine usato da H. SURDEN, *Artificial Intelligence and Law*, *op. cit.*, p. 1309 e *passim* e ripresa, *ex multis*, da F. CONSULICH–M. MAUGERI–C. MILIA–T.N. POLI–G. TROVATORE, *AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?*, Quaderno giuridico Consob n. 29, maggio 2023; F. ANNUNZIATA, *Artificial Intelligence and Market Abuse Legislation. A European Perspective*, Edward Elgar, 2023 p. 32 e 60-63 e O. POLLICINO – P. DUNN, *Intelligenza artificiale*, *op. cit.*, pp. 75-77.

[88] In inglese: *assisted AI*, *augmented AI* e *autonomous AI*

dell'apprendimento 'profondo per rinforzo')[89], in base alla capacità di apprendimento (c.d. *machine learning*)[90].

4.1. IA deboli e IA forti

Una parte della letteratura distingue fra intelligenze artificiali 'deboli' e intelligenze artificiali 'forti'[91].

Alla prima categoria – in inglese *weak AI* o *narrow AI* – appartengono i sistemi i cui *output* dipendono dalle istruzioni prestabilite dai produttori, programmatori o utenti. L'intelligenza artificiale 'debole', è progettata per svolgere compiti specifici e limitati, ossia per eseguire una particolare funzione o un insieme limitato di funzioni[92].

Sono invece definiti 'forti' i programmi dotati di capacità di autoapprendimento, che producono *output* autonomi rispetto agli *input* inizialmente impartiti. Ciò implica la capacità di un sistema di comprendere, apprendere e prendere decisioni in modo analogo agli esseri umani. Le principali caratteristiche dei sistemi 'forti' sono la capacità di ragionamento e risoluzione di problemi in contesti nuovi, la capacità di apprendimento autonomo e adattamento, la comprensione e generazione di linguaggio naturale al pari di quello umano. In definitiva, si tratta di sistemi con un buon grado di autonomia e sui quali ha un ridotto controllo per quanto attiene al loro funzionamento e ai risultati che da questi sono prodotti.

4.2. IA assistita, IA aumentata, e IA autonoma

Sul diverso livello di interazione fra l'umano e la 'macchina' si fonda la seconda classificazione dei sistemi di intelligenza artificiale.

Il controllo umano è totale nella c.d. IA assistita.

---

[89] In inglese, rispettivamente, *supervised learning*, *unsupervised learning* e *reinforcement learning* (e sottocategoria del *deep reinforcement learning*).

[90] Approccio classificatorio che si basa sui differenti modelli statistico-matematici di elaborazione delle informazioni e di apprendimento automatico. Sul punto O. POLLICINO – P. DUNN, *Intelligenza artificiale*, *op. cit.*, pp. 81-83.

[91] La distinzione è riportata da P. RUSSELL–S.J. NORVIG, *Artificial Intelligence, op. cit.*, che definiscono le IA 'deboli' come prassi di ragionamento elementari in grado di trovare soluzioni complete; mentre le IA 'forti' si basano essenzialmente sulla possibilità di avere una coscienza.

[92] Alcuni esempi di IA c.d. debole, fra i più noti, sono: assistenti vocali come Siri e Alexa, i software di riconoscimento facciale, l'algoritmo di ricerca di Google e le auto a guida autonoma.

Questa forma di intelligenza artificiale è infatti concepita per eseguire specifici compiti sotto la supervisione dell'essere umano, senza alcuna capacità di prendere decisioni autonome che restano completamente nel dominio dell'uomo. I sistemi di intelligenza artificiale assistista applicati al *trading* costituiscono quindi uno strumento avanzato di analisi dei dati, ad esempio dei dati storici relativi ai prezzi degli strumenti finanziari e delle tendenze di mercato, e sono in grado di fornire indicazioni sull'acquisto o la vendita degli stessi. Le decisioni finali di acquisto o vendita vengono però prese dagli operatori umani.

L'intelligenza artificiale aumentata (o potenziata), invece, ha un minimo grado di autonomia e capacità di prendere decisioni. Si basa sull'interazione continua con gli esseri umani e combina le capacità analitiche della macchina alla supervisione umana.

Un sistema di *trading* aumentato, ad esempio, esegue operazioni basate su segnali generati dall'IA, ma richiede conferma o supervisione umana. Il sistema di intelligenza artificiale individua le migliori opportunità di *trading*, sulla base di modelli predittivi – eventualmente agisce in modo autonomo sul mercato –, mentre l'essere umano interviene per confermare le decisioni o modificare i parametri del modello[93].

I sistemi di intelligenza artificiale autonoma operano, invece, con un intervento umano assai limitato. Questi sistemi sono progettati per prendere decisioni e agire autonomamente, basandosi esclusivamente sui dati e sugli algoritmi con cui sono stati programmati. L'IA autonoma rappresenta il livello più avanzato di intelligenza artificiale, dove la macchina è in grado di eseguire compiti complessi e prendere decisioni in modo indipendente, adattandosi dinamicamente all'ambiente senza bisogno di supervisione costante[94].

Il sistema di *trading* basato su IA autonoma, sulla base dei dati elaborati, prende decisioni di *trading* ed esegue le relative operazioni senza bisogno di un intervento umano[95].

---

[93] Ad esempio, il *trader* umano si serve di una piattaforma che analizza i dati di mercato in tempo reale e genera segnali di *trading*. Quando viene identificata una potenziale opportunità di acquisto di un'azione, il sistema invia una notifica al *trader*, che può confermare l'operazione. La piattaforma continua a monitorare l'operazione e suggerisce modifiche, che il *trader* può approvare o modificare.

[94] S. CHOPRA–L.F. WHITE, *A legal theory for autonomous artificial agents*, University of Michigan Press, 2011.

[95] Ciò non significa, evidentemente, che l'essere umano non possa controllare o intervenire in alcun modo sull'operato dell'algoritmo.

4.3. *Machine learning*: apprendimento supervisionato, non supervisionato e 'per rinforzo'

Un terzo approccio distingue, nell'ambito del *machine learning* – o 'apprendimento automatico' – fra apprendimento supervisionato, non supervisionato e apprendimento 'per rinforzo'.

Il *machine learning* è un ambito dell'informatica che si basa, tra l'altro, su algoritmi e tecniche finalizzate all'apprendimento automatico, sfruttando la statistica computazionale e l'ottimizzazione matematica. I sistemi di *machine learning* si caratterizzano per la capacità di generare modelli predittivi partendo da grandi *dataset*.

L'uso del termine 'apprendimento' non deve però trarre in inganno: la capacità di osservazione dei dati e di riconoscimento di *pattern* che consente di stabilire degli schemi da seguire per ottenere il risultato desiderato – metodo induttivo-probabilistico[96] – non significa che la macchina sia in grado di apprende come un essere umano[97]. Piuttosto, quello dei sistemi di *machine learning* è un apprendimento 'funzionale', che parte dall'analisi dei dati, passa per la valutazione dei dati stessi e la formulazione di modelli statistici che descrivano la realtà osservata, e si conclude con l'ottimizzazione di tali modelli e la conseguente formulazione di una strategia che risponda ai *feedback* raccolti con l'esperienza e l'interazione con l'ambiente circostante. L'apprendimento in questione è un concetto legato non tanto alla semantica, quanto più facoltà della macchina modificare le proprie prestazioni nel corso del tempo, in virtù dell'interazione con l'esterno[98].

Ebbene, come detto, queste caratterstiche rendono l'apprendimento automatico un candidato naturale per l'applicazione al *trading*[99].

---

[96] Anche detto di *bottom-up*, in contrapposizione al metodo simbolico-deduttivo (di *top down*) tipico dei sistemi a programmazione esplicita (in cui il programmatore usa impartisce comandi del tipo '*if-then*').

[97] Benché sia capace di prendere delle decisioni sulla base dei dati raccolti, a differenza dell'essere umano, l'AI non è in grado di attribuire ad essi dei significati. Cfr. M.B. MAGRO, *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, in Leg. pen., 10 maggio 2020, p. 12.

[98] Cfr. H. SURDEN, *Artificial Intelligence and Law*, *op. cit*., p. 1311 che sottolinea in questo contesto il termine "apprendimento" è usata come metafora e che non coincide con la capacità di apprendimento dell'essere umano. Nello stesso senso: P. RUSSELL–S.J. NORVIG, *Artificial*, *op. cit.*

[99] Cfr. M. KEARNS–Y. NEVMYVAKA, *Machine Learning*, op. cit., pp. 91-124.

Il *machine learning* nell'ambito del *fintech* è utilizzato, oltre che per il *trading*, anche per:

I meccanismi di *machine learning* creano un sistema che non si limita ad applicare e replicare serie di comandi o impulsi, va oltre la mera riproduzione di un compito delegato dall'essere umano, essendo capace, sulla base delle regole definite dal proprio programmatore, di elaborare in modo autonomo criteri di inferenza tra i dati forniti[100].

Il procedimento di apprendimento è più o meno assistito dall'uomo, a seconda che si tratti di *supervised learning*, *unsupervised learning* o *reinforcement learning*[101].

L'apprendimento supervisionato è un approccio all'apprendimento automatico definito dall'uso di *set* di dati etichettati. Viene infatti utilizzato allo scopo di classificazione e regressione di dati pre-etichettati. Il programma viene cioè addestrato per essere in grado di classificare correttamente dei dati, in base all'etichetta fornita dal programmatore. Nell'apprendimento supervisionato è, dunque, il programmatore a guidare la 'macchina' nella corretta classificazione dei dati forniti[102].

---

5) rilevamento e prevenzione delle frodi, tramite monitoraggio in tempo reale delle transazioni, identificazione di *pattern* o comportamenti insoliti. (Analizzando i dati storici delle transazioni, i sistemi basati su *machine learning* possono segnalare attività potenzialmente fraudolente con maggiore precisione rispetto ai sistemi tradizionali basati su regole);
6) *credit scoring* e gestione del rischio. I sistemi basati sul *machine learning* valutano la probabilità di insolvenza o morosità sulla base di dati diversi da quelli usati dai sistemi tradizionali (i.e. storia creditizia del singolo), come l'attività sui social media, la cronologia dei pagamenti e persino i modelli di utilizzo dello smartphone. L'ampia gamma di dati a cui possono attingere i sistemi basati su intelligenza artificiale consente quindi di prendere decisioni più informate e di gestire il rischio in modo più efficace;
7) fornitura servizi finanziari personalizzati, ad esempio *robo advisory* su investimenti e gestione del portafoglio, in base agli obiettivi finanziari, alla propensione al rischio e alle condizioni di mercato o la creazione di prodotti finanziari personalizzati servizio clienti e assistenza;
8) chatbot e assistenti virtuali per la gestione delle richieste dei clienti, elaborare le transazioni e fornire consulenza finanziaria. Questi sistemi sono in grado di gestire grandi volumi di domande, fornendo risposte immediate e liberando gli agenti umani per compiti più complessi.

[100] Cfr. F. PAOLUCCI, *Algoritmi e intelligenza artificiale alla ricerca di una definizione: l'esegesi del Consiglio di Stato, alla luce dell'*AI Act, in Quest. giust., 8 aprile 2022.

[101] Le prime due sono spesso integrate nei c.d. ATS (*autonomous trading system*).

[102] L'addestramento del modello di *supervised learning* si basa su dati raccolti e pre-etichettati (sulla base di precisi *input).* Ad esempio, in un dataset per il riconoscimento di immagini di gatti, le immagini sono gli *input* e le etichette "gatto" o "non gatto" sono gli *output*. Questi dati vengono forniti all'algoritmo, che impara ad associare gli input agli output, ottimizzando i suoi parametri per minimizzare ogni errore.

In ambito finanziario il *supervised learning* applicato al *trading* algoritmico viene utilizzato per scopi di tipo predittivo, ad esempio per prevedere il prezzo di una determinata azione, sulla base dei dati storici. In questo caso, il programmatore addestra l'algoritmo con dati come lo storico dei prezzi delle azioni, i volumi di scambio, dati macroeconomici (es. tassi di interesse, inflazione), notizie finanziarie. Mentre l'*output* è il prezzo dell'azione in un determinato futuro (ad esempio, il prezzo del giorno successivo)[103].

L'apprendimento non supervisionato, invece, utilizza algoritmi di apprendimento automatico per analizzare e raggruppare *set* di dati non pre-etichettati[104].

L'algoritmo crea categorie di dati simili fra di loro, facendo associazioni: individua autonomamente dei *pattern* (ad esempio la regolarità) nei dati con caratteristiche

---

In ambito finanziario, tipicamente vengono usati algoritmi di *supervised learning* per stabilire il merito di credito: sulla base di dati relativi a una società (bilanci, notizie o comunicati) si stabilisce il *rating*.

In ambito differente, gli algoritmi di apprendimento supervisionato vengono utilizzati per per classificare lo *spam* in una cartella separata dalla casella di posta elettronica. Sul punto, h. SURDEN, *Artificial Intelligence and Law*, *op. cit.*, pp. 1312 ss.

[103] In altre parole, l'algoritmo predittivo viene addestrato usando dati storici per prevedere come cambierà il prezzo di un'attività finanziaria. Per fare queste previsioni, il modello utilizza un insieme di variabili che spiegano il cambiamento dei prezzi (c.d. *features* o variabili esplicative). Ad esempio, la tendenza storica del prezzo delle azioni potrebbe indicare qualcosa sulla direzione futura del prezzo.

Una volta fatte le previsioni, queste vengono utilizzate per decidere le azioni di *trading*. Ad esempio, se la previsione indica che il prezzo aumenterà oltre una certa soglia, il sistema di *trading* può decidere che è opportuno acquistare lo strumento finanziario.

La letteratura finanziaria individua alcune criticità in questo approccio bifasico. Innanzitutto il fatto che il modello predittivo cerca di minimizzare l'errore di previsione (cioè, fare previsioni il più accurate possibile), ma questo obiettivo non coincide necessariamente con l'obiettivo finale dell'investitore (ad es. massimizzare il rendimento in relazione al rischio). Inoltre, è frequente che il sistema di utilizzi solo la previsione del modello e ignori altre informazioni utili che potrebbero essere dedotte dalle variabili esplicative. Infine, vi è il rischio che il sistema non prenda in considerazione alcuni fattori esterni, come la mancanza di liquidità e i costi di transazione (applicati alle operazioni di *trading*). Cfr. T. G. FISCHER, *Reinforcement learning in financial markets: a survey*, in FAU Discussion Papers in Economics, 2018, n. 12, Nürnberg, 2018.

[104] Cfr. F. ANNUNZIATA, *Artificial* Intelligence, *op. cit.*, p. 34 che fornisce un esempio che chiarisce in modo efficace la differenza fra apprendimento supervisionato e non supervisionato, differenza che si basa essenzialmente sulla necessità o meno dell'intervento umano per elaborare i dati in modo appropriato. Un modello di *supervised learning* può prevedere quanto tempo ci vuole per far bollire un uovo, ma richiede l'intervento umano per calcolare quanto tempo ci vuole affinché l'acqua raggiunga il punto di ebollizione, a seconda del tipo di apparecchio utilizzato in cucina (ad esempio, a gas, elettrico o a induzione).

simili[105]. In questo ambito, l'intervento umano si inserisce nella fase di validazione dei dati[106].

In finanza, l'utilizzo di questi algoritmi consente di classificare titoli che si muovono in modo simile ad altri, ad esempio per la selezione del portafoglio. O ancora, gli algoritmi di *unsupervised learning* sono integrati negli *automated trading system* (*ATS*) insieme agli algoritmi di *supervised learning* e vengono usati eseguire un'analisi dei *cluster* per estrarre le caratteristiche dai dati e identificare le possibilità di *trading*. Il risultato è usato come *input*, che viene inviato al componente di apprendimento supervisionato per ulteriori passaggi computazionali, come la previsione del prezzo delle azioni[107]. Benché l'apporto in termini di automazione dei processi di investimento dato da questi sistemi sia elevavo, ciò non significa che l'attività di *trading* sia del tutto autonoma rispetto all'essere umano, a cui rimane il compito di analizzare le condizioni di mercato (ad esempio i c.d. *tail risk* e eventi che l'algoritmo non è in grado di cogliere).

Il più avanzato fra i sistemi *machine learning* è l'apprendimento 'per rinforzo' (o *reinforcement learning*), che – a differenza dei sistemi sopra citati - non impara né da *set* di dati etichettati né da dati non etichettati, bensì per tentativi ed errori ('*trial and error*')[108].

---

[105] In sostanza, mentre nell'intelligenza supervisionata si addestra la macchina, nell'intelligenza non supervisionata invece non c'è addestramento e l'algoritmo consente di creare correlazioni che altrimenti l'umano non coglierebbe.

[106] Cfr. F. ANNUNZIATA, *Artificial* Intelligence, *op. cit.*, p. 34, ad esempio, un modello USL può identificare che, in certi momenti della giornata, ci sono più o meno persone attive come acquirenti online. Tuttavia, un analista interviene per determinare quali acquisti possono effettivamente essere collegati alle loro preferenze (traduzione nostra).

[107] Allo stato attuale, benché vengano chiamati sistemi "autonomi", gli ATS dipendono ancora grandemente dal controllo umano e dalla capacità umana di analizzare la continua evoluzione dei mercati. Cfr. A. AZZUTTI–W.G. RINGE–H.S. STIEHL, *Machine Learning, Market Manipulation*, *op. cit.*, P. 91 rilevano che entrambi i metodi sono limitati dalla natura empirica dei dati e non sono in grado di replicare del tutto la capacità umana di reagire ai diversi eventi che accadono sui mercati (capacità di reazione che spesso si basa su intuizioni difficilmente esplicabili).

[108] Cfr. R.S. SUTTON–A. G. BARTO, *Reinforcement Learning: an introduction*, MIT Press, Cambridge, 2017. Rientra nell'ambito dell'apprendimento per rinforzo anche il c.d *deep reinfocerment learning*. Si tratta di una tecnologica basata sulle c.d. reti neurali artificiali (ANNs) - ossia, modelli matematici che in larga misura assomigliano alla struttura del cervello umano - che mirano a migliorare l'approssimazione dei dati di input apprendendo su più livelli di astrazione. Si tratta di una tecnologia che, allo stato attuale, ha trovato applicazione in alcuni settori, fra cui quello dei videogiochi. Nel settore finanziario, invece, il *deep reinforcement learning* è oggetto di studi e simulazioni e, sebbene promettente, non di applicazioni reali. Cfr. A. AZZUTTI–W.G. RINGE–H.S. STIEHL, *Machine Learning, Market Manipulation*, *op. cit.*, p. 111 a conferma del fatto che sono oggetto di ricerca in ambito di finanza computazionale per l'applicazione di metodi di *deep reinforcement learning* sempre più sofisticati e autonomi.

Gli agenti di *reinforcement learning* operano al fine di ottenere un obiettivo determinato e sono in grado di scegliere – interagendo con l'ambiente circostante – in modo autonomo le azioni da compiere per il suo conseguimento. La macchina sceglie qual è l'azione che consente di raggiungere l'obiettivo e, quindi, di ottenere un *reward*. Si lascia quindi alla macchina l'esplorazione delle diverse strategie, remunerandola se e quando trova quella migliore. Per questo si afferma che il sistema di apprendimento per rinforzo impara attraverso un processo di tentativi ed errori: i valori positivi sono associati alle azioni desiderate, e i valori negativi a quelle non desiderate. Nel tempo, l'agente impara ad evitare azioni negative e a cercare azioni positive[109].

Considerando che, nel contesto finanziario, l'agente è il *trader*, l'ambiente in cui agisce è il mercato azionario, l'azione è l'ordine da inviare al mercato, lo stato sono i prezzi o i volumi e il *reward* è il profitto, l'apprendimento per rinforzo agisce sui mercati in modo paragonabile a un *trader* umano: impara dalle proprie esperienze di *trading* ed elabora strategie per perseguire i loro obiettivi di massimizzazione del profitto.

Le specifiche caratteristiche di questa tecnologia sono particolarmente interessanti per un impiego in ambito finanziario: a differenza del *supervised learning* e dell'*unsupervised learning*, gli algoritmi basati sull'apprendimento per rinforzo sono in grado di cogliere aspetti come la liquidità dei mercati e i costi di transazione. Per questo motivo la letteratura finanziaria ha sviluppato modelli di *reinforcement learning* che possono essere impiegati ad esempio per l'allocazione degli *asset*, la gestione del portafoglio e la gestione del rischio, la

---

[109] L'agente di RL (*reinforcement learning*) viene addestrato – tendenzialmente in un ambiente simulato – a scegliere la migliore azione in ogni circostanza. Studiando il contesto, l'algoritmo 'memorizza' quanto ciascuna azione ha contribuito a un obiettivo, ad esempio trarre profitto o ridurre i costi di esecuzione. Se un'azione ha avuto un esito positivo (cioè, cancellare un ordine è seguito da alti profitti alla fine della sessione di *trading*), allora l'algoritmo di *trading* 'impara' a replicare l'azione in un momento successivo in cui le condizioni di mercato sono le medesime. Se invece l'effetto è stato negativo (ad esempio, all'invio di un grande ordine di acquisto sono seguiti alti costi di esecuzione), allora l'azione verrà replicata meno frequentemente.

L'apprendimento per rinforzo integrato in algoritmi di *trading* non svolge la funzione di prevedere il futuro prezzo dello strumento finanziario, bensì quella di scegliere quali azioni compiere per ottenere il maggior profitto dall'acquisto o la vendita dello strumento, scoprendo nel tempo e attraverso l'esperienza qual è la strategia ottimale (cioè quella che storicamente ha portato i migliori risultati). Attraverso un processo di "tentativi ed errori", all'interno di un ambiente incerto e dinamico e dunque sfrutta quanto appreso in passato per ottenere le migliori ricompense (*reward*). Ciò implica anche la capacità di individuare in anticipo le migliori strategia tra tutte le opzioni possibili, sia note che ignote, al fine di prendere decisioni migliori nel futuro. Cfr. A. AZZUTTI–W.G. RINGE–H.S. STIEHL, *Machine Learning, Market Manipulation*, *op. cit.*, 2021, p. 88.

generazione di ordini da inviare al mercato[110], con risultati particolarmente promettenti nel *trading* ad alta frequenza.

Ebbene, benché l'utilizzo dei sistemi di *machine learning* in ambito finanziario sia un fenomeno largamente diffuso, recenti studi dell'ESMA e dell'Autorità di vigilanza sui mercati finanziari olandese – a conferma di quanto già affermato in passato[111] – dimostrano che l'apprendimento supervisionato è la tecnica attualmente più utilizzata per il *machine learning* ma che l'apprendimento per rinforzo rappresenta solo una possibile prospettiva futura[112].

D'altronde, come si è detto, si tratta di una tecnologia che si nutre di dati e il settore finanziario in questo senso è un ambito particolarmente privilegiato. Si pensi ad esempio, all'*high frequency trading*: esso consente di realizzare una quantità assai significativa di scambi, attività produttiva di altrettanti dati, linfa vitale per lo sviluppo di sistemi dei sistemi in questione.

---

[110] Uno fra tutti, M. KEARNS–Y. NEVMYVAKA, *Machine Learning*, *op. cit*., pp. 91-124 che analizzano tre casi sull'applicazione pratica dell'apprendimento automatico a problemi di *trading;* nonché, A. AZZUTTI–W.G. RINGE–H.S. STIEHL, *Machine Learning, Market Manipulation*, *op. cit.*, 2021, pp. 88-89.

Nel *trading* finanziario, l'utilizzo dell'apprendimento per rinforzo RL consente di integrare in un unico sistema le funzioni predittive e quelle di costruzione del portafoglio. Infatti, a differenza dei metodi (non) supervisionati, gli agenti di *reinforcement learning* sono in grado di individuare quali siano le migliori azioni di *trading* (ossia quelle che massimizzano la probabilità di raggiungere l'obiettivo a lungo termine), tenendo conto anche dei vincoli dei mercati reali, come liquidità e costi di transazione.

Il fatto che, nel *reinforcement learning*, il *trader* interagisca con l'ambiente e che, nel processo decisionale, tenga conto di vincoli come la liquidità e i costi di transazione, rende questo sistema più coerente con gli obiettivi dell'investitore e dunque, secondo la letteratura, preferibile rispetto ai sistemi di *trading* basati sull'apprendimento supervisionato e non supervisionato. Cfr. T.G. FISCHER, *Reinforcement learning in financial markets, op. cit.*, pp. 1-48.

[111] M. KEARNS–Y. NEVMYVAKA, *Machine Learning*, *op. cit*., pp. 91-124.

[112] Molte società di *trading* proprietario hanno integrato modelli di apprendimento automatico nei loro algoritmi di *trading*, principalmente sotto forma di apprendimento supervisionato, ma stanno svolgendo studi che riguardano anche l'apprendimento per rinforzo. Tutte le società olandesi che fanno *trading* proprietario, oggetto dello studio, fanno ricordo al *trading* algoritmico, l'80-100% di queste ricorrono a sistemi basati sul *machine learning*. Cfr. DUTCH AUTHORITY FOR THE FINANCIAL MARKETS*, Machine Learning in Algorithmic Trading Application by Dutch Proprietary Trading Firms and Possible Risks*, 2023, p. 12: "questa percentuale è superiore a quanto previsto dall'AFM e dimostra che l'apprendimento automatico non è una 'bolla', ma una parte intrinseca dei modelli di business di molte società di *trading*" (traduzione nostra).

Il *machine learning* e i *big data* sono elementi fondanti del *trading* algoritmico più d'avanguardia[113] e rendono più efficienti molte delle strategie già illustrate con riferimento al *trading* algoritmico 'classico'. Ad esempio, lo *spoofing*[114], il *pinging*[115] *o* il *momentum ignition*[116].

Oltre ai numerosi effetti positivi, l'aumento del ricorso a sistemi automatizzati nei mercati e la progressiva degradazione dell'intervento umano, come si vedrà *infra*, può tuttavia avere anche effetti negativi sull'integrità dei mercati, che non possono essere trascurati, soprattutto se si tiene conto della rilevanza del fenomeno[117].

---

[113] Ci si riferisce al *signal processing* (filtraggio di informazioni significative dai dati grezzi per individuare schemi di *trading*), l'analisi del *sentiment* di mercato, il *news reading* (che sfrutta il ruolo delle notizie provenienti da diversi media per cercare opportunità di investimento) e il riconoscimento di *pattern* (ovvero la capacità computazionale di apprendere dai cambiamenti nei *pattern* dei prezzi sui mercati per classificare le diverse dinamiche dei prezzi di mercato e anticipare movimenti dei prezzi per ottenere un profitto. Si ricorre quindi agli algoritmi basati su IA anche per l'esecuzione. Secondo il Rapporto ESMA 2021, alcuni fondi pensione e fondi speculativi hanno sviluppato modelli di apprendimento automatico per eseguire grandi ordini su diversi mercati e ridurre tempi di negoziazione, al fine di minimizzare il loro impatto sul mercato e, di conseguenza, i costi di transazione.

[114] L'apporto dei sistemi di apprendimento 'per rinforzo' consente una migliore analisi delle microstrutture di mercato, tramite l'immissione di ordini a titolo meramente esplorativo (i.e. che non si intende portare effettivamente a esecuzione).

[115] Il *deep reinforcement learning* sarebbe in grado di trarre deduzioni dall'analisi di mercato e persino apprendere le strategie di *trading* degli altri operatori. Tramite questa conoscenza, i *trader* ai potrebbero essere in grado di anticipare le strategie altrui e gli ordini in procinto di essere immessi sul mercato.

[116] L'obiettivo del *momentum ignition*, è anticipare e dare avvio una tendenza dei prezzi sui mercati per attirare altri *trader* a fare operazioni sullo stesso *asset*. Qui ancora una volta, l'AI può portare rendere più efficiente la strategia, sviluppando la capacità di leggere le tendenze dalla dinamica di mercato tramite dei metodi di *machine learning*.

[117] Nelle principali piattaforme di *trading* dell'UE, così come negli Stati Uniti, una parte significativa delle transazioni è il risultato dell'attività di *trading* automatizzato, compreso l'*hft*.
Come anticipato, fino alla metà del 2019, nel *trading* in obbligazioni non si registrava la presenza di strumenti algoritmici; nel terzo trimestre del 2019, invece, il *trading* algoritmico ha rappresentato circa l'80 per cento del volume. Per i derivati, il rapporto tra *trading* algoritmico e non algoritmico è rimasto stabile fino al secondo trimestre del 2019; dopo quel periodo, il *trading* algoritmico (non *hft*) ha iniziato ad aumentare.
La capillare diffusione del fenomeno si deduce anche dal diffondersi di numerosi schemi fraudolenti posti in essere da soggetti che si dichiarano *leader* nello sviluppo dell'i.a. e che promettono di creare numerose opportunità di investimento e profitto. Tali false informazioni possono, peraltro, essere parte di schemi di *pump and dump*. Cfr. U.S. SECURITIES AND EXCHANGE COMMISSION, *Artificial Intelligence (AI) and Investment Fraud: Investor Alert*, 25 gennaio 2024.

4.4. Autonomia e *black box*: la rilevanza penale

A prescindere dal criterio di classificazione adottato, ciò che caratterizza tutti i sistemi di *trading* automatizzato attualmente impiegati sui mercati è la capacità di rilevare e analizzare i dati che emergono dall'ambiente circostante e utilizzarli per raggiungere un profitto.

Il percorso logico seguito per giungere a tale obiettivo, tuttavia, può risultare più o meno comprensibile per l'essere umano[118] e di frequente il rapporto fra prestazioni dell'algoritmo e comprensibilità del suo agire è inversamente proporzionale[119].

L'oscurità è quindi una caratteristica che definisce, seppur in diversa misura, tutte le forme di intelligenza artificiale descritta.

Meno complesso è comprendere perché un sistema di *supervised learning* a cui sono stati forniti dati pre-etichettati per individuare cani e gatti, attribuisca l'etichetta 'gatto' all'immagine di un felino. Ben più arduo è comprendere i meccanismi di funzionamento degli algoritmi c.d. di *black box*[120], ossia quelle caratterizzati dall'impossibilità di comprendere appieno il processo decisionale seguito dall'IA e di predire quali saranno le conseguenti decisioni o *output*.

---

[118] *Risoluzione del Parlamento europeo 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, 2015/2103 (INL). A. DAVOLA, *Algoritmi decisionali e trasparenza bancaria*, *op. cit.*, p. 184 rileva che "la riconduzione della predizione di un modello complesso ad una spiegazione intuitivamente comprensibile per un soggetto umano rischia di condurre a risultati peggiori di quelli derivanti dal mero uso del modello stesso".

[119] Gli algoritmi che utilizzano una molteplicità di variabili hanno *performance* migliori, ma proprio per questo perdono in trasparenza e verificabilità. D'altra parte occorre rilevare che, nella prassi, le imprese di investimento che utilizzano algoritmi di *trading* sembrano privilegiare le *performance* rispetto alla comprensibilità dei modelli, poiché ciò che rileva – dal punto di vista dell'investitore – non è tanto la comprensione dei meccanismi interni, ma piuttosto i risultati che l'algoritmo produce. Cfr. DUTCH AUTHORITY FOR THE FINANCIAL MARKETS*, Machine Learning in Algorithmic*, *op. cit*., p. 13.

[120] Cfr Y. BATHAEE, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, in Harvard Journal of Law & Technology, 2018, vol. 31, issue 2, pp. 889-938.; F. PASQUALE, *The black box society: the secret algorithms that control money and information*, London, Harvard University Press, 2015. Sui tentativi dare una spiegazione alla logica dell'apprendimento automatico, espressa in un formato comprensibile e leggibile da un essere umano, che evidenzi i *bias* appresi dal modello e permetta di comprendere e validare la logica decisionale: D. PEDRESCHI–F. GIANNOTTI–R. GUIDOTTI–A. MONREALE–S. RUGGIERI–F. TURINI, *Meaningful Explanations of Black Box AI Decision Systems*, Proceedings of the AAAI Conference on Artificial Intelligence, 2019, vol. 33, pp. 9780-9784. Sui rapport fra *black box* e accertamento del nesso causale, si veda C. PIERGALLINI, *Danno da prodotto*, *op. cit.*, p. 475.

La *black box* impedirebbe dunque, anche al programmatore, di ricostruire *ex post* il motivo specifico per cui il sistema ha agito in un determinato modo[121].
Questo sarebbe vero, in particolare, per specifiche tipologie di intelligenza artificiale, riconducibili alle categorie sopra citate come AI 'forte', sistemi di (*deep) reinforcement learning* (che si basano, ad esempio su reti neurali) e AI autonome.
Tuttavia, con riferimento a queste ipotesi, occorre soffermarsi su due aspetti.
Il primo riguarda l'effettiva diffusione di tali sistemi sofisticati nella realtà dei mercati finanziari. Una parte della dottrina ipotizza infatti che allo stato attuale le applicazioni di AI 'forte' e sistemi di *deep reinforcement learning* sono più che altro oggetto di studi teorici e simulazioni, mentre, nella prassi, gli algoritmi di *trading* più diffusi si basano sul *supervised learning*[122]*.* Quest'ultimo agisce sulla base di regole codificate in modo più rigido e limita il proprio campo di azione all'invio di ordini di acquisto o vendita o alla cancellazione di ordini esistenti, limitando la possibilità di porre in essere atti non voluti o non previsti dal programmatore o che comunque potrebbero avere effetti negativi prima di tutto per l'investitore stesso, oltre che per l'integrità del mercato[123]. Cosa che invece potrebbe accadere impiegando il *reinforcement learning*, che come detto è in grado di agire sui mercati con un buon livello di autonomia.
Il secondo aspetto riguarda invece i reali confini dei problemi sollevati con riferimento alla *black box*.
La scarsa comprensione dei meccanismi di funzionamento interno dell'algoritmo interroga infatti la dottrina sulla possibilità di applicare innanzitutto le regole di accertamento della causalità penale[124].
Tuttavia, anche ai fini di dipanare la questione di se e come sia possibile accertare il nesso fra un determinato evento dannoso e l'agire del sistema di *trading*, sembra prioritario interrogarsi sulle conseguenze che l'indipendenza (o

---

[121] Si parla di '*explainability*' dell'algoritmo. Cfr, fra gli altri, A. DAVOLA, *Algoritmi decisionali e trasparenza bancaria*, *op. cit.*, pp 183-189; DUTCH AUTHORITY FOR THE FINANCIAL MARKETS*, Machine Learning*, *op. cit*., pp. 13-14; A. AZZUTTI– W.G. RINGE–H.S. STIEHL, *Machine Learning, Market Manipulation*, *op. cit.,* nonché ID, *Regulating AI Trading*, *op. cit.*; D. PEDRESCHI–F. GIANNOTTI–R. GUIDOTTI–A. MONREALE–S. RUGGIERI–F. TURINI, *Meaningful Explanations*, 2019, *op. cit.*, pp. 9780-9784; F. PASQUALE, *The black box society*, *op. cit.*, pp. 59-100.

[122] Cfr. DUTCH AUTHORITY FOR THE FINANCIAL MARKETS*, Machine Learning*, *op. cit*., p. 13.

[123] Ci si riferisce al rischio di manipolazione del mercato, *insider trading* e collusione tacita, di cui si parlerà *infra*.

[124] La capacità di spiegare i risultati e le decisioni degli algoritmi è rilevante ai fini dell'accertamento della responsabilità penale nella misura in cui occorre individuare il contributo specifico di diversi soggetti intervenuti. Cfr., con specifico riferimento al diritto penale, F. CONSULICH–M. MAUGERI–C. MILIA–T.N. POLI–G. TROVATORE, *AI e abusi di mercato*, *op. cit*., p. 50.

limitata dipendenza) dell'algoritmo dall'uomo potrebbe comportare ai fini dell'accertamento della responsabilità penale.

Si è parlato infatti di algoritmi che agiscono con diversi gradi di autonomia, che raggiunge i livelli più alti nei sistemi 'forti', di *reinforcement learning* o nell'AI autonoma. Dunque, le domande che occorre porsi sono: di che autonomia si tratta? E soprattutto: la diretta conseguenza di questa autonomia è il fatto che le 'macchine' impareranno 'da sole' comportamenti abusivi?

La letteratura finanziaria pare abbastanza cauta sull'effettiva autonomia degli algoritmi di *trading*[125]. Ciò non toglie che valga la pena valutare le possibili implicazioni di un agire 'autonomo' di questi strumenti. Per quanto allo stato attuale si ritenga quantomeno azzardato escludere la presenza un 'umano nel *loop*'[126], se i sistemi più avanzati saranno in grado di apprendere e perfezionare una certa strategia di *trading* in modo autonomo, dato un obiettivo predefinito (tendenzialmente, la massimizzazione del profitto), questo sviluppo è potenzialmente foriero di condotte illecite[127].

Il raffinarsi delle competenze analitiche e computazionali degli algoritmi di *trading* basati sull'intelligenza artificiale potrebbe comportare il rischio di comportamenti abusivi[128]. Ad esempio, considerando come sono concepiti, non è difficile

---

[125] M. KEARNS–Y. NEVMYVAKA, *Machine Learning*, *op. cit,* p. 123 "[we] are not believers in the use of machine learning as a black box, nor the discovery of "surprising" strategies via its application. In each of the case studies, the result of learnings made broad economic and market sense in light of the trading problem considered. However, the numerical optimization of these qualitatitve strategies is where the real power lies. […] Perhaps the most important overarching implication of these lessons is that there will always be a "human in the loop" in machine learning applications to hft (or any other long-term effort to apply machine learning to a challenging, changing domain). But applied tastefully and with care, the approach can be powerful and scalable, and is arguably necessary in the presence of microstructure data of such enormous volume and complexity as confronts us today".

Nello stesso senso, più di recente: DUTCH AUTHORITY FOR THE FINANCIAL MARKETS*, Machine Learning*, *op. cit*., p. 13.

[126] Espressione ricorrente nella letteratura finanziaria per descrivere la presenza di una supervisione umana sull'agire degli algoritmi di *trading:* il sistema funziona principalmente in modo autonomo, ma si rimette al programmatore/utente qualora debba per formulare un giudizio complesso o una valutazione che rimane al di fuori delle proprie capacità del sistema. *Ex multis,* KEARNS–NEVMYVAKA, *Machine Learning*, *op. cit*., p. 123 e H. SURDEN, *Artificial Intelligence and Law*, *op. cit.*, p. 1320.

[127] Sul punto, in particolare, A. AZZUTTI–W.G. RINGE–H.S. STIEHL, *Machine Learning, Market Manipulation*, *op. cit.*, p. 120.

[128] Anche in considerazione delle possibili conseguenze – maggiormente lesive – delle interazioni degli algoritmi di *trading* fra loro (collusione algoritmica). Senza contare l'enorme ruolo che in questo senso potrebbe avere internet come facilitatore di strategie manipolative. Si pensi

immaginare situazioni in cui sistemi di *trading* automatizzato sopra descritti considerino vantaggiosa – e quindi la perseguano – una attività potenzialmente abusiva, anche oltre alla volontà dell'essere umano. Oppure che le strategie illecite vengano poste in essere sfruttando la scarsa comprensibilità dei meccanismi di funzionamento dell'intelligenza artificiale[129].

A seconda di quanto siano sofisticati o meno i sistemi, le azioni illecite commesse da o tramite questi mettono più o meno in discussione la capacità del sistema attualmente vigente di contrastare questi fenomeni abusivi. Ove l'autonomia e l'opacità – che si celano dietro l'elaborazione di enormi quantità di dati e la capacità inferenziale – raggiungono livelli tali da rendere l'azione dell'algoritmo pressoché imprevedibile è maggiore il rischio che i canoni tradizionali della responsabilità penale si rivelino inadeguati.

Si tratta di una questione su cui è ormai aperto il dibattito dottrinale e il settore finanziario può essere un ambito privilegiato per analizzare l'adeguatezza del sistema[130].

Occorre quindi chiedersi se gli algoritmi di *trading* – specie (ma non solo) quelli che si basano su sistemi di intelligenza artificiale – sono in grado di compiere condotte, anche inedite, riconducibili ai reati di *market abuse*[131] e di valutare l'efficacia di contrasto di tale fenomeno delle attuali norme in materia di l'abuso di mercato, specie con riferimento all'individuazione del soggetto responsabile e all'accertamento del nesso causale fra un'azione e la lesione del bene giuridico tutelato.

---

all'influenza che un *tweet bombing* (mezzo che consente una diffusione capillare e a basso costo di informazioni false o fuorvianti) può avere sul prezzo di uno strumento finanziario, tramite la diffusione capillare (e a basso costo) di informazioni false o fuorvianti.

[129] F. CONSULICH, *Intelligenza artificiale e reati finanziari*, in F. Consulich (a cura di), Reati in materia finanziaria, Torino, 2024, p. 243 "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 automazione: non è mera capacità di svolgere un compito senza un operatore umano, ma indipendenza da istruzione esterne di azione, libertà da determinazioni altrui".

[130] F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale. Prospettive punitive nazionali dopo l'*AI Act, in Diritto di difesa, 17 dicembre 2024, nota che "un ragionamento fondato in chiave di offesa ed eventuale imputazione penale è attuale solo rispetto ai mercati finanziari, poiché questi hanno sperimentato violenti eventi manipolativi" poiché solo in tale ambito si è, ad oggi, avuta manifestazione di offese compiute da o attraverso l'intelligenza artificiale.

[131] A. AZZUTTI– W.G. RINGE–H.S. STIEHL, *Machine Learning, Market Manipulation*, *op. cit.*, p. 121.

CAPITOLO II

IL CONTESTO NORMATIVO

SOMMARIO: 1. Premessa – 2. Le fonti normative sovranazionali – 2.1. La Direttiva MAD II – 2.2. Il Regolamento MAR – 2.3. La Direttiva MiFID II – 2.4 Gli interventi normativi più recenti: AI Act e AI Liability Act Proposal – 3. La disciplina italiana – 3.1. Premessa – 3.2. Il reato di abuso di informazioni privilegiate – 3.3. L'illecito amministrativo di abuso di informazioni privilegiate – 3.4. Il reato di manipolazione del mercato – 3.5. L'illecito amministrativo di manipolazione del mercato – 3.6 Profili regolamentari

1. Premessa

Le principali criticità emerse negli ultimi anni in riferimento al *trading* algoritmico concernono in particolare il legame fra il ricorso a tale forma di negoziazione e le perturbazioni del mercato.

Sempre maggiore attenzione è stata riservata - anche dalle autorità di vigilanza – allo studio delle possibili ripercussioni derivanti dall'incremento della velocità operativa dei partecipanti al mercato, specie in termini di immissione, modifica e cancellazione degli ordini. D'altronde, non si può trascurare il fatto che alcuni eventi *shock* occorsi nei primi anni duemila abbiano dimostrato una connessione fra utilizzo di algoritmi di *trading* e aumento del rischio sistemico per la qualità del mercato (in termini di efficienza informativa dei prezzi, volatilità e liquidità) e, più in generale, per l'integrità del mercato.

In questo senso è quindi rilevante analizzare le disposizioni normative in materia – di fonte nazionale e sovranazionale – per comprendere se vi siano strumenti di tutela dell'integrità dei mercati capaci di prevenire o contrastare le nuove condotte potenzialmente lesive, agevolate dall'evoluzione tecnologica nei sistemi di *trading*.

A tal fine, è innanzitutto necessario volgere lo sguardo all'oggetto di tutela dell'ampio *corpus* normativo in materia di abusi di mercato. Sebbene l'individuazione del bene giuridico protetto delle diverse norme in materia di abusi di mercato sia stata ampiamente discussa in dottrina[132], matrice comune della

[132] L'individuazione del bene giuridico tutelato dalle norme che sanzionano gli abusi di mercato è stato oggetto di ampio dibattito in dottrina, di cui dà conto M. MIEDICO, *Gli abusi di*

disciplina è certamente la necessità di garantire che il mercato non sia alterato da comportamenti che possono frustrarne il corretto funzionamento. A tale scopo, oltre alla tutela del risparmio e della fiducia nei mercati finanziari, è centrale la protezione di alcuni beni strumentali individuabili nella correttezza, nella veridicità e nell'accessibilità delle informazioni, nella trasparenza oltre che nella regolarità del funzionamento del mercato[133]. D'altronde, come sottolinea da tempo la più attenta dottrina, la corretta e completa informazione al mercato è presupposto necessario per il suo corretto funzionamento[134].

---

mercato, in A. Alessandri (a cura di), Reati in materia econmica, Torino, Giappichelli, 2017, II. ed., pp. 306-308. Si rinvia dunque ai riferimenti ivi citati e, in particolare, senza pretesa di esaustività alcuna, a C. PEDRAZZI, *Problemi del delitto di aggiotaggio*, 1958, ora in Id., *Diritto penale*, vol. IV - Scritti di diritto penale dell'economia, Milano, Giuffrè, 2003, pp. 12-15, nonché ID, *Interessi economici e tutela penale*, 1958, ora in Id, Diritto penale, vol. III - Scritti di diritto penale dell'economia, Milano, Giuffrè 2003, pp. 187-200; S. SEMINARA, Insider trading *e diritto penale*, Milano, Giuffrè, 1989, p. 22; F. BRICOLA, *Profili penali della disciplina del mercato finanziario*, in Banca, borsa e tit. cred., 1990, fasc. I, p. 16 poi in, Scritti di diritto penale, vol. II, tomo II, Milano, Giuffrè, 1997, pp. 3425-3466; L. FOFFANI, *La nuova disciplina penale dell'"insider trading" e delle frodi nel mercato mobiliare*, in Riv. trim. dir. pen. econ., 1991, p. 911; F. CONSULICH, *La giustizia e il mercato. Miti e realtà di una tutela penale dell'investimento mobiliare*, Milano, Giuffrè, 2010, p. 8; F. MUCCIARELLI, *Art. 184*, in Il testo unico della finanza, a cura di M. Fratini–G. Gasparri, vol. III, Milano, Utet, 2012, p. 2338; nonché ID, *Art. 185*, in Il testo unico della finanza, a cura di M. Fratini–G. Gasparri, vol. III, Milano, Utet, 2012, p. 2392; F. D'ALESSANDRO, *Regolatori del mercato, enforcement e sistema penale*, Torino, Giappichelli, 2014, p. 28; M. GAMBARDELLA, *Condotte economiche e responsabilità penale*, Torino, Giappichelli, 2020, p. 387 e, più di recente, F. MUCCIARELLI, *Mercato finanziario e tutela penale*, in F. Consulich (a cura di), *Reati in materia finanziaria*, Torino, Giappichelli, 2024, pp. 111-116.

[133] Cfr., *ex multis,* F. D'ALESSANDRO, *Regolatori del mercato*, *op. cit.*, pp. 172-173 che sottolinea l'evoluzione della tutela che ha caratterizzato il reato dalla dimensione del patrimonio individuale a quella del risparmio collettivo.

[134] *Ex multis,* C. PEDRAZZI, *Interessi economici e tutela penale*, *op. cit.*, pp. 187-200; nonché F. D'ALESSANDRO, *Regolatori del mercato, op. cit.*, p. 171, secondo cui il regolare andamento dei mercati è un'espressione capace di sintetizzare l'interesse diffuso a che le scelte di investimento "possano svolgersi in un contesto di efficienza economica […] che non sia strumentalizzato né da sfruttamenti abusivi di posizioni di vantaggio informativo, né da condotte che alterino surrettiziamente il corretto meccanismo di formazione dei prezzi".
Nello stesso senso, S. SEMINARA, *Informazione finanziaria e mercato: alla ricerca di una strategia del controllo penale amministrativo*, in *Analisi Giuridica dell'Economia, Studi e discussioni sul diritto dell'impresa*, 2006, fasc. 2, pp. 255-278; nonché S. SEMINARA, *Diritto penale commerciale. Il diritto penale del mercato mobiliare*, III, Torino, 2022, pp. 8-12 nonché 63-66 secondo cui tutte le notizie rilevanti devono raggiungere tempestivamente il mercato con modalità tali da garantire al pubblico la simultanea accessibilità, con il connesso divieto di uno sfruttamento anticipato delle conoscenze destinate a influire sul prezzo dei titoli ed è altresì necessario che sul mercato non circolino notizi false né si compiano operazioni in grado di distorcere i prezzi e così alterare il gioco della domanda e dell'offerta. Per questa via l'efficienza informativa del mercato si converte nella sua efficienza allocativa. L'Autore individua l'elemento che accomuna i reati di abuso di

Di qui la distinzione fra il caso in cui l'informazione assume i caratteri della veridicità e della non pubblicità ed è oggetto del reato di abuso di informazioni privilegiate e il caso in cui essa si connota per non veridicità e pubblicità e costituisce oggetto del reato di manipolazione del mercato[135].

2. Le fonti normative sovranazionali

La centralità della tutela dell'informazione emerge prepotentemente nella normativa europea, che nel tempo si è evoluta, mantenendo fermo l'obiettivo di preservare la fiducia degli investitori nei mercati e rimuovere gli ostacoli alla piena trasparenza e disparità di accesso alle informazioni[136].
La prima Direttiva europea risale al 1979[137], seguita nel 1989 da una seconda Direttiva: la *insider dealing directive*[138]. Quest'ultima in particolare segnò un significativo punto di svolta in materia perché, per quanto il proprio ambito di applicazione fosse limitato – così come quello della prima Direttiva – alla condotta di *insider trading*, gettò le basi per l'attuale struttura delle norme UE che sanzionano l'abuso di informazioni privilegiate[139]. Successivamente, vennero le

---

informazioni privilegiate e manipolazione del mercato nella lesività nei confronti del corretto funzionamento del mercato e nell'oggetto costituito dall'informazione.

[135] In questo senso F. MUCCIARELLI, *Gli illeciti di abuso di mercato, la responsabilità dell'ente e l'informazione*, in Riv. trim. dir. pen. econ., 2008, fasc. 4, pp. 823-860.

[136] Sul ruolo della legislazione europea in ambito finanziario, cfr. S. SEMINARA, *L'evoluzione europea del diritto penale del mercato finanziario nella prospettiva italiana*, in S. CANESTRARI−L. FOFFANI (a cura di), Il diritto penale nella prospettiva europea, 2005, pp. 219-253; A. ALESSANDRI, *Impresa e giustizia penale: tra passato e futuro. Un'introduzion*e, in Atti del Convegno di studio "Enrico de Nicola", Milano 14 marzo 2008, Milano, 2009, 32 ss.; L. FOFFANI, *Politica criminale europea e sistema finanziario: l'esempio degli abusi di mercato*, in Dir. Pen. Cont., Riv. Trim., 2014, fasc. 3-4, pp. 65-72.

[137] Direttiva 79/279/CEE del Consiglio del 5 marzo 1979 sul coordinamento delle condizioni per l'ammissione dei titoli al listing ufficiale della borsa valori prevede per la prima volta a livello europeo l'obbligo di divulgare sviluppi rilevanti non pubblici nell'ambito di attività dell'emittente, suscettibili di provocare variazioni sostanziali nel prezzo delle proprie azioni o di influenzare in modo sostanziale la propria capacità di adempiere agli impegni derivanti da titoli di debito.

[138] Direttiva 89/592/CEE del Consiglio del 13 novembre 1989 sul coordinamento delle normative concernenti le operazioni effettuate da persone in possesso di informazioni privilegiate (*insider trading*).

[139] In particolare, come evidenzia F. ANNUNZIATA, *Artificial Intelligence*, *op. cit.*, p. 6, la Direttiva offriva già una formulazione delle tre proibizioni di base contro: (a) l'acquisizione o la disposizione di titoli a cui si riferiscono informazioni privilegiate (Art. 2(1)); (b) la divulgazione di informazioni privilegiate a terzi, salvo alcune eccezioni limitate (Art. 3(a)); e (c) raccomandare a terzi di acquistare o dismettere i titoli sulla base di informazioni privilegiate (Art. 3(b)). Inoltre,

direttive 93/6/CEE e 93/22/CEE, che peraltro fornirono al legislatore italiano l'occasione di un primo complessivo riordino della materia, attuato in particolare con il D.lgs. 24 febbraio 1996 n. 58, testo unico in materia di intermediazione finanziaria e dei mercati (di seguito: t.u.f.).

A dieci anni di distanza vennero poi approvate le direttive MAD I[140] e MiFID I[141]. Benché nella prassi dei mercati, anche nei primi anni duemila, fosse già diffuso il ricorso a sistemi di negoziazione algoritmica, né MiFID I, né MAD I contenevano alcun riferimento a questi strumenti di *trading*. Per questa ragione, l'ESMA elaborò, nel 2012, le Linee Guida "Systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities"[142], con l'obiettivo di dare applicazione coerente e uniforme anche in questo ambito delle disposizioni della MiFID I e della MAD I. Il testo aveva come destinatarie le piattaforme di *trading* e le imprese di investimento che usavano sistemi di negoziazione automatizzata, nonché le piattaforme di negoziazione e le imprese di investimento che offrivano servizi di *direct market access* (DMA) o *sponsored access* (SA). Anticipando l'entrata in vigore di MiFID II, le Linee Guida ESMA del 2012 fornirono per la prima volta una definizione di *trading* algoritmico[143] e stabilirono una serie di indicazioni specifiche relative al monitoraggio dell'attività, alla prevenzione delle interruzioni di mercato, ai controlli a cui sottoporre gli algoritmi, alle salvaguardie necessarie a garantire equità e ordine nel *trading*, nonché specifici obblighi di conservazione dei registri e gestione dei rischi connessi a questo tipo di attività.

---

l'articolo 1(1) forniva una definizione di informazioni privilegiate che è diventata la base per ulteriori sviluppi, fino alle disposizioni attuali contenute nell'articolo 7 del MAR. la quale aveva lo scopo di fornire un primo quadro europeo.

[140] Direttiva 2003/6/CE del Parlamento europeo e del Consiglio del 28 gennaio 2003 relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato (abusi di mercato), a cui l'Italia ha dato attuazione con la c.d. legge comunitaria 2004 (l. 18 aprile 2005, n. 62). Si tratta della prima norma che istituisce una disciplina organica alla materia a livello europeo, estendendosi anche alla manipolazione del mercato.

[141] Direttiva 2004/39/CE del Parlamento europeo e del Consiglio, del 21 aprile 2004, relativa ai mercati degli strumenti finanziari, che modifica le direttive 85/611/CEE e 93/6/CEE del Consiglio e la Direttiva 2000/12/CE del Parlamento europeo e del Consiglio e che abroga la Direttiva 93/22/CEE del Consiglio. Si tratta della fonte che ha disciplinato dal 31 gennaio 2007 al 2 gennaio 2018 i mercati finanziari dell'Unione europea. Recepita in Italia dal D.lgs. 17 luglio 2009 n. 101.

[142] Oggi abrogate, ma in vigore fino al 2018. Il testo è disponibile al seguente link: https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_2012_122_en.pdf

[143] Testualmente: "computer software operating on the basis of key parameters set by an investment firm or a client of an investment firm that generates orders to be submitted to trading platforms automatically in response to market information".

È interessante notare come, già in quella sede, l'ESMA sottolineasse il rischio che i sistemi di trading automatizzato venissero usati per porre in essere condotte abusive, fra cui: *ping orders*[144], *quote stuffing*[145], *momentum ignition*[146] e infine *layering and spoofing*[147], pratiche che verranno riprese dal legislatore europeo a più di un decennio di distanza.

Fu infatti solo con le direttive MAD II e MiFID II e il Regolamento MAR del 2014, che – tra l'altro – si diede finalmente atto del progresso tecnologico raggiunto dai mercati, disciplinando in modo specifico anche l'uso degli algoritmi di *trading* e le conseguenze penalistiche dell'abuso di tali strumenti.

2.1. La Direttiva MAD II

L'entrata in vigore, nel 2014, della seconda Direttiva MAD[148] – c.d. MAD II (così d'ora innanzi) –, che introduce regole comuni per gli Stati membri in materia di sanzioni penali contro l'abuso di informazioni privilegiate e la manipolazione del mercato, rappresenta un punto di svolta nella disciplina della responsabilità penale per le condotte *latu sensu* abusive[149].

---

[144]Guideline n. 5: "entering small orders in order to ascertain the level of hidden orders and particularly used to assess what is resting on a dark platform".

[145]Guideline n. 5: "entering large numbers of orders and/or cancellations/updates to orders so as to create uncertainty for other participants, slowing down their process and to camouflage their own strategy".

[146]Guideline n.5: "entry of orders or a series of orders intended to start or exacerbate a trend, and to encourage other participants to accelerate or extend the trend in order to create an opportunity to unwind/open a position at a favorable price".

[147] Guideline n. 5: "submitting multiple orders often away from the touch on one side of the order book with the intention of executing a trade on the other side of the order book. Once that trade has taken place, the manipulative orders will be removed".

[148] Direttiva 2014/57/UE del Parlamento europeo e del Consiglio del 16 aprile 2014 relativa alle sanzioni penali in caso di abusi di mercato (Direttiva abusi di mercato), recepita in Italia dal D.lgs. 10 agosto 2018 n. 107. La Direttiva si evidenzia per una scelta netta in favore della sanzione penale come strumento essenziale di contrasto agli abusi di mercato, cfr. F. MUCCIARELLI, *La nuova disciplina eurounitaria sul market abuse: tra obblighi di criminalizzazione e* ne bis in idem, in Dir. Pen. Cont. Riv. Trim., 2015, fasc. 4, pp. 295–324.

[149] Si legge nel Considerando 14: "la presente Direttiva dovrebbe obbligare gli Stati membri a prevedere, nei rispettivi ordinamenti nazionali, sanzioni penali per l'abuso di informazioni privilegiate, la manipolazione di mercato e la comunicazione illecita di informazioni privilegiate cui la presente Direttiva si applica. […]". Il legislatore europeo ritiene inoltre opportuno, se del caso e qualora il diritto nazionale preveda la responsabilità penale delle persone giuridiche, che gli Stati membri estendano alle persone giuridiche la responsabilità in relazione ai reati previsti nella Direttiva medesima, attraverso l'irrogazione di sanzioni penali o non penali o altre misure che siano effettive, proporzionate e dissuasive. Quando al regime del doppio binario, nel considerando 22 si afferma: "gli obblighi previsti nella presente Direttiva di prevedere negli

La crisi finanziaria e lo scandalo del Libor avevano dimostrato l'impatto che episodi di gravi forme di *market abuse* possono avere non solo sulla fiducia nei mercati, ma anche in termini di perdite finanziarie per gli investitori. Di qui l'esigenza del legislatore europeo di approvare norme minime comuni che prevedessero anche sanzioni penali per le condotte più gravi e che dimostrassero una forma più forte di disapprovazione sociale rispetto alle sanzioni amministrative[150]. L'esigenza di fornire strumenti di contrasto agli abusi di mercato più efficaci nasceva dal fatto che, in vigore della disciplina precedente, non tutti gli Stati membri avevano adottato sanzioni amministrative (con conseguenti rischi di arbitraggio normativo) e dal fatto che anche negli Stati in cui tali sanzioni erano previste, si erano dimostrate insufficienti a prevenire e contrastare gli abusi di mercato.

Per questo motivo, la Direttiva MAD II prevede espressamente che gli Stati membri adottino sanzioni penali effettive, proporzionate e dissuasive – anche di natura detentiva almeno nei casi di illeciti gravi commessi con dolo – per i reati di abuso di informazioni privilegiate, comunicazione illecita di informazioni privilegiate e manipolazione del mercato (artt. 3 – 6)[151] siano esse commesse da persone fisiche o vantaggio o nell'interesse di persone giuridiche.

Come noto, nella prospettiva della MAD II, si distingue fra diverse ipotesi di abuso di informazioni privilegiate.

La prima – art. 3, parr. 2 e 3 – consiste nell'abuso di informazioni privilegiate "in senso stretto". Può essere commessa da chiunque possiede informazioni

---

ordinamenti nazionali pene per le persone fisiche e sanzioni per le persone giuridiche non esonerano gli Stati membri dall'obbligo di contemplare in tali ordinamenti nazionali sanzioni amministrative e altre misure per le violazioni previste nel regolamento (UE) n. 596/2014".

[150] Cfr. F. MUCCIARELLI, *La nuova disciplina eurounitaria*, 2015, *op. cit.*, p. 296.

[151] L'articolo 3 della Direttiva prevede che gli Stati Membri debbano adottare le misure necessarie affinché l'abuso di informazioni privilegiate, la raccomandazione o l'induzione di altri alla commissione di un abuso di informazioni privilegiate, costituiscano reati, almeno nei casi gravi e allorquando siano commessi con dolo. Mentre, articoli 4 e 5, rispettivamente per le condotte di comunicazione illecita di informazioni privilegiate e di manipolazione del mercato, impone l'adozione di sanzioni penali nei casi gravi e se commesse con dolo.

Il requisito del dolo non è comunque vincolante, tenuto conto del fatto che il Considerando 21 della Direttiva lascia agli Stati membri la possibilità di stabilire la rilevanza penale delle condotte di manipolazione anche se commesse con colpa grave o negligenza. Come nota F. MUCCIARELLI, *La nuova disciplina eurounitaria*, 2015 *op. cit.*, p. 314 la clausola della gravità del caso e realizzazione della condotta con dolo "segna il limite inferiore della risposta sanzionatoria pretesa dal legislatore eurounitario, ciò che lascia piena facoltà di prevedere (o di mantenere, se già contemplate) ipotesi d'illecito punite con sanzioni (anche) detentive per fattispecie non connotate dai requisiti (selettivi) minimali richiesti dalla Direttiva stessa (e dal Regolamento), ovvero con sanzioni penali più gravi".

privilegiate “in quanto membro di organi amministrativi, di direzione o di controllo dell’emittente o del partecipante al marcato delle quote di emissioni” (par. 3, lett. a), “in ragione della sua partecipazione al capitale dell’emittente o del partecipante al mercato delle quote di emissioni” (par. 3, lett. b), “in quanto avente accesso a tali informazioni nell’esercizio di un’attività lavorativa, di una professione ovvero di una funzione o ufficio” (par. 3, lett. c), “in ragione del suo coinvolgimento in attività delittuose” (par. 3, lett. d) ovvero, infine, “chiunque abbia ottenuto informazioni privilegiate anche in ragione di circostanze diverse” da quelle elencate e sia a conoscenza del carattere privilegiato delle informazioni (par. 4). La condotta rilevante consiste nell’utilizzo di informazioni acquisendo o cedendo, per conto proprio o per conto di terzi, direttamente o indirettamente, gli strumenti finanziari cui tali informazioni si riferiscono”.

La seconda ipotesi è quella di raccomandazione o induzione a commettere un abuso di informazioni privilegiate; ossia, appunto la raccomandazione o l’induzione, sulla base delle informazioni, fatta ad altri di acquisire o cedere strumenti finanziari cui le informazioni si riferiscono ovvero di annullare o modificare un ordine concernente uno strumento finanziario cui le informazioni si riferiscono; sempreché la persona che sfrutta la raccomandazione o l’induzione sia a conoscenza del fatto che queste si basano su informazioni privilegiate. Nella prospettiva del legislatore europeo, costituisce illecito anche la condotta di chi, essendo in possesso di informazioni privilegiate, comunica tal informazioni al di fuori del normale esercizio di un lavoro, della professione, della funzione o dell’ufficio, ovvero al di fuori dei sondaggi di mercato ammessi.

Inoltre, la MAD II impone agli Stati membri di sanzionare la manipolazione del mercato intesa come conclusione di un’operazione, immissione di un ordine di compravendita o qualsiasi altra condotta che fornisce segnali falsi o fuorvianti relativi all’offerta o alla domanda o al prezzo di uno strumento finanziario o un contratto a pronti su merci collegato o ne fissa il prezzo a un livello anomalo o artificiale, salvo si tratti di prassi di mercato ammesse (art. 5 par. 2, lett. a)[152]. Parimenti, secondo le disposizioni della Direttiva, costituisce manipolazione di mercato la conclusione di un’operazione, l’immissione di un ordine di compravendita o il compimento di qualsiasi altra attività o condotta che, attraverso l’uso di artifizi o ogni altro tipo di inganno o espediente, incide sul

[152] La definizione di “manipolazione del mercato” contenuta nella MAD rispecchia, come si vedrà, quella del Regolamento MAR, con differenza che il testo della Direttiva impone che, per essere penalmente rilevante, il comportamento manipolatorio debba avere un effettivo effetto distorsivo sul meccanismo di incontro di domanda e offerta o sui prezzi.

prezzo di uno o più strumenti finanziari o di un contratto a pronti su merci collegato (art. 5 par. 2, lett. b). Sono infine ricondotte al medesimo divieto la manipolazione di *benchmark* (art. 5 par. 2 lett. d)[153] e la divulgazione di informazioni, attraverso i media "che forniscono segnali falsi o fuorvianti riguardo all'offerta, alla domanda o al prezzo di uno o più strumenti finanziari o di un contratto a pronti su merci collegato a un livello anomalo o artificiale, quando colui che ha divulgato le informazioni o altri ne traggono vantaggio o profitto (art. 5, par. 2 lett. c).
Tuttavia, nella Direttiva in esame, non è fatto alcun riferimento alla negoziazione algoritmica.

2.2. Il Regolamento MAR

Contestualmente all'approvazione della Direttiva MAD II è stato emanato il Regolamento sul *market abuse* (d'ora innanzi MAR)[154].
Il Regolamento MAR individua l'integrità dei mercati finanziari nell'Unione, la protezione degli investitori e la fiducia nei mercati quale principale obiettivo di tutela[155], nell'idea che il corretto funzionamento dei mercati e la fiducia in essi siano prerequisiti per la crescita economica e la ricchezza dell'Unione stessa [156].
In questo contesto, gli abusi di mercato sono considerati come principali fonti di danno per l'integrità dei mercati finanziari. Dunque, i divieti di manipolazione di mercato, abuso di informazioni privilegiate e divulgazione illecita di informazioni privilegiate mirano a garantire l'integrità del mercato e a proteggere la fiducia degli investitori, mentre il dovere di divulgare informazioni privilegiate mira a sostenere l'efficienza informativa dei mercati e (anche) a prevenire il reato di *insider trading*[157]. Si presume infatti che le asimmetrie informative e i

[153] Ossia la trasmissione di informazioni false o fuorvianti, o comunicazioni di dati falsi o fuorvianti ovvero qualsiasi altra condotta che manipola il calcolo di un indice di riferimento.

[154] Regolamento 596/2014 del Parlamento europeo e del Consiglio del 16 aprile 2014 relativo agli abusi di mercato (regolamento sugli abusi di mercato) e che abroga la Direttiva 2003/6/CE del Parlamento europeo e del Consiglio e le direttive 2003/124/CE, 2003/125/CE e 2004/72/CE della Commissione.

[155] Art. 1 Regolamento 596/2014.

[156] Considerando 1 e 2 del Regolamento, per i quali "un autentico mercato interno dei servizi finanziari è di importanza fondamentale per la crescita economica e la creazione di posti di lavoro nell'Unione" e "un mercato finanziario integrato, efficiente e trasparente non può esistere senza che se ne tuteli l'integrità. Il regolare funzionamento dei mercati mobiliari e la fiducia del pubblico nei mercati costituiscono fattori essenziali di crescita e di benessere economico. Gli abusi di mercato ledono l'integrità dei mercati finanziari e compromettono la fiducia del pubblico nei valori mobiliari e negli strumenti derivati".

[157] In questo senso, F. ANNUNZIATA, *Artificial Intelligence*, *op. cit*., p. 10.

comportamenti abusivi scoraggino la volontà degli investitori di operare, e pregiudichino la capacità dei mercati finanziari di allocare efficientemente le risorse finanziarie a sostegno dell'economia reale[158]. Di tali fattispecie e degli altri elementi fondamentali per la disciplina degli abusi di mercato il Regolamento dà una descrizione puntuale[159], che deve essere letta in combinato disposto con le previsioni della MAD II[160] e della Direttiva MiFID II[161]. Esso costituisce dunque un riferimento interpretativo essenziale in relazione alle ipotesi di illecito già previste dagli ordinamenti degli Stati membri e di quelle di nuova creazione. Si tratta di una normativa fortemente innovativa, le cui disposizioni sono rimaste sostanzialmente immutate nel tempo e che, sin dalla sua approvazione pareva orientato a evitare la propria obsolescenza. Tale sforzo può, tra l'altro, dedursi dal fatto che il Regolamento prende in considerazione le modalità più innovative tramite le quali si possono compiere condotte abusive.

Il testo del Regolamento fa espressamente riferimento al fatto che la negoziazione di strumenti finanziari è sempre più automatizzata e pone l'accento in particolare sul fatto che le strategie abusive possono essere effettuate con qualsiasi strumento di negoziazione, incluse le negoziazioni algoritmiche e quelle ad alta frequenza[162]. All'art. 12, par. 2, lett. c.) il Regolamento MAR[163], con un espresso riferimento al *trading* algoritmico, include fra le condotte che possono essere considerate manipolazione del mercato[164] anche "l'inoltro di ordini in una sede di negoziazione, comprese le relative cancellazioni o modifiche, con ogni

---

[158] F. ANNUNZIATA, *Artificial Intelligence*, *op. cit.*, p. 10 sottolinea però che l'integrità del mercato e la fiducia degli investitori forniscono solo una panoramica parziale della logica alla base del MAR. È infatti anche la ricerca di un altro obiettivo fondamentale, ovvero l'efficienza del mercato, che sta al centro delle sue nozioni e delle disposizioni più importanti. Tale concezione trova le sue più influenti teorizzazioni nella *Efficient Capital Market Hypothesis* (ECMH).

[159] Si pensi ad esempio all'art. 3 del Regolamento, oltre che alla definizione di informazione privilegiata di cui all'art. 7, di condotte legittime e delle c.d. prassi ammesse (artt. 9 e 13).

[160] Cfr. Considerando 17: "la presente Direttiva dovrebbe essere applicata tenendo conto del quadro normativo stabilito dal regolamento (UE) n. 596/2014 e delle relative misure applicate":

[161] Come si vedrà *infra,* il raccordo fra MiFID II e MAR è quantomeno opportuno, se si considera la precisione delle disposizioni della Direttiva MiFID II in relazione al ruolo degli intermediari e delle piattaforme di *trading* e alle specifiche nome in esso contenuto sui rischi associati all'uso di algoritmi di *trading* e all'*hft*.

[162] Si fa riferimento al Considerando 38 e all'art. 12 del Mar.

[163] Regolamento 2014/596/UE.

[164] Ai sensi dell'art. 12. par. 1 lett. a) e b).

mezzo disponibile di negoziazione, anche attraverso mezzi elettronici, come le strategie di negoziazione algoritmiche e ad alta frequenza"[165].

Lo stesso riferimento ai sistemi algoritmici non è invece contenuto nelle previsioni in materia di abuso di informazioni privilegiate.

Ciò posto, benché né il MAR (né il suo Allegato I)[166], né il Regolamento delegato 522/2016[167] siano stati redatti con un *focus* specifico sulla negoziazione algoritmica, molti dei comportamenti abusivi (o degli indicatori di manipolazione

---

[165] Art. 12 par. 2 lett c): "le seguenti condotte sono considerate, tra le altre, manipolazione del mercato: […] c) 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 gestori individuare gli ordini autentici sul sistema di negoziazione della sede di negoziazione, o è probabile che lo faccia, anche emettendo 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 emettendo ordini per avviare o intensificare una tendenza".

Gli effetti di cui al paragrafo 1, lettere a) o b) sono, testualmente:

"a) l'avvio 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 altro prodotto oggetto d'asta sulla base di quote di emissione; oppure

ii. consenta, o è probabile che consenta, di fissare 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;

[…]

b) l'avvio 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"

[166]Cfr. Regolamento Ue n. 596/2014, Allegato I Sezione A ("Indicatori di manipolazioni consistenti nel fornire indicazioni false o fuorvianti o fissare i prezzi") e Sezione B ("Indicatori di manipolazioni consistenti nell'utilizzazione di strumenti fittizi o di altri tipi di inganno o espediente").

[167]Cfr. Regolamento delegato (UE) 2016/522 della Commissione del 17 dicembre 2015 che integra il regolamento (UE) del Parlamento europeo e del Consiglio (UE) n.596/2014 per quando riguarda gli indicatori di manipolazioni del mercato *et. al.*, Allegato II "Indicatori di manipolazioni", Sezione 1 ("Indicatori di manipolazioni consistenti nel fornire indicazioni false o fuorvianti e nel fissare i prezzi [Allegato I, Sezione A, del Regolamento (UE) n.596/2014]") e Sezione 2 ("Indicatori di manipolazioni consistenti nell'utilizzazione di strumenti fittizi o di altri tipi di inganno o espediente [Allegato I, Sezione B, del Regolamento (UE) n.596/2014]").

di mercato) ivi descritti possono essere supportati e agevolati dall'uso di algoritmi, specialmente quando impiegati in modo intensivo come nell'*hft*. Si tratta infatti di condotte caratterizzate dalla presenza di artifici relativi alle modalità o alle tempistiche di esecuzione, in grado di trasmettere indicazioni false o fraudolente in merito all'offerta, alla domanda o al prezzo degli strumenti finanziari.
Fra le diverse disposizioni del testo in esame, meritano in particolare un'analisi gli "indicatori di manipolazioni consistenti nel fornire indicazioni false o fuorvianti e nel fissare i prezzi"[168] e gli "indicatori di manipolazioni consistenti nell'utilizzazione di strumenti fittizi o di altri tipi di inganno o espediente"[169]. Si può affermare infatti che, fra le operazioni che il legislatore eurounitario considera "sospette", benché non espressamente menzionati, molte possano essere commesse – o perfino agevolate – dall'uso di algoritmi di *trading*[170].

Per quanto riguarda gli "indicatori di manipolazioni consistenti nel fornire indicazioni false o fuorvianti e nel fissare i prezzi", il primo indicatore ha come oggetto gli ordini di compravendita che rappresentano una quota significativa del volume giornaliero degli scambi in un dato titolo, in particolare quando tali operazioni determinano una significativa variazione di prezzi[171]. Nella prassi, ciò

---

[168] Regolamento Ue n.596/2014, Allegato I Sezione A in combinato disposto con Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1. Un esplicito rinvio all'Allegato I del Regolamento MAR è fatto, nell'ordinamento italiano, dall'art. 74 del Regolamento Mercati (Adottato con dalla Consob con delibera n. 20249 del 28 dicembre 2017 e successivamente modificato con delibere n. 21028 del 3 settembre 2019, n. 21339 del 29 aprile 2020, n. 21536 del 15 ottobre 2020 e n. 21624 del 10 dicembre 2020 e n. 22804 del 6 settembre 2023), rubricato "Elementi e circostanze da valutare per l'identificazione di manipolazioni del mercato".

[169] Regolamento Ue n.596/2014, Allegato I Sezione B in combinato disposto con Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 2.

[170] Cfr. Considerando 6 Regolamento delegato (UE) 2016/522 "[…] Tali indicatori non dovrebbero essere considerati né esaustivi né determinanti e i loro rapporti con uno o più esempi di prassi non dovrebbero essere considerati limitativi. Gli esempi di prassi non dovrebbero essere considerati di per sé una manipolazione del mercato; tuttavia, i partecipanti al mercato e le autorità competenti dovrebbero tenerne conto quando esaminano le operazioni o gli ordini di compravendita" e Considerando 8: "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 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".

[171] Regolamento Ue n.596/2014, Allegato I Sezione A, lett. a).

si riscontra in varie occasioni. Innanzitutto, in caso di *ping orders*[172] e *phising*[173]. In secondo luogo, quando avvengono acquisite, anche da parte di soggetti collusi fra loro, posizioni di un titolo sul mercato secondario dopo la collocazione sul mercato primario, al fine di fisare il prezzo e generare quindi interesse negli investitori[174]. Sono indicatori aggiuntivi della natura manipolatoria di tale prassi: "l'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 ovvero le operazioni o ordini di compravendita senza altra giustificazione apparente se non quella di aumentare il prezzo o il volume delle negoziazioni, in particolare in prossimità di un punto di riferimento durante la giornata di negoziazione"[175]. In terzo luogo, si segnala la natura potenzialmente manipolatoria della prassi della creazione di un valore minimo o un valore massimo nell'andamento dei prezzi[176]. Anche in questo caso ci sono indicatori aggiuntivi della potenzialità abusiva del comportamento. Fra questi, la circostanza che tali operazioni possano avere l'effetto di aumentare o diminuire o mantenere il prezzo nei giorni precedenti l'emissione; il riscatto volontario o la scadenza di uno strumento derivato o convertibile collegato, che possano avere l'effetto di aumentare o diminuire il prezzo medio ponderato del giorno o di un periodo nel corso della sessione di negoziazione, che mantengano il prezzo al di sotto o al di sopra di un prezzo di esercizio (o di un altro elemento utilizzato per calcolare il valore di rimborso di uno strumento derivato collegato alla data di scadenza) ovvero modifichino il prezzo in modo tale che superi o non raggiunga

[172] Inserire piccoli ordini di compravendita per accertare il livello degli ordini nascosti e, in particolare, per valutare ciò che è collocato su una *dark pool*.

[173] Eseguire ordini di compravendita o una serie di tali ordini per scoprire gli ordini di altri partecipanti e successivamente inserire un ordine di compravendita per trarre vantaggio dalle informazioni ottenute.

[174] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, lett. a) che specifica che si tratta di una "prassi generalmente nota, ad esempio nel contesto azionario, come collusione nel dopo borsa di un'offerta pubblica iniziale (OPI) in cui sono coinvolti soggetti collusi".

[175] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 1, lett. a), punti i) e ii).

[176] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 1 lett. b), si tratta di operazioni effettuate in modo tale da impedire che i prezzi degli strumenti finanziari, contratto a pronti su merci collegato o prodotti oggetto d'asta sulla base di quote di emissioni scendano o superino un certo livello di prezzo al fine di evitare conseguenze negative derivanti da variazioni di prezzo degli stessi.

tale prezzo di esercizio e ovvero infine che modifichino il prezzo di regolamento di un titolo qualora tale prezzo sia utilizzato come riferimento[177].

Un secondo indicatore evidenziato dall'Allegato I del Regolamento MAR è la misura in cui ordini di compravendita inoltrati o operazioni avviate da persone con un'importante posizione di acquisto o vendita in un titolo, ne determinano significative variazioni di prezzo[178]. Nella prassi, tali operazioni potenzialmente abusive possono declinarsi, oltre che nelle modalità già descritte con riferimento al primo indicatore, anche in caso di *abusive squeeze*[179], manipolazione tra sedi

[177] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 1 lett. b), "[…] i) operazioni o ordini di compravendita che hanno o è probabile che abbiano l'effetto di aumentare o diminuire o mantenere il prezzo nei giorni precedenti l'emissione, il riscatto volontario o la scadenza di uno strumento derivato o convertibile collegato; ii) operazioni o ordini di compravendita che hanno o è probabile che abbiano l'effetto di aumentare o diminuire il prezzo medio ponderato del giorno o di un periodo nel corso della sessione di negoziazione; iii) operazioni o ordini di compravendita che hanno o è probabile che abbiano l'effetto di mantenere il prezzo di uno strumento finanziario, un contratto a pronti su merci collegato o un prodotto oggetto d'asta sulla base di quote di emissioni sottostanti al di sotto o al di sopra di un prezzo di esercizio o di un altro elemento utilizzato per calcolare il valore di rimborso (ad esempio la barriera) di uno strumento derivato collegato alla data di scadenza; iv) operazioni effettuate in qualsiasi sede di negoziazione che hanno o è probabile che abbiano l'effetto di modificare il prezzo dello strumento finanziario, del contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni sottostanti in modo tale che il prezzo superi o non raggiunga il prezzo di esercizio o un altro elemento utilizzato per calcolare il valore di rimborso (ad esempio la barriera) di uno strumento derivato collegato alla data di scadenza; v) operazioni che hanno o è probabile che abbiano l'effetto di modificare il prezzo di regolamento di uno strumento finanziario, un contratto a pronti su merci collegato o un prodotto oggetto d'asta sulla base di quote di emissioni qualora tale prezzo sia utilizzato come riferimento o sia determinante in particolare per il calcolo dei requisiti in materia di margini"

[178] Regolamento Ue n.596/2014, Allegato I Sezione A, par. 1, lett. b).

[179] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 2, lett. b), "trarre vantaggio dall'influenza significativa di una posizione dominante sull'offerta o la domanda di meccanismi di consegna di uno strumento finanziario, un contratto a pronti su merci collegato o un prodotto oggetto d'asta sulla base di quote di emissioni per creare o rendere probabile una distorsione sostanziale dei prezzi ai quali altri soggetti devono consegnare, prendere in consegna o rinviare la consegna al fine di adempiere i propri obblighi":

di negoziazione diverse (*inter-trading venues manipulation*)[180] e manipolazione tra prodotti diversi (*cross-product manipulation*)[181].

Terzo indicatore di manipolazioni consistenti nel fornire indicazioni false o fuorvianti e nel fissare i prezzi è rappresentato dalle operazioni che non portano a modificare la reale titolarità economica di uno strumento finanziario, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di

[180] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 2, lett. c): "effettuare negoziazioni o inserire ordini di compravendita in una sede di negoziazione o al di fuori di una sede di negoziazione allo scopo di influenzare scorrettamente il prezzo dello stesso strumento finanziario in un'altra sede di negoziazione o al di fuori di una sede di negoziazione, di un contratto a contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni". Sono indicatori aggiuntivi di manipolazione, relativi a tale prassi: "effettuare un'operazione, modificando i prezzi di acquisto e di vendita, quando il differenziale tra questi due prezzi è fattore di calcolo del prezzo di una qualsiasi altra operazione, sia essa effettuata nella stessa sede di negoziazione o in altre sedi" e gli indicatori di cui alla sezione 1, par. 1, lett b).

[181] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 2, lett. d): "effettuare negoziazioni o inserire ordini di compravendita in una sede di negoziazione o al di fuori di una sede di negoziazione allo scopo di influenzare scorrettamente il prezzo di uno strumento finanziario collegato in un'altra sede o nella stessa sede di negoziazione o al di fuori di una sede di negoziazione, di un contratto a contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni collegato. Questa prassi può essere illustrata anche dagli indicatori aggiuntivi di manipolazioni del mercato di cui alla presente sezione, paragrafo 1, lettera b), punti i), iii), iv) e v), e paragrafo 2, lettera c), punto i)".

quote di emissioni[182]. Si tratta delle operazioni di *wash trade*[183], *painting the tape*[184], *improper matched orders*[185] e *concealing ownership*[186].

Il quarto indicatore è la misura in cui gli ordini – che rappresentano una quota significativa del volume giornaliero degli scambi – prevedono inversioni di posizione nel breve periodo e possono essere associati a significative variazioni di prezzo degli strumenti finanziari, dei contratti a pronti su merci collegato o di prodotti oggetto d'asta sulla base di quote di emissioni[187]. Si riferiscono a questo

---

[182] Regolamento Ue n.596/2014, Allegato I Sezione A, par. 1, lett. c).

[183] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 3, lett. a): "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. […] 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; iii) l'indicatore di cui alla presente sezione, paragrafo 1, lettera a), punto i)".

[184] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 3, lett. b): "aderire a ordini di compravendita o partecipare a un'operazione o una serie di operazioni riportate su dispositivi di visualizzazione pubblica al fine di creare, su un determinato strumento finanziario, un contratto a pronti su merci collegato o un prodotto oggetto d'asta sulla base di quote di emissioni, l'apparenza di attività o di movimento del relativo prezzo […]. Questa prassi può essere illustrata anche dagli indicatori di cui alla presente sezione, paragrafo 1, lettera a), punto i), e paragrafo 3, lettera a), punto i)".

[185] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 3, lett. c): "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 […]. 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), e paragrafo 3, lettera a), punti i) e ii)".

[186] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 3, lett. d): "un'operazione o una serie di operazioni progettate per celare la proprietà di uno strumento finanziario, un contratto a pronti su merci collegato o un prodotto oggetto d'asta sulla base di quote di emissioni violando gli obblighi di comunicazione attraverso il possesso dello strumento finanziario, del contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni a nome di uno o più soggetti in collusione tra loro. Le comunicazioni sono fuorvianti per quanto riguarda il reale possessore sottostante dello strumento finanziario, del contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni […]. Questa prassi può essere illustrata anche dall'indicatore di cui alla presente sezione, paragrafo 3, lettera a), punto i)".

[187] Regolamento Ue n.596/2014, Allegato I Sezione A, par. 1, lett. d).

indicatore le prassi di *painting the tape*, *improper matched orders*, *pump and dump*[188], *trash and cash*[189], *quote stuffing*[190] e *momentum ignition*[191].
Il quinto indicatore attiene alla concentrazione, in un breve lasso di tempo nel corso della sessione di negoziazione, di ordini di compravendita e operazioni che determinano una variazione del prezzo che successivamente si inverte. A questi elementi si possono ricondurre prassi come quella della creazione di un valore minimo o massimo nell'andamento del prezzo, della *inter-trading venues*

[188] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 4, lett. c): "assumere una posizione *long* (lunga) in uno strumento finanziario, un contratto a pronti su merci collegato o un prodotto oggetto d'asta sulla base di quote di emissioni e poi effettuare ulteriori attività di acquisto e/o diffondere informazioni positive fuorvianti relative allo strumento finanziario, al contratto a pronti su merci collegato o a un prodotto oggetto d'asta sulla base di quote di emissioni allo scopo di aumentarne il prezzo attirando altri acquirenti. Quando il prezzo è a un livello artificialmente elevato, la posizione long detenuta è liquidata".

[189] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 4, lett. d): "assumere una posizione *short* (corta) in uno strumento finanziario, un contratto a pronti su merci collegato o un prodotto oggetto d'asta sulla base di quote di emissioni e poi effettuare ulteriori attività di vendita e/o diffondere informazioni negative fuorvianti relative allo strumento finanziario, al contratto a pronti su merci collegato o a un prodotto oggetto d'asta sulla base di quote di emissioni allo scopo di abbassarne il prezzo attirando altri venditori. Quando il prezzo è sceso, la posizione detenuta viene chiusa".

[190] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 4, lett. e): "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".

[191] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 4, lett. f): "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 […]. Questa prassi può essere illustrata anche dall'alto tasso di ordini cancellati (ad esempio coefficiente ordini-negoziazioni), che può essere associato a un tasso relativo al volume (ad esempio numero di strumenti finanziari per ordine)".

manipulation e *cross-product manipulation*, *marking the close*[192], nonché *layering and spoofing*[193], *quote stuffing* e *momentum ignition*.

Il sesto indicatore è la modifica della rappresentazione dei migliori prezzi delle proposte in denaro o lettera dei titoli o più in generale la rappresentazione del *book* di negoziazione a disposizione dei partecipanti al mercato e la revoca prima dell'esecuzione. Si rifanno a questo indicatore l'inserimento di ordini senza avere l'intenzione di eseguirli (*placing orders with no intention of exectuing them*)[194], la creazione di un valore minimo o massimo nell'andamento del prezzo, la creazione di differenziali eccessivi fra il prezzo di acquisto e il prezzo di

[192] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 5, lett. d): "acquistare o vendere uno strumento finanziario, un contratto a pronti su merci collegato o un prodotto oggetto d'asta sulla base di quote di emissioni deliberatamente nel momento di riferimento della sessione di contrattazione (ad esempio al momento dell'apertura, della chiusura, del regolamento) nell'intento di aumentare, diminuire o mantenere il prezzo di riferimento (ad esempio prezzo di apertura, prezzo di chiusura, prezzo di regolamento) a un determinato livello […] Questa prassi può essere illustrata anche dai seguenti indicatori aggiuntivi di manipolazioni del mercato: i) inserimento di ordini che rappresentano volumi significativi del book di negoziazione (*order book*) centrale del sistema di negoziazione pochi minuti prima della fase di determinazione del prezzo dell'asta e cancellazione di tali ordini pochi secondi prima che il book di negoziazione sia congelato per calcolare il prezzo d'asta, cosicché il prezzo teorico di apertura potrebbe sembrare più alto/basso di quanto sarebbe altrimenti; ii) gli indicatori di cui alla presente sezione, paragrafo 1, lettera b), punti i), iii), iv) e v); iii) esecuzione di operazioni o presentazione di ordini di negoziazione in particolare in prossimità di un punto di riferimento durante la giornata di negoziazione che, per le loro dimensioni rispetto al mercato, hanno chiaramente un impatto significativo sull'offerta o sulla domanda oppure sul prezzo o sul valore; iv) operazioni o ordini di compravendita senza altra giustificazione apparente se non quella di aumentare/ diminuire il prezzo o di aumentare il volume delle negoziazioni, in particolare in prossimità di un punto di riferimento durante la giornata di negoziazione, ad esempio in apertura o verso la chiusura".

[193] Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 5, lett. e): "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. […] Questa prassi può essere illustrata anche dall'indicatore citato al paragrafo 4, lettera f), punto i);"

[194] Indicatori aggiuntivi: "i) ordini di compravendita inseriti a un prezzo tale che aumentano la domanda o diminuiscono l'offerta e hanno o è probabile che abbiano l'effetto di aumentare o diminuire il prezzo di uno strumento finanziario collegato; ii) l'indicatore di cui alla presente sezione, paragrafo 4, lettera f), punto i)". Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 6, lett. a).

vendita[195], l'*advancing the bid*[196], la *inter-trading venues* e *cross-product manipulation*, il *layering and spoofing*, il *quote stuffing* e *momentum ignition* e lo *smoking*[197].

Infine, l'avvio di operazioni nel momento preciso o in prossimità del momento in cui vengono calcolati i prezzi di riferimento, i prezzi di regolamento e le valutazioni, determinando variazioni nei prezzi che hanno effetti su detti prezzi e sulle valutazioni. Il *marking the close*, la collusione nel dopoborsa di un'offerta pubblica iniziale in cui sono coinvolti soggetti collusi, la creazione di un valore minimo o massimo nell'andamento del prezzo, la manipolazione tra sedi di negoziazione diverse o tra prodotti diversi e la partecipazione ad accordi per distorcere i costi associati a un contratto su merci con l'effetto di fissare un prezzo anormale o artificiale sono tipiche prassi riconducibili all'indicatore in questione.

Quanto poi alla manipolazione operativa[198], gli indicatori elencati dal Regolamento MAR sono due.

Il primo aggiunge alla dimensione operativa una componente informativa pura, poiché si sostanzia nella diffusione di informazioni false o fuorvianti precedente all'invio di ordini di compravendita o all'avvio di operazioni da parte delle stesse persone o da persone a esse collegati. Ciò può avvenire nella prassi tramite i media, internet o qualsiasi altro mezzo idoneo a provocare variazioni nel prezzo dei titoli in senso favorevole alla posizione detenuta o a un'operazione programmata ovvero aprendo una posizione e chiudendola immediatamente dopo aver comunicato pubblicamente e con grande enfasi il lungo periodo dell'investimento (*opening a position and closing it immediately afert its public*

---

[195] Ossia spostare il differenziale tra il prezzo di acquisto e il prezzo di vendita verso livelli artificiali e/o mantenerlo a tali livelli abusando del potere di mercato. "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 aggirare le misure di salvaguardia della negoziazione attuate nel mercato (ad esempio limiti di prezzo, limiti di volume, parametri per il differenziale prezzo di acquisto/prezzo di vendita ecc.); ii) l'indicatore di cui alla presente sezione, paragrafo 2, lettera c), punto i)", Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 1, par. 6, lett. c).

[196] Inserire ordini di compravendita che aumentano la domanda (o diminuiscono l'offerta) di uno strumento finanziario, un contratto a pronti su merci collegato o un prodotto oggetto d'asta sulla base di quote di emissioni, al fine di aumentarne (o diminuirne) il prezzo.

[197] Inserire ordini di compravendita per attirare altri partecipanti al mercato che utilizzano tecniche di negoziazioni tradizionali 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*.

[198] Nel linguaggio dell'Allegato I del Regolamento MAR "manipolazione consistente nell'utilizzazione di strumenti fittizi o di altri tipi di inganno o espediente".

disclosure), o ancora con condotte riconducibili al *pump and dump*, al *trash and cash*, *concealing ownership*, lo spostamento o lo stoccaggio di merci (che potrebbe creare un'apparenza fuorviante dell'offerta o la domanda, il prezzo o il valore di un prodotto in uno strumento finanziario o un contratto a pronti su merci collegato) o ancora lo spostamento di una nave da carico vuota che potrebbe creare un'apparenza falsa o fuorviante per quanto riguarda l'offerta, la domanda o il prezzo di un prodotto in uno strumento finanziario o un contratto a pronti su merci collegato[199].

Il secondo indicatore invece fa riferimento all'inoltro di ordini di compravendita o all'avvio di operazioni, prima o dopo che le stesse persone che li hanno inoltrati o avviati abbiano elaborato o diffuso raccomandazioni di investimento errate, tendenziose o manifestamente influenzate da interessi determinanti. Si ricollegano a questo indicatore le pratiche di *pump and dump*, *trash and cash*, la diffusione di informazioni false o fuorvianti tramite media, internet o qualsiasi altro mezzo che provoca (o è probabile che provochi) variazioni nel prezzo dei titoli in senso favorevole alla posizione detenuta o a un'operazione programmata, nonché l'inserimento di ordini di compravendita o esecuzione di operazioni prima o subito dopo che il partecipante al mercato (o le persone di cui sono pubblicamente noti i legami con quest'ultimo) abbia elaborato o diffuso ricerche o raccomandazioni di investimento di tenore contrario che sono resi pubblicamente disponibili.

Ebbene, come è emerso, l'elencazione delle operazioni sospette è assai dettagliata. Certamente, molte delle operazioni descritte possono essere agevolate dall'uso di algoritmi, quantomeno per la capacità di elaborazione di significative quantità di dati e di agire in modo assai più rapido rispetto al *trader* non automatizzato[200]. Anche il linguaggio usato dal legislatore europeo richiama molte delle espressioni che ricorrono in letteratura con riferimento alle strategie poste in essere dagli algoritmi di *trading*. Si tratta dunque di un'ulteriore conferma dello sforzo operato dal legislatore europeo per adeguare le norme alla realtà dei

---

[199] Regolamento Ue n.596/2014, Allegato I Sezione B in combinato disposto con Regolamento delegato (UE) 2016/522, Allegato II "Indicatori di manipolazioni", Sezione 2, par. 1.

[200] Ciononostante, come rileva A. AZZUTTI, *AI-driven Market Manipulation*, 2022, *op. cit*, par. 3.1 i contorni effettivi della manipolazione del mercato descritta nel MAR non appaiono definiti in modo chiaro, ciò comporta il rischio di consegnare ai mercati una previsione incerta, soprattutto con riferimento ad alcune forme di manipolazione algoritmica. Inoltre, l'autore rileva che, complessivamente, l'assenza di qualsiasi riferimento a elementi soggettivi combinata con una formulazione piuttosto vaga dell'elemento oggettivo potrebbe compromettere la prevedibilità della norma e creare incertezza giuridica, specie con riferimento ai *trader* algoritmici.

mercati e ai rischi che il ricorso a forme così avanzate di tecnologia può comportare in termini di abusi di mercato. Tale sforzo è particolarmente apprezzabile se si considera che prima dell'entrata in vigore di MAR e MAD II nessuna disposizione si era occupata di regolare in modo puntuale la responsabilità penale per le condotte abusive poste in essere sfruttando gli algoritmi di *trading*. In questo senso, è la Direttiva MiFID II[201] a segnare la definitiva presa d'atto della rilevanza del fenomeno, considerata la profonda evoluzione che ha interessato le tecniche di negoziazione dell'ultimo ventennio, l'ampio utilizzo di questa da parte dei partecipanti al mercato[202] e i noti *flash crash*.

2.3. La Direttiva MiFID II

La Direttiva "relativa ai mercati degli strumenti finanziari" (d'ora innanzi MIDIF II)[203] disciplina la materia partendo dal presupposto che il *trading* algoritmico non è una strategia in sé (abusiva), ma che esso consiste piuttosto in un insieme di tecnologie sofisticate utilizzate per attuare strategie di negoziazione più tradizionali, il *market making* o l'arbitraggio. Forte dell'esperienza dei *flash*

[201] Direttiva 2014/65/UE del Parlamento Europeo e del Consiglio del 15 maggio 2014 relativa ai mercati degli strumenti finanziari e che modifica la Direttiva 2002/92/CE e la Direttiva 2011/61/UE.

[202] Considerando 59 della Direttiva. Come già anticipato, lo sforzo definitorio del fenomeno della negoziazione algoritmica attuato dalla Direttiva M MiFID II si spinge fino alla descrizione puntuale del *trading* ad alta frequenza (Considerando 61). Esso viene inteso come un sottoinsieme della negoziazione algoritmica in cui un sistema di negoziazione analizza dati o segnali del mercato a velocità elevata per poi inviare o aggiornare un gran numero di ordini entro un tempo brevissimo in risposta all'analisi. "In particolare, la negoziazione algoritmica ad alta frequenza può contenere elementi quali l'inizializzazione, la generazione, la trasmissione e l'esecuzione dell'ordine che sono determinati dal sistema senza intervento umano per ciascun singolo ordine o negoziazione, un tempo breve per la creazione e la liquidazione delle posizioni, un elevato indice giornaliero di rotazione del portafoglio, un elevato rapporto infragiornaliero ordini/operazioni e la chiusura del giorno di negoziazione in una posizione *flat*, o prossima a essa. La negoziazione algoritmica ad alta frequenza è caratterizzata, tra l'altro, da elevati traffici infragiornalieri di messaggi che costituiscono ordini, quotazioni o cancellazioni. Nel determinare che cosa costituisce un traffico infragiornaliero elevato di messaggi, si dovrebbe tenere conto dell'identità del cliente al quale è riconducibile l'attività in ultima analisi, della lunghezza del periodo di osservazione, della comparazione con l'attività complessiva del mercato durante tale periodo e della concentrazione o frammentazione relativa di attività". Cfr. sul punto F. ANNUNZIATA, *Artificial intelligence*, 2023, *op. cit*., pag 124.

[203] Direttiva 2014/65/UE del Parlamento europeo e del Consiglio del 15 maggio 2014 relativa ai mercati degli strumenti finanziari e che modifica la Direttiva 2002/92/CE e la Direttiva 2011/61/UE.

crash occorsi negli anni precedenti alla stesura di MiFID II[204], la scelta del legislatore europeo è dunque quella fornire regole specifiche che si applichino alla negoziazione algoritmica perché, come ogni altra forma di negoziazione, può prestarsi a talune forme di comportamento abusivo[205]. Tutto ciò, tenuta presente una delle principali caratteristiche della negoziazione algoritmica più evoluta: la capacità di determinare in modo automatico taluni aspetti di un ordine con intervento umano minimo o nullo.

Ne risulta un *corpus* di regole assai dettagliato, basato su un robusto sistema di controlli sul corretto funzionamento del *trading* algoritmico.

Tali controlli hanno l'obiettivo di prevenire i rischi potenziali connessi al ricorso alla tecnologia nell'attività di *trading* (in particolare alla negoziazione algoritmica ad alta frequenza), come l'aumento del sovraccarico dei sistemi nelle sedi di negoziazione a causa del gran numero di ordini, la possibilità che la negoziazione algoritmica generi ordini erronei o doppi o che comunque non funzioni correttamente e crei così un mercato disordinato[206], oltre al rischio che i sistemi di negoziazione algoritmica reagiscano in modo eccessivo ad altri eventi di mercato, esacerbando così la volatilità qualora preesista un problema di mercato.

Lungi dall'imporre requisiti di autorizzazione specifici per operatori algoritmici, MiFID II delinea dunque un regime specifico per il *trading* automatizzato – all'interno del più ampio contesto del quadro normativo applicabile alla prestazione di servizi di investimento e alle sedi di negoziazione – che ha come obiettivo la garanzia di resilienza dei mercati e la capacità di impedire l'invio di ordini erronei e prevenire il disordine nei mercati stessi, prevedendo anche meccanismi efficaci di continuità operativa per rimediare a eventuali malfunzionamenti dei sistemi di negoziazione[207].

Tale regime – basato sull'idea della prevenzione del rischio – si compone di disposizioni che si rivolgono a destinatari diversi: le imprese di investimento

---

[204] Cfr. F. ANNUNZIATA, *Artificial intelligence*, 2023, *op. cit.* p. 124 che sottolinea come gli episodi di *flash crash* abbiano mostrato ai regolatori dell'UE che le tecniche algoritmiche devono essere, "maneggiate con cura" e richiedono particolare cautela.

[205] Cfr. F. ANNUNZIATA, *Artificial intelligence*, 2023, *op. cit.* p. 125 rende merito alla scelta di non imporre divieti o limitazioni al *trading* algoritmico di per sé, specificando che "se un tale divieto fosse stato in atto, il *trading* algoritmico e l'*hft* sarebbero comunque rimasti fenomeni globali, che le restrizioni locali non avrebbero potuto affrontare adeguatamente" (traduzione nostra).

[206] Considerando 62 della Direttiva.

[207] Art. 17, par. 1 della Direttiva MiFID II. La norma rinviava all'ESMA il dovere di elaborare progetti di norme tecniche di regolamentazione in tal senso (art. 17 par. 7).

utilizzano algoritmi[208] da un lato e le sedi di negoziazioni in cui si fa uso di sistemi di *trading* algoritmico[209] dall'altro.

Fra i vari obblighi per le imprese di investimento, vale la pena menzionare tre aspetti.

---

[208] Le imprese di investimento devono rispettare requisiti organizzativi, requisiti di trasparenza e sono destinatarie di un regime speciale se attuano strategie di *market making* (art. 17).

Più in particolare, l'impresa deve possedere sistemi efficaci e controlli sul rischio adeguati all'attività che svolge per garantire che i suoi sistemi di *trading* siano resilienti e abbiano capacità sufficienti, siano soggetti a soglie e limiti di *trading* appropriati e impediscano l'invio di ordini erronei o il funzionamento dei sistemi in modo tale da poter creare o contribuire a un mercato disordinato. Inoltre, le imprese devono essere in grado di garantire che i sistemi di *trading* non possano essere utilizzati per scopi contrari al MAR o alle regole della sede di negoziazione al quale sono collegate. Infine, l'impresa di investimento deve disporre di meccanismi di continuità operativa per affrontare qualsiasi malfunzionamento dei suoi sistemi di *trading* e deve garantire che i suoi sistemi siano regolarmente testati e monitorati correttamente per garantire che soddisfino i requisiti citati.

Il sistema dei controlli degli algoritmi è specificato nel Regolamento delegato (UE) 2017/589 della Commissione del 19 luglio 2016 e si struttura attraverso meccanismi preventivi rispetto alla messa in funzione e all'aggiornamento degli stessi – di cui all'art. 5 – che:

- consentano di evitare che gli algoritmi si comportino in modo imprevisto
- permettano agli algoritmi di operare in modo conforme agli obblighi imposti alle imprese di investimento e alle microstrutture dei mercati
- l'algoritmo non contribuisca a creare condizioni di negoziazione anormale, conitnui a funzionare efficacemente in caso di condizioni di stress del mercato e in quest'ultimo caso, se necessario, consentano la disattivazione del sistema di negoziazione algoritmica o dell'algoritmo di negoziazione)

Inoltre, il Regolamento delegato impone imposti alle imprese di investimento di: eseguire delle prove di conformità dei sistemi di negoziazione algoritmica e degli algoritmi di negoziazione (art. 6); fissare dei limiti predefiniti riguardanti il numero di strumenti finanziari negoziati, il prezzo, il valore e il numero degli ordini, le posizioni strategiche, nonché il numero di sedi di negoziazione a cui gli ordini vengono trasmessi (art. 8).

Inoltre, si impongono obblighi di gestione post installazione (artt. 9-11) che includono un processo di autovalutazione e convalida annuale, nonché degli *stress test*.

A questi si aggiungono i mezzi per assicurare la resilienza, fra i quali controlli pre-negoziazione di cui all'art. 15 riguardanti i limiti di prezzo, il valore massimo dell'ordine e del volume e la quantità massima di messaggi al *book* di negoziazione; oltre alla predisposizione di sistemi che disattivino automaticamente le esecuzioni automatiche di una strategia di negoziazione algoritmica dopo un numero predeterminato di esecuzioni ripetute. A questi si aggiungono meccanismi di continuità operativa (art. 14) e monitoraggio in tempo reale (art. 16).

Infine, l'art. 17 impone agli operatori responsabili dell'algoritmo e della funzione di controllo dei rischi dell'impresa di investimento un monitoraggio post negoziazione.

[209] Art. 48 par. 1.

Innanzitutto, il fatto che le imprese di investimento che effettuano negoziazioni algoritmiche debbano darne notifica alle autorità dello Stato membro in cui operano e alla sede di negoziazione[210].

Il secondo aspetto rilevante attiene all'organizzazione dell'impresa di investimento e al personale responsabile dei controlli sull'attività degli algoritmi[211]. L'impresa di investimento è infatti tenuta a istituire un dispositivo di *governance* chiaro e formalizzato che definisca linee di responsabilità precise, comprese le procedure di soluzione dei problemi individuati durante il monitoraggio degli algoritmi, oltre che una separazione netta fra le responsabilità operative e le funzioni di controllo del rischio per impedire che vengano occultate le attività di negoziazione non autorizzate. Si richiede inoltre che il personale preposto al controllo abbia almeno una conoscenza generale delle modalità di funzionamento dei sistemi di negoziazione algoritmica e degli algoritmi di negoziazione dell'impresa e delle relative strategie e che abbia competenze sufficienti per dare seguito alle informazioni trasmesse con allarmi automatici e "sufficiente autorità per opporsi alla persona responsabile nei casi in cui questa attività crei condizioni negoziazione anormali o faccia sorgere sospetti di abusi di mercato"[212].

Il terzo aspetto rilevante riguarda l'obbligo di adozione di sistemi di sorveglianza automatizzati per l'individuazione delle manipolazioni di mercato (basandosi sugli indicatori di manipolazione previsti dal MAR, illustrati *supra*). Tali sistemi devono essere in grado di monitorare l'intera gamma dell'attività di *trading* svolta dall'impresa di investimento e tutti gli ordini e le operazioni da questa effettuate, di generare allarmi e produrre rapporti in presenza dei segnali di potenziale manipolazione previsti dal Regolamento MAR. L'impresa di investimento deve confrontare tutte le segnalazioni di attività di negoziazione sospetta generate dal sistema automatizzato con tutte le altre attività di *trading* pertinenti svolte

---

[210] Art. 17 par. 2 MiFID II.

[211] Artt. 1-3 Regolamento delegato (UE) 2017/589.

[212] Art. 3 Regolamento delegato (UE) 2017/589. In particolare, per quanto riguarda il dovere di monitoraggio in tempo reale, è fatto obbligo, durante le ore di invio di ordini ai mercati regolamentati, di monitorare in tempo reale tutte le attività di *trading* algoritmico che avvengono sotto il codice di *trading* dell'impresa, comprese quelle dei suoi clienti, per segni di *trading* disordinato, inclusa l'attività di *trading* tra mercati, classi di *asset* o prodotti, nei casi in cui l'impresa o i suoi clienti si impegnano in tali attività. Il monitoraggio in tempo reale del *trading* algoritmico deve essere effettuato dal responsabile dell'algoritmo di *trading* o della strategia di *trading* algoritmico e dalla funzione di gestione del rischio o da una funzione di controllo del rischio indipendente stabilita per questo scopo. Tale funzione di controllo non deve essere gerarchicamente dipendente dal responsabile dell'algoritmo.

dall'impresa. Il sistema deve poi essere in grado di leggere, riprodurre e analizzare *ex post* i dati sugli ordini e sulle operazioni e "generare allarmi operabili all'inizio del successivo giorno di negoziazione o, in caso di elaborazione manuale, alla fine del successivo giorno di negoziazione"[213]. Infine, il sistema di sorveglianza dell'impresa di investimento deve essere dotato di documentazione e procedure adeguate che consentano di dare un seguito effettivo agli allarmi da esso generati.

Norme specifiche sono dedicate alla disciplina dell'attività di *market making* posta in essere dalle imprese che effettuano negoziazione algoritmica[214] e alle imprese di investimento che forniscono servizi di accesso elettronico diretto a una sede di negoziazione[215]. A questi sono imposti limiti temporali, oltre che l'obbligo di predisporre sistemi di controllo sulla propria attività.

Volgendo invece lo sguardo agli obblighi per le sedi di negoziazioni in cui si fa uso di sistemi di *trading* algoritmico – siano essi mercati regolamentati, MTF o OTF –, la Direttiva MiFID II adotta una logica orientata al rischio, da prevenire o gestire *ex post*[216].

Essa infatti impone agli Stati membri di assicurarsi che le sedi di negoziazione "dispongano di sistemi, procedure e dispositivi efficaci per garantire che i sistemi di negoziazione siano resilienti, abbiano capacità sufficiente per gestire i picchi di volume di ordini e messaggi, siano in grado di garantire negoziazioni ordinate in condizioni di mercato critiche, siano pienamente testati per garantire il rispetto di tali condizioni, siano soggetti a efficaci disposizioni in materia di continuità operativa per garantire la continuità dei servizi in caso di malfunzionamento dei

---

[213] Art. 13 Regolamento delegato (UE) 2017/589.

[214] Art. 17, par. 3, a norma del quale si ritiene che le imprese di investimento che effettuano negoziazioni algoritmiche perseguano una strategia di *market making* quando "quali membri o partecipanti in una o più sedi di negoziazione e operando per conto proprio, la loro strategia implica la trasmissione di quotazioni ferme, simultanee di acquisto e di vendita, di entità comparabile e a prezzi competitivi relative a uno o più strumenti finanziari o a diversi strumenti finanziari in un'unica sede di negoziazione o in diverse sedi di negoziazione, con il risultato di fornire liquidità in modo regolare e frequente al mercato complessivo" (traduzione ufficiale).

[215] Art. 17, par. 5.

[216] Sul punto sono rilevanti le disposizioni del Regolamento delegato (UE) 2017/584 della Commissione del 14 luglio 2016, che delinea un complesso sistema di test degli algoritmi di negoziazione a partire dalla fase precedente all'accesso alla piattaforma di negoziazione. Si ritiene infatti che testare gli algoritmi sia fondamentale per garantire il corretto funzionamento delle sedi di *trading*, riducendo il rischio di disordine nei mercati (anche individuando eventuali carenze prima dell'utilizzo). Sulla dimostrata efficacia del sistema dei test cfr. ESMA, *Mifid II review report*, 2021, *op. cit..* Sono poi previsti dei meccanismi per rallentare il flusso degli ordini (*speed bumps*). Cfr. sul punto F. ANNUNZIATA, *Artificial intelligence*, *op. cit.* pp. 136-137.

loro sistemi di negoziazione"[217]. Inoltre, le sedi di negoziazione devono essere predisposte per rifiutare gli ordini che eccedono soglie predeterminate di prezzo e volume o che sono chiaramente errati; nonché siano in grado di sospendere o limitare le negoziazioni in caso di oscillazione significativa nel prezzo di un titolo in un breve lasso di tempo (sospendendo, modificando o correggendo le transazioni, ove necessario)[218].

Rispondono alla logica di prevenzione del rischio, le norme della Direttiva che mirano scongiurare l'eventualità che i sistemi di negoziazione algoritmica possano contribuire a creare condizioni di mercato anomale o comportamenti abusivi e che conferiscono agli Stati la facoltà di autorizzare la previsione di commissioni più elevate ai partecipanti che impiegano *hft* e che presentano un elevato rapporto tra ordini annullati e ordini eseguiti[219].

Infine, la Direttiva MiFID II si occupa della vigilanza da parte delle singole autorità degli Stati membri. La Direttiva attribuisce alle autorità competenti poteri di controllo sulle imprese di investimento che effettuano negoziazioni algoritmiche, compresa la possibilità di richiedere alle imprese stesse di fornire una descrizione della natura delle strategie usate, dei meccanismi interni predisposti per impedire la violazione delle disposizioni del MAR, nonché un potere di richiedere ulteriori informazioni in qualsiasi momento[220]. Le autorità hanno poi il potere di richiedere alle imprese che ricorrono alla negoziazione algoritmica ad alta frequenza registrazioni accurate e sequenziali di tutti gli ordini collocati, compresi la cancellazione di ordini, gli ordini eseguiti e le quotazioni sulle sedi di negoziazione, che le imprese stesse hanno l'obbligo di conservare.

Nel complesso, dunque, l'approccio della Direttiva, prudentemente orientato ad affrontare i principali rischi e implicazioni del trading algoritmico, può considerarsi altamente tecnico e preciso. Lo sforzo di costruire un sistema che potesse adattarsi alle evoluzioni tecnologiche ha consentito alle norme citate di risultare adeguate e tuttora funzionanti[221], sebbene – come si vedrà – a un

---

[217] Art. 48 par. 1 MiFID II.

[218] Art. 48 parr. 4 e 5 MiFID II.

[219] Art. 48 par. 9 MiFID II.

[220] Art. 17, par 2. In questo senso anche l'obbligo di cui all'art. 48, par. 10, in base al quale i mercati regolamentati devono essere in grado di mettere a disposizione delle autorità competenti le informazioni relative agli ordini generati mediante negoziazione algoritmica, i diversi algoritmi utilizzati per la creazione degli ordini e le corrispondenti persone che avviano tali ordini.

[221] Specie se si considera il comportamento dei mercati dell'Unione Europea nel periodo di forte volatilità seguito all'epidemia di COVID-19, come sottolinea ESMA, *Mifid II rewiew review report*, 2021, *op. cit.*, par. 28. Cfr. in questo senso anche F. CONSULICH–M. MAUGERI–C. MILIA–T.N. POLI–G. TROVATORE, *AI e abusi di mercato*, *op. cit.*, p. 47.

decennio di distanza dall'entrata in vigore, si renderebbero necessarie alcune modifiche che tengano conto dell'aumentato livello sofisticatezza degli algoritmi di *trading*[222].

2.4 Gli interventi normativi più recenti: AI Act e AI Liability Act Proposal

L'occasione per tale intervento di adeguamento delle norme all'evoluzione tecnologica nei mercati finanziari avrebbe senza dubbio potuto essere l'approvazione del c.d. AI Act (o "Regolamento sull'intelligenza artificiale")[223].

---

[222] Cfr. ESMA, *Mifid II rewiew review report*, 2021, *op. cit.*, par. 29. Il rapporto fa però presente che per quanto riguarda l'identificazione di altri rischi che meriterebbero un'ulteriore attenzione regolamentare oltre a quelli presentati nella MiFID II, la maggior parte delle parti interessate non è riuscita a individuare rischi e impatti sulle strutture di mercato diversi da quelli già menzionati nella MiFID II. Piuttosto, una parte degli *stakeholder* consultati ha riferito che solo i più potenti partecipanti al mercato, al momento, riescono a tenere il passo con gli ingenti investimenti richiesti dall'attuale "corsa agli armamenti tecnologici", rilevando un rischio di riduzione della concorrenza. In questo senso anche F. CONSULICH–M. MAUGERI–C. MILIA–T.N. POLI–G. TROVATORE, *AI e abusi di mercato*, 2023, *op. cit.*, p. 57 con riferimento alla disciplina della manipolazione operativa notano come l'attuale quadro normativo "rischi (forse in modo non voluto) di supportare adeguatamente la diffusione e lo sviluppo dei sistemi di IA 'forti' nei mercati finanziari, così limitando altresì il progresso scientifico e tecnologico e i significativi benefici che esse sono suscettibili di apportare alla crescita dei mercati stessi e dell'economia in generale". Inoltre, A. AZZUTTI, *AI-driven Market Manipulation and Limits of the EU law enforcement regime to credible deterrence*, *in ILE Working Paper Series,* 2022, vol. 45 parla di possibile obsolescenza della legislazione europea (MAR e MAD II) al crescere della complessità della tecnologia usata per progettare i sistemi di *trading* algoritmico. Sottolineano le possibili criticità delle norme europee in materia: C. MARTINS PEREIRA, *Unregulated Algorithmic Trading: Testing the Boundaries of the European Algorithmic Trading Regime*, in Journal of Financial Regulation, 2020, vol. 6, issue 2, pp. 270–305 in partic. 285-305; M. GARGANTINI, *The European Regulation of Securities Exchanges: Regulated Markets in an Evolving Technological and Legal Context*, Torino, Giappichelli, 2022.

[223] Regolamento (Ue) 2024/1689 del Parlamento Europeo e del Consiglio, entrato in vigore l'1 agosto 2024. https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=OJ%3AL_202401689#d1e2918-1-1.
Numerose le iniziative regolatorie intraprese, anche al di fuori dell'Unione europea, in materia di intelligenza artificiale. Fra le più significative si segnalano: la Dichiarazione di Blethcley del novembre 2023, adottata all'esito dell'AI Safety Summit impegna ventotto Paesi alla promozione sul piano internazionale di un approccio cooperativo nell'adozione di strategie di *governance* nel settore dell'i.a. (https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration) e l'*Executive Order on the Safe, Scure and Trustworthy Development and Use of Artificial* Intelligence statunitense del 30 ottobre 2023 (https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/); nonché la Decisione quadro sull'intelligenza artificiale del Consiglio d'Europa, che – in linea con le previsioni dell'AI Act – ha l'obiettivo di garantire la compatibilità dei sistemi di intelligenza artificiale con i

Il Regolamento sull'intelligenza artificiale si pone come obiettivo la tutela dei diritti fondamentali, nell'ottica di prevenzione da possibili rischi derivanti dal ricorso a sistemi di intelligenza artificiale e stabilisce obblighi per i fornitori e gli utenti di tali sistemi a seconda del livello di rischio che essi comportano[224]. Il testo distingue

diritti umani, la democrazia e lo Stato di diritto, consentendo nel contempo l'innovazione e la fiducia (https://rm.coe.int/1680afae3c) Per una ricostruzione si veda O. POLLICINO – P. DUNN, *Intelligenza artificiale*, *op. cit.*, pp. 67-72.

[224] Considerando 26 del Regolamento. Secondo l'art. 3, par. 1 per "rischio" si intende "la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso"

infatti fra sistemi a rischio inaccettabile[225], sistemi ad alto rischio[226] e sistemi a basso rischio[227].

---

[225] Art. 5 del Regolamento. Sono sistemi che comportano un rischio inaccettabile per i diritti fondamentali delle persone e dunque la loro immissione sul mercato è vietata.
L'art. 5 (lett. a-h) stabilisce un divieto assoluto per le pratiche di immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali manipolative o ingannevoli per distorcere il comportamento delle persone e provocare un danno significativo; che sfrutta le vulnerabilità di una persona (dovuta all'età, alla disabilità o altra condizione sociale o economica) con lo scopo di distorcerne il comportamento in modo da causare un danno significativo; di valutazione o classificazione delle persone sulla base del loro comportamento sociale o caratteristiche personali i cui risultati determinino un trattamento pregiudizievole o sfavorevole in contesti sociali non collegati a quelli in cui i dati sono stati raccolti o in modo ingiustificato o sproporzionato rispetto al comportamento sociale o alla sua gravità (c.d. *social scoring*); che valutino dil rischio che una persona commetta un reato unicamente sulla base della profilazione della persona o della valutazione dei tratti della personalità; che costituiscono o ampliano banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini da internet o da filmati di telecamere a circuito chiuso; che inferiscono le emozioni di una persona nel luogo di lavoro o istituiti di istruzione; che classificano le persone sulla base di dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, condizioni religiose o filosofiche, vita o orientamento sessuale; sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico non necessari a individuare vittime di tratta di esseri umani, sfruttamento sessuale o persone scomparsi, prevenzione di minacce specifiche per la vita o l'incolumità delle persone fisiche o di attacchi terroristici, localizzazione o identificazione di persona sospettata di aver commesso determinati reati.

[226] Art. 6 del Regolamento. I sistemi ad alto rischio si possono suddividere in due gruppi: quelli integrati in prodotti critici per la sicurezza e i sistemi autonomi con implicazioni sui diritti fondamentali (elencati nell'Allegato III del Regolamento. Si tratta di sistemi ammessi, a condizione che non presentino un rischio significativo di danni per la salute, la sicurezza o i diritti fondamentali delle persone fisiche.
La prima categoria comprende i sistemi di IA integrati in prodotti critici per la sicurezza come dispositivi medici, ascensori e alcuni veicoli.
La seconda categoria comprende i sistemi di IA autonomi con implicazioni per i diritti fondamentali, come quelli utilizzati nella gestione delle infrastrutture critiche e nelle valutazioni educative.
Tali sistemi devono essere vagliati prima dell'ammissione sul mercato e durante tutto il ciclo di vita. Inoltre sono obbligati ad adottare e assicurare sistemi di mitigazione del rischio, elevata qualità dei set di dati, registrazione dell'attività, documentazione dettagliata, informazioni chiare per l'utente, supervisione umana e un alto livello di robustezza, accuratezza e sicurezza informatica. Per i sistemi ad alto rischio l'AI Act introduce requisiti tecnici e documentali stringenti, comprese le valutazioni d'impatto sui diritti fondamentali e le valutazioni di conformità. Si richiede inoltre la supervisione umana per i sistemi ad alto rischio e la *governance* dei dati.
Esempi di tali sistemi di IA ad alto rischio includono determinate infrastrutture critiche, ad esempio nei settori dell'acqua, del gas e dell'elettricità; dispositivi medici; sistemi per determinare l'accesso alle istituzioni educative o per reclutare persone; o determinati sistemi utilizzati nei settori dell'applicazione della legge, del controllo delle frontiere, dell'amministrazione della giustizia e dei processi democratici.

Prima dell'adozione del provvedimento sono stati analizzati un ampio numero di sistemi di intelligenza artificiale, ai fini dell'inserimento in ciascuna delle categorie, fra questi anche i sistemi di negoziazione algoritmica. Tuttavia, nella versione finale del testo essi sono stati espressamente esclusi, poiché tale attività risultavano regolate "in modo esaustivo dal Regolamento delegato (UE) 2017/589 della Commissione"[228]. Si è infatti ritenuto che nell'ambito delle norme che regolano il settore finanziario, esistesse già una normativa adeguata e specifica capace di affrontare i rischi generati dalle applicazioni di intelligenza artificiale[229]. Perciò si è esclusa la necessità di un aggiornamento o una revisione delle norme già citate.

Si tratta, tuttavia, di una considerazione solo in parte corretta e che pone in parziale discussione l'intento del legislatore eurounitario di voler fornire un quadro giuridico completo sull'intelligenza artificiale[230], comprensivo di tutte le attività svolte sfruttando tale tecnologia.

L'opportunità di includere il *trading* algoritmico quantomeno nella categoria dell'AI a rischio non elevato avrebbe dovuto infatti essere confermata dalla sempre maggiore autonomia degli algoritmi di *trading* rispetto alla volontà dello sviluppatore e dai crescenti problemi di opacità e comprensibilità determinati dalla *black box*[231]. In questo senso, avrebbe potuto essere valutata positivamente l'imposizione degli obblighi di trasparenza previsi per i fornitori di sistemi di

---

[227] Art. 50 Regolamento sull'intelligenza artificiale. Alcuni sistemi di IA a rischio limitato devono soddisfare requisiti minimi di trasparenza e/o marcatura. Gli obblighi di trasparenza riguardano principalmente i sistemi di IA destinati a interagire direttamente con le persone fisiche. Esempi di questa categoria sono applicazioni come i gli *AI-enabled recommender systems*, *chatbox* o i filtri antispam, si tratta di sistemi che presentano solo un rischio minimo o nullo per i diritti o la sicurezza dei cittadini.

[228] Cfr. *Commission staff working document impact assessment accompanying the proposal for a regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative* act, nota 237, pag. 51

[229] *Commission staff working document impact assessment accompanying the proposal for a regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative act*, par. 5.3, pag. 43.

[230] Cfr. *Press release*, 9 December 2023, *Commission welcomes political agreement on Artificial Intelligence Act* e, nello specifico, le dichiarazioni di Ursula Von Der Leyen ivi riportate.

[231] Al contrario, gli obblighi di trasparenza previsti dall'AI Act riguardano solo determinati sistemi AI, ovvero: sistemi che interagiscono con gli esseri umani, sistemi che vengono utilizzati per rilevare emozioni o determinare l'associazione con categorie (sociali) basate su dati biometrici, o sistemi che generano o manipolano contenuti (*deep fake*).

intelligenza artificiale per finalità generali[232] anche agli sviluppatori o ai fornitori dei sistemi di *trading* che impiegano intelligenza artificiale.

D'altra parte, nessun riferimento esplicito al *trading* algoritmico si rinviene nemmeno nella proposta di Direttiva sulla responsabilità dell'intelligenza artificiale[233], che pure fa emergere la necessità di superare gli ostacoli determinati dal problema della c.d. *black box.*

La proposta di c.d. AI Liability Directive mira infatti ad adeguare le norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale, partendo dal presupposto che le vigenti normative nazionali in materia di responsabilità, specie se per colpa, non siano idonee a regolare in modo appropriato le azioni di responsabilità per danni causati da prodotti e servizi basati sull'intelligenza artificiale. La spiegazione di tale inadeguatezza si rinviene proprio nella complessità, nell'autonomia e nell'opacità tipiche dei sistemi di intelligenza artificiale[234].

Sicché, le regole contenute nella Proposta di Direttiva forniscono norme comuni per quanto riguarda "la divulgazione di elementi di prova relativi a sistemi di intelligenza artificiale ad alto rischio per consentire all'attore in un'azione civile di responsabilità extracontrattuale per colpa di motivare adeguatamente la domanda di risarcimento del danno[235]", nonché le regole di distribuzione dell'onere della prova nell'ambito dei procedimenti civili di responsabilità extracontrattuale per colpa.

Il testo della Proposta di Direttiva non fa specifico riferimento a sistemi di intelligenza artificiale, ma emergono chiari riferimenti al fatto che "quando l'intelligenza artificiale si interpone fra l'azione o l'omissione di una persona e il danno, le specifiche caratteristiche di alcuni sistemi di IA, come l'opacità, il comportamento autonomo e la complessità, possono rendere eccessivamente difficile, se non impossibile, soddisfare l'onere della prova"[236]. In particolare, si

---

[232] Cfr. Art. 53 "Obblighi dei fornitori di modelli di IA per finalità generali", Regolamento sull'intelligenza artificiale.

[233] Proposta di Direttiva del Parlamento europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (Direttiva sulla responsabilità da intelligenza artificiale) COM(2022) 496 Final.

[234] Nella relazione di accompagnamento alla proposta di Direttiva si specifica che tali caratteristiche "possono rendere difficile o eccessivamente costoso, per quanti subiscono un danno, identificare la persona responsabile e dimostrare che sussistono i presupporti ai fini dell'esito positivo di un'azione di responsabilità".

[235] Art. 1 Proposta di Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale.

[236] Considerando 3 della Proposta di AI Liability Directive.

evidenza la "difficoltà di dimostrare che un determinato *input* di cui è responsabile la persona tenuta a rispondere del danno, ha provocato un determinato *output* del sistema di intelligenza artificiale, che ha sua volta ha causato il danno"[237]. Tale difficoltà è peraltro accentuata dall'elevato numero di persone normalmente coinvolte nella progettazione, nello sviluppo, nell'impiego e nel funzionamento"[238] dei sistemi di intelligenza artificiale e rende complesso individuare la persona potenzialmente tenuta a rispondere del danno cagionato.

La Proposta di Direttiva fornisce una soluzione a tali ostacoli prevedendo obblighi di divulgazione di elementi di prova da parte dei sistemi di intelligenza artificiale e presunzioni di sussistenza del nesso di causalità tra colpa delle persone responsabili del sistema e *output* prodotto da quest'ultimo[239]. Si tratta di regole

---

[237] Considerando 3 della Proposta di AI Liability Directive.

[238] Considerando 17 della Proposta di AI Liability Directive.

[239] Secondo l'attuale formulazione dell'art. 4 della Proposta prevede: "1. Fatti salvi i requisiti di cui al presente articolo, ai fini dell'applicazione delle norme in materia di responsabilità alle domande di risarcimento del danno gli organi giurisdizionali nazionali presumono l'esistenza del nesso di causalità tra la colpa del convenuto e l'output prodotto da un sistema di IA o la mancata produzione di un output da parte di tale sistema se sono soddisfatte tutte le condizioni seguenti:

a) l'attore ha dimostrato o l'organo giurisdizionale ha presunto, a norma dell'articolo 3 paragrafo 5, la colpa del convenuto o di una persona della cui condotta il convenuto è responsabile, consistente nella non conformità a un obbligo di diligenza previsto dal diritto dell'Unione o nazionale e direttamente inteso a proteggere dal danno verificatosi:

b) si può ritenere ragionevolmente probabile, sulla base delle circostanze del caso, che il comportamento colposo abbia influito sull'output prodotto dal sistema di IA o sulla mancata produzione di un output da parte di tale sistema:

c) l'attore ha dimostrato che il danno è stato causato dall'output prodotto dal sistema di IA o dalla mancata produzione di un output da parte di tale sistema.

2. In caso di domanda di risarcimento del danno presentata contro un fornitore di un sistema di IA ad alto rischio soggetto ai requisiti stabiliti al titolo III, capi 2 e 3, della [legge sull'IA] una persona soggetta agli obblighi del fornitore a norma [dell'articolo 24 o dell'articolo 28, paragrafo 1, della legge sull'IA], le condizioni di cui al paragrafo 1, lettera a), sono soddisfatte unicamente se l'attore ha dimostrato che il fornitore o, se del caso, la persona soggetta a obblighi del fornitore non ha rispettato uno dei requisiti stabiliti da tali capi e indicati di seguito, tenendo conto delle misure adottate nel quadro del sistema di gestione dei rischi e dei relativi risultati a norma [dell'art. 9 e dell'art. 16, lettera a), della legge sull'IA]:

a) il sistema di IA è un sistema che utilizza tecniche che prevedono l'uso di dati per l'addestramento di modelli e che non è stato sviluppato sulla base di set di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui [all'art. 10, paragrafi da 2 a 4 della legge sull'IA];

b) il sistema di IA non è stato progettato e sviluppato in modo da soddisfare gli obblighi di trasparenza di cui [all'articolo 13 della legge sull'IA];

che evidentemente non possono valere in ambito penale, ma che testimoniano l'aumentare della complessità di accertamento delle responsabilità quando si opera attraverso sistemi – come quelli di intelligenza artificiale – che agiscono in modo più o meno oscuro e che prevedono l'intervento di numerosi soggetti, nonché una alta dose di autonomia operativa.
Tali considerazioni, allo stato attuale, non hanno però portato il legislatore europeo a intervenire anche in ambito penalistico (e nemmeno nello specifico settore della responsabilità penale per i reati di *market abuse* commessi tramite il ricorso al *trading* algoritmico). Si discuterà nei capitoli che seguono sulla validità di questa scelta.

3. La disciplina italiana

3.1. Premessa

Nell'ordinamento italiano, l'esito dei reiterati interventi normativi sopracitati è la presenza di un *corpus* normativo i cui limiti sono stati più volte evidenziati dalla dottrina[240]. Il percorso di adeguamento delle norme interne al Regolamento

---

c) il sistema di IA non è stato progettato e sviluppato in modo da consentire una supervisione efficace da parte di persone fisiche durane il periodo in cui il sistema di IA è in uso a norma [dell'articolo 14 della legge sull'IA];
d) il sistema di IA non è stato progettato e sviluppato in modo da conseguire, alla luce della sua finalità prevista, un adeguato livello di accuratezza, robustezza e cibersicurezza a norma [dell'articolo 15 e dell'articolo 16, lettera a), della legge sull'IA; oppure
e) non sono state immediatamente adottate le azioni correttive necessarie per rendere il sistema di IA conforme ai requisiti stabiliti [dal titolo III, capo 2, della legge sull'IA] o per ritirarlo o richiamarlo, a seconda dei casi, a norma [dell'articolo 16, lettera g) e dell'articolo 21 della legge sull'IA]. […]

5. In caso di domanda riguardante un sistema di IA che non è ad alto rischio, la presunzione di cui al paragrafo 1 si applica solo se l'organo giurisdizionale ritiene eccessivamente difficile per l'attore dimostrare l'esistenza del nesso di causalità di cui al paragrafo 1. […]"

[240] Gli interventi, oltre ad essere stati scarsamente tempestivi, hanno generato (e mai veramente risolto) numerose questioni.
La prima attiene all'adeguamento solo parziale della normativa italiana – anche dopo il 2021 – alle fonti sovranazionali, come nota S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., p. 95 "le fonti sovranazionali prevedono un'unica fattispecie di abuso di informazioni privilegiate e un'unica fattispecie di manipolazione di mercato e, nel prescrivere per entrambe sanzioni penali effettive, proporzionate e dissuasive (art. 7.1 Direttiva 2014/57/UE), ovviamente non consentono che – come attualmente in Italia – il loro recepimento testuale sia avvenuto esclusivamente nell'illecito amministrativo".
La seconda riguarda invece la compatibilità del doppio binario sanzionatorio (amministrativo e penale) con il principio del *ne bis in idem*. Cfr. *ex multis* F. VIGANÒ, Ne bis in idem *e pluralità di sistemi sanzionatori per lo stesso fatto*, in Rivista delle società, 2023, fasc. 1, pp. 189-207; C.

MAR e di recepimento delle Direttive MAD II e MiFID II è stato assai travagliato e, come noto, ha avuto un primo – insoddisfacente[241] – esito nel 2018[242] e uno successivo nel 2022[243].

Nel tempo, l'impianto delle principali norme incriminatrici (art. 184 e 185 t.u.f.) è rimasto sostanzialmente immutato – nonostante le fattispecie di illecito siano state integrate e modificate in modo significativo dal d.lgs. 107/2018 –, salvo da un lato estenderne l'applicazione alle condotte aventi ad oggetto un novero più ampio di strumenti finanziari, dall'altro degradare a reato contravvenzionale talune ipotesi che riguardano essenzialmente le operazioni aventi ad oggetto strumenti finanziari ammessi alla negoziazione o per i quali sia stata presentata

---

SILVA, *La proporzionalità della pena in materia di abusi di mercato. Profili problematici di un sindacato diffuso di ri-equilibrio sanzionatorio*, in *Sist. Pen.*, 2023; M. GAMBARDELLA, *Condotte economiche*, *op. cit.*, pp. 435-450; E. BASILE, *Il "doppio binario" sanzionatorio degli abusi di mercato in Italia e la trasfigurazione del* ne bis in idem europeo, in *Giur. comm*., 2019, fasc. 1, pp. 129-141; F. MUCCIARELLI*, Gli abusi di mercato riformati e le persistenti criticità di una tormentata disciplina*, in Dir. Pen. Cont. Riv. Trim., 2018, fasc. 3, pp. 174-189; F. VIGANÒ, *Doppio binario sanzionatorio e* ne bis in idem*: verso una diretta applicazione dell'art. 50 della carta? (a margine della sentenza Grande Stevens della Corte edu)*, in Dir. Pen. Cont. Riv. Trim, fasc. 3-4, pp. 219-238.

[241] La limitata riforma disattende l'auspicio di un "intervento di adeguamento assai approfondito al cospetto di una disciplina eurounitaria che, già sul piano della descrizione delle condotte vietate, importa variazioni notevolissime derivanti dall'uso della tecnica analitica" in F. MUCCIARELLI, *La nuova disciplina eurounitaria*, 2015 *op. cit.*, p. 317. Cfr. anche S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., pp. 73-74; F. MUCCIARELLI–E. BASILE, *Market abuse evolution after the MAD II and the MAR: how Italy amended its legislation in light of Regulation (EU) 596/2014*, in Criminal Justice Network, 2018, pp. 1-5; nonché F. MUCCIARELLI, *Gli abusi di mercato* riformati, *op. cit.*, pp. 174-189 criticano il ricorso alla tecnica del rinvio e le problematiche relative alla mancanza di tassatività e determinatezza dell'intervento di riforma.

[242] Decreto Legislativo 10 agosto 2018, n. 107, Norme di adeguamento della normativa nazionale alle disposizioni del regolamento (UE) n. 596/2014, relativo agli abusi di mercato e che abroga la Direttiva 2003/6/CE e le Direttive 2003/124/UE, 2003/125/CE e 2004/72/CE. Con tale provvedimento, il Governo ha adeguato (parzialmente) la normativa interna al solo MAR, invece di attuare la Direttiva MAD II. Cfr. E. BASILE, *Riforma del* market abuse: *quando la toppa (parlamentare) è peggiore del buco (governativo)*, in Dir. Pen. Cont., Riv. Trim., 2017, fasc. 11, 228-230.; ID., *Mini-riforma del* market abuse*: obiettivi mancati ed eterogenesi dei fini del d. lgs. n. 107/2018*, in Dir. Pen. Proc., 2018, fasc. 3, p. 336.

[243] Dopo anni di attesa e in pendenza di una procedura di infrazione (n.2109/2130), l'ulteriore modifica del TUF in tema di abusi di mercato avviene con la Legge 23 dicembre 2021, n. 238 - Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2019-2020. Tale norma – tra l'altro – attribuisce rilevanza penale alle condotte dell'*insider* secondario (art. 184 t.u.f.), inasprisce ulteriormente le sanzioni penali per l'*insider* primario e limita la confisca obbligatoria ex art. 187 t.u.f. al solo profitto derivante dal reato. Anche questo secondo intervento di adeguamento alla normativa eurounitaria risulta però insoddisfacente, cfr. S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., p. 74.

richiesta di ammissione in un sistema multilaterale di negoziazione o in un sistema organizzato di negoziazione.

3.2. Il reato di abuso di informazioni privilegiate

La condotta di chi sfrutta, mediante utilizzo in operazioni borsistiche ovvero comunicazione o trasmissione a terzi, informazioni privilegiate non derivanti da una superiore capacità di analisi, ma ottenute per ragioni funzionali[244] è sanzionata nell'ordinamento italiano dall'art. 184 t.u.f.[245]

Ratio della norma è essenzialmente impedire lo sfruttamento di vantaggi informativi dei quali si può godere per via di posizioni ricoperte nell'ambito di un emittente, ovvero di legami professionali o personali con chi ricopre simili posizioni o, ancora, di sfruttare informazioni ottenute anche casualmente o fortuitamente ma, comunque, senza meriti o capacità specifiche[246]. Lungi dal contrastare in sé e per sé qualsivoglia vantaggio informativo di taluni operatori del mercato, obiettivo del legislatore è piuttosto tutelarne l'efficienza e la

---

[244] Cfr. S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., p. 78.

[245] L'attuale formulazione è l'esito di un articolato susseguirsi di riforme, accomunate fino al 2021 dalla previsione di un reato proprio del detentore qualificato delle informazioni in ragione di una posizione interna all'emittente, il lavoro, la funzione o l'ufficio e dalla distinzione fra *insider* primari e secondari (destinatari di divieto penale solo a seguito della l. 238/2021).
La prima introduzione del reato risale agli inizi degli anni Novanta. La l'art. 2 della l. 17 maggio 1991, n. 157, in attuazione della Direttiva 89/592/CEE, sanzionava il compimento di operazioni, anche per interposta persona, su valori mobiliari, da parte di chi fosse in possesso di informazioni riservate in virtù della partecipazione a capitale di una società ovvero in ragione dell'esercizio di una funzione, anche pubblica, professione o ufficio; nonché la comunicazione a terzi di tali informazioni o la raccomandazione di operazioni sulla base di queste. Era inoltre prevista la punibilità di chi riceveva le informazioni.
A distanza di sette anni, è intervenuta una significativa modifica ad opera del d.lgs. 58/1998, che ha inserito il divieto di *insider trading* nel t.u.f. (art. 180), seguita dalla l. 18 aprile 2005, n. 62 (recepimento della Direttiva 2003/6/CE) che ha ulteriormente modificato la fattispecie, oltre a ricollocarla all'art. 184 del neo introdotto Titolo I *bis* (Abuso di informazioni privilegiate e manipolazione del mercato), Parte V, d.lgs. n. 58/1998. Nello stesso anno, l. 28 dicembre 2005, n. 262, sono state raddoppiate le sanzioni e quattro anni dopo, il d.lgs. 17 luglio 2009, n.101 ha introdotto una fattispecie contravvenzionale al comma 3 *bis* dell'art. 184 t.u.f.
Le modifiche più recenti risalgono al 2018 (d.lgs. 10 agosto 2018, n. 107) e infine alla l. 23 dicembre 2021, n.238, che ha, tra l'altro, modificato l'ambito di applicazione degli illeciti penali e amministrativi, inasprito le sanzioni e introdotto ulteriori ipotesi di incriminazione.

[246] Cfr. sul punto *ex multis* M. VENTORUZZO, *Qualche nota sul cosiddetto "insider di sé stesso" alla luce del Regolamento UE sugli abusi di mercato*, in Le società., 2018, fasc. 6, pp. 739-751.

credibilità e attrarre così risparmio e liquidità. La fattispecie è costruita come reato di pericolo astratto[247].

Quanto al soggetto attivo, la disciplina ha risentito dell'impulso eurounitario e, a seguito della l. n.238 del 2021, la punibilità è espressamente estesa – oltre che all'*insider* primario[248]e al *criminal insider*[249] la cui punibilità era già prevista dalla formulazione precedente – anche all'*insider* secondario[250]. Secondo la dottrina, tali categorie sono accomunate dalla necessaria alterità nei confronti della fonte dell'informazione, posto che il concetto stesso di informazione supporrebbe una preesistenza di essa al momento dell'acquisizione[251].

---

[247] Sul punto si veda F. D'ALESSANDRO, *Regolatori del mercato, op. cit.*, p. 135 che, ai fini della realizzazione del reato non è necessaria la dimostrazione di un guadagno da parte dell'agente, posto che la scelta di ricorrere allo schema del pericolo astratto esime il giudice dalla verifica della concreta potenzialità lesiva della singola condotta, ma non dal rispetto dei principi di offensività e colpevolezza che ostano all'utilizzo di schemi probatori presuntivi. Cfr. anche S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., p. 77 secondo cui "la strumentalizzazione del divieto penale al conseguimento di scopi come la credibilità del mercato finanziario o la fiducia degli investitori solleva forti perplessità, a causa della traslazione così operata tra lo scopo finale del divieto e la lesività intrinseca della condotta, assunta in una dimensione seriale e proiettata su conseguenze talmente mediate e impalpabili da indurre a ravvisare un'esasperazione della funzione promozionale del diritto penale". Perplessità che secondo l'Autore sono rafforzate dall'opzione per la struttura del pericolo astratto del reato, che impedisce la ricerca nella condotta di un qualsiasi coefficiente di offensività".
Nonché, in giurisprudenza, Cass. Pen., Sez. V, 15 aprile 2019 (dep. 27 settembre 2019), n. 39999, in C.E.D. Cass., n. 276963 nonché in Sist. Pen. con nota di C. PAGELLA, *L'inafferrabile concetto di "connessione sostanziale e temporale sufficientemente stretta": la Cassazione ancora su* ne bis in idem *e* insider trading, in Sist. Pen., 9 gennaio 2020.

[248] Il soggetto che è in possesso di informazioni privilegiate "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". Art. 184, primo comma, t.u.f.

[249] Il c.d. *criminal insider,* ai sensi dell'art. 184, secondo comma, t.u.f., è chi è in possesso delle informazioni a motivo della preparazione o dell'esecuzione di attività delittuose.

[250] Il soggetto consapevolmente in possesso di informazioni privilegiate per ragioni diverse da quelle dell'*insider* primario e del *criminal insider*, salvi i casi di concorso con questi. Art. 184, terzo comma, t.u.f. Con riferimento alla figura dell'insider secondario, pare opportuno sottolineare che nelle intenzioni del legislatore europeo (sia della MAD II che del MAR) le due figure, insider primario e insider secondario, avrebbero dovuto essere sostanzialmente equiparate.

[251]*Ex multis,* S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., p. 81. L'Autore nota però che "l'estensione della soggettività attiva al *criminal insider* è avvenuta mediante una distorsione del concetto di informazione privilegia, il cui abuso viene ora configurato anche rispetto al suo creatore". A questo proposito si segnala il dibattuto tema della responsabilità dell'*insider* di se stesso. Parte della dottrina – S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., pp. 79-80; M. VENTORUZZO, *Qualche nota sul cosiddetto "insider di sé stesso"*, *op. cit.*, p.742

Ad ogni modo, la scelta di ricorrere a definizioni ampie per individuare i soggetti attivi del reato porta la dottrina ad affermare la particolarità della norma "che esordisce con un reato proprio e, con una minima riduzione di pena, lo trasforma in reato comune".

Le condotte sanzionate sono, come noto, tre[252].

La prima – art. 184, primo comma, lett. a) – consiste essenzialmente nello sfruttamento delle conoscenze privilegiate per realizzare operazioni su strumenti finanziari ("acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime")[253].

La seconda condotta è il c.d. *tipping* - art. 184, primo comma, lett. b) – e consiste nella comunicazione a terzi di informazioni privilegiate, al di fuori del normale esercizio del lavoro, della professione o dell'ufficio o di sondaggi di mercato.

Infine, la terza, il c.d. *tuyautage* – art. 184, primo comma, lett. c) – è la condotta di raccomandazione o induzione di terzi, sulla base delle informazioni privilegiate, a compiere operazioni su strumenti finanziari[254].

– esclude la punibilità dell'*insider* di se stesso affermando che si errato pensare che l'espressione "informazione" vada intesa quale conoscenza, indipendentemente dal fatto che tale conoscenza sia stata o meno trasmessa dall'agente. Al contrario, in giurisprudenza si è ormai consolidato l'orientamento favorevole alla punibilità del soggetto – c.d. insider di sé stesso – che abusa di un'informazione attinente a un evento dallo stesso progettato o ideato.

[252] Per un'analisi completa delle condotte, si veda F. SGUBBI, *La manipolazione del mercato*, in F. Sgubbi–D. Fondaroli–A. Tripodi, Diritto penale del mercato finanziario. Abuso di informazioni privilegiate, manipolazione del mercato, ostacolo alle funzioni di vigilanza della Consob, falso in prospetto. Lezioni, II ed., Padova, Cedam, 2013, pp. 71-112.

[253] Secondo una parte della dottrina, S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., p. 93, stando alla formulazione della norma, rimangono escluse dal tipo le condotte di annullamento o modifica di un ordine concernente uno strumento finanziario al quale le informazioni si riferiscono quando tale ordine è stato inoltrato (prima che la persona entrasse in possesso delle informazioni privilegiate) e poi revocato. In questo senso, il t.u.f. divergerebbe dalla previsione di cui all'art. 3.4 della Direttiva MAD II, che qualifica espressamente tale condotta come abusiva. In senso contrario, F. MUCCIARELLI, *La nuova disciplina eurounitaria*, 2015 *op. cit.*, p. 315.

[254] L'art. 3.6 della MAD II prevede espressamente che la condotta di induzione o raccomandazione possano avere ad oggetto l'annullamento o la modifica di un precedente ordine di acquisto o di vendita di strumenti finanziari. Inoltre, l'art. 8.3 del MAR puntualizza che il la raccomandazione o l'induzione costituiscono abuso di informazioni privilegiate quando l'agente è consapevole che essa si basa su conoscenze riservate. La stessa precisazione non è riportata nella formulazione italiana della fattispecie. Secondo S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*.. p. 96 ciò implica che "il precetto ruoti sempre intorno al possesso delle informazioni utilizzate o comunicate o impiegate per la raccomandazione o l'induzione, con la conseguenza che il destinatario della raccomandazione o induzione – il quale (…) non detiene un'informazione privilegiata – è libero di farne uso o cederla a terzi".

Tutte e tre le condotte sono sanzionate se sorrette da dolo: il soggetto attivo deve rappresentarsi la natura privilegiata dell'informazione e volerla sfruttare o comunicare a terzi; oggetto del dolo, in caso di induzione o raccomandazione (*tuyautage*) è anche l'utilizzo dell'informazione da parte del destinatario[255].
Il reato è punito anche a titolo di tentativo.
Con riferimento all'abuso di informazioni privilegiate, l'art. 187 *ter.1* t.u.f. – che riprende l'art. 18 del MAR – impone un obbligo di redazione di un elenco delle persone aventi accesso a informazioni privilegiate sulla base di rapporti lavorativi. Tale elenco deve essere stilato dagli intermediari (gestori del mercato e le imprese di investimento che gestiscono una sede di negoziazione). È inoltre previsto un obbligo di segnalazione delle operazioni sospette[256]. A questi si aggiungono, per le persone fisiche, obblighi comunicativi sulle variazioni dei possessi azionari[257].

3.3. L'illecito amministrativo di abuso di informazioni privilegiate

Come noto, la condotta di abuso di informazioni privilegiate integra anche l'illecito amministrativo di cui all'art. 187 *bis*, che punisce con la sanzione amministrativa pecuniaria da ventimila euro a cinque milioni di euro chiunque viola il divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate di cui all'articolo 14 del Regolamento MAR. Per la fattispecie amministrativa, in virtù del rinvio alla normativa europea, alle condotte tipizzate dall'art. 184 t.u.f., si aggiunge anche l'uso delle informazioni privilegiate "tramite annullamento o modifica di un ordine concernente uno strumento finanziario al quale le informazioni si riferiscono quando tale ordine è stato inoltrato prima che la persona interessata entrasse in possesso di dette informazioni privilegiate" e la condotta di chi "raccomanda, sulla base di tali informazioni, a un'altra persona di cancellare o di modificare un ordine concernente uno strumento finanziario cui si riferiscono le informazioni o induce tale persona a effettuare la cancellazione o la modifica".

---

[255] La dottrina rileva che il Regolamento MAR equipara la piena consapevolezza della natura privilegiata dell'informazione alla situazione di "dovrebbe sapere che si tratta di informazioni privilegiate" (art. 8 MAR) e ritiene che la formula "dovrebbe sapere" evochi una regola di esperienza sulla base della quale operare l'accertamento del dolo. Cfr. S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit.*, p. 97 Tale interpretazione pare supportata dal fatto che, anche nella formulazione eurounitaria, la condotta può essere sorretta anche da dolo eventuale.

[256] Cfr. art. 16 Regolamento MAR.

[257] Art. 114, settimo comma, t.u.f. e art. 19 Regolamento MAR.

Dal punto di vista oggettivo, fra la fattispecie penale e quella amministrativa sussiste una pedissequa identità[258].
Quanto all'elemento psicologico, l'illecito amministrativo risulta punibile anche nella forma colposa[259], a differenza di quello penale, stante la regola generale in tema di illecito amministrativo di cui all'art. 3 l.689/1981 - nonché l'espresso riferimento al dolo e alla colpa grave contenuto nell'art. 187 *bis*, comma 2 *bis*, t.u.f.[260]

3.4. Il reato di manipolazione del mercato

La tutela del regolare funzionamento dei mercati nel sistema legislativo italiano si realizza, oltre che tramite la sanzione alle condotte di abuso di informazioni privilegiate, anche per mezzo del divieto di porre in essere condotte artificiose che incidano sui meccanismi di formazione del prezzo dei titoli[261].
L'art. 185 t.u.f. prevede infatti un reato comune di pericolo concreto, a dolo generico, che sanziona la diffusione di notizie false o il compimento di operazioni simulate o altri artifici[262], qualora questi siano concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

---

[258] Sul punto la dottrina è unanime. Cfr., *ex multis*, S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*.. pp. 91, F. D'ALESSANDRO, *Regolatori del mercato*, *op. cit.*, p. 153.

[259] In questo senso A. TRIPODI, *Gli illeciti amministrativi in tema di abusi di mercato*, in F. Consulich (a cura di), Reati in materia finanziaria, Torino, Giappichelli, 2024, pp. 286-288 secondo cui nella fattispecie amministrativa sono presenti "chiari indici di responsabilità per colpa", fra cui il riferimento alla conoscenza o conoscibilità della natura privilegiata dell'informazione (sia per l'*insider* primario, che per *l'insider* secondario), di cui all'art. 8, quarto comma, e art. 10, secondo e terzo comma Regolamento MAR; *idem* M. GAMBARDELLA, *Condotte economiche*, *op. cit.*, p. 398; V. NAPOLEONI, *L'*insider trading, in C. Santoriello (a cura di), La disciplina penale dell'economia, vol. I, Torino, Giappichelli, 2008, p. 746 nonché F. D'ALESSANDRO, *Regolatori del mercato*, *op. cit.*, p. 153 "tra le caratteristiche maggiormente degne di nota di tale previsione, che dal punto di vista delle condotte tipiche ripercorre pedissequamente la struttura del delitto, vi è quella, coerente con la previsione generale di cui all'art. 3, comma 1, legge 24 novembre 1981, n. 689, di essere punita indifferentemente sia a titolo di dolo, sia a titolo di colpa".

[260] In senso contrario S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*.. pp. 93-94 che sostiene la sola punibilità a titolo di dolo, nonostante la "svista legislativa" contenuta nell'art.187 *quater* comma 2 *bis* t.u.f..

[261] La condotta – riconducibile all'antica nozione di 'aggiotaggio' – è, come noto, sanzionata anche dall'art. 2637 c.c. (che, a seguito dell'introduzione degli artt. 185 e 187 *ter* t.u.f. mantiene un'operatività residuale e limitata agli strumenti finanziari non quotati o per il quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato) e dall'art. 501 c.p. (che si ritiene implicitamente abrogato rispetto alle condotte incidenti su strumenti finanziari).

[262] Per la definizione della vaga nozione di "altri artifizi", che rinvia alle tecniche suggerite dall'esperienza, la dottrina ritiene di poter fare rinvio agli indicatori di manipolazione del Regolamento MAR e Reg. delegato 2016/522 illustrati *supra*.

Fulcro della fattispecie italiana è dunque la concreta idoneità della condotta a provocare la sensibile alterazione del prezzo di uno o più strumenti finanziari[263].
Le fattispecie di manipolazione del mercato di cui agli artt. 185, essendo un illecito di pericolo (concreto) e di mera condotta a consumazione anticipata, non richiede la realizzazione di alcun evento lesivo causalmente riconducibile alla condotta tipizzata, quantomeno in senso naturalistico[264].
Secondo la dottrina, il riferimento all'idoneità alterativa oltre a caratterizzare la condotta, costituisce l'evento di pericolo concreto[265]. Sicché, la condotta di manipolazione assume rilevanza penale solo ove i comportamenti descritti dalla

---

[263] C.d. *price sensitivity* o 'materialità', da intendersi come capacità di influire in terminin di rialzo o ribasso dei prezzi, ma anche di mantenimento forzato a livelli diversi da quelli che sarebbero stati senza la condotta manipolatoria cfr. sul punto M. B. MAGRO, *Manipolazioni dei mercati finanziari e diritto penale. Una critica al modello di razionalità economica*, Milano, Giuffrè, 2012, p. 255. D'altra parte, l'attitudine a cagionare un aumento o una diminuzione dei prezzi borsistici caratterizza anche la condotta delle fattispecie codicistiche di aggiotaggio (artt. 501 e 501 *bis* c.p.), reato che – a differenza della manipolazione del mercato – è concepito come reato di pericolo astratto Cfr. sul punto, C. PEDRAZZI, *Problemi del delitto di aggiotaggio*, *op. cit.*, pp. 41-43. Nello stesso senso, S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., p. 107, il quale nota inoltre come "l'espressa previsione nell'art. 185 di una concreta idoneità delle condotta esclude certo ogni plausibilità all'idea di un pericolo solo astratto, ma non può negare che il reato di manipolazione del mercato presenti la natura di un pericolo solo tendenzialmente concreto".
L'accertamento del pericolo concreto deve essere operato tramite un giudizio di prognosi postuma *ex ante* a base totale, volto a verificare la capacità della condotta di alterare l'equilibrio delle contrattazioni ovvero di influenzare le decisioni di un investitore ragionevole, secondo l'insegnamento di G. MARINUCCI–E. DOLCINI–G.L. GATTA, *Manuale di diritto penale. Parte Generale*, XIII ed., Milano, Giuffrè, 2024, p. 286. Sulla centralità dell'accertamento dell'attitudine decettiva del fatto si impone un rinvio a C. PEDRAZZI, *Problemi di tecnica legislativa*, 1979, ora in Id, Diritto penale, vol. III - Scritti di diritto penale dell'economia, Milano, Giuffrè, 2003, pp. 129-156.
Il tema della natura del reato e della nozione di "sensibile" alterazioni dei prezzi degli strumenti finanziari è oggetto di ampio dibattito dottrinale, sul quale si rinvia a S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., pp. 109 ss,. In particolare sul significato da attribuire all'aggettivo 'sensibile' e sui parametri alla stregua del quale definirla, in base alla storia e alle oscillazioni che il titolo ha subito, di recente e con prospettive di riforma che prevedano un ancoraggio a un dato quantitativo del concetto di 'sensibile idoneità alterativa', cfr. F. MUCCIARELLI, *Materialità e offensività dell'alterazione, investitore ragionevole e giudizi nella manipolazione del mercato*, in Dir. Pen. Cont. Riv. Trim., 2024, fasc. 3, pp. 24-25.

[264] Così M.B. MAGRO, *Manipolazioni dei mercati finanziari*, *op. cit.*, p. 245. Nello stesso senso, Cass. Pen., Sez. II, 28 novembre 2012, n. 12989 in Pen. Cont., 7 aprile 2013 con nota di F. VIGANÒ, *La Cassazione chiude il caso della scalata Antonventa (e perde una preziosa occasione per fare un po' di chiarezza sui delitti di aggiotaggio);* nonché Cass. Pen., Sez. V, 19 ottobre 2018, n. 53437, in Cass. Pen., 2019, p. 3723. Sulla natura di reato di pericolo concreto F. MUCCIARELLI, *Materialità e offensività dell'alterazione*, *op. cit.*, p. 18 e 22.

[265] Cfr. F. D'ALESSANDRO, *La manipolazione del mercato*, in F. Consulich (a cura di), Reati in materia finanziaria, Torino, 2024, p. 212.

norma “siano concretamente idonei a provocare, in misura ‘sensibile’ l’alterazione del prezzo degli strumenti finanziari, mettendo concretamente in pericolo gli interessi protetti dalla norma penale”[266].

Si tratterebbe cioè di un “evento da collegare *potenzialmente* alla condotta”[267] che consiste nella potenzialità o probabilità di alterazione “delle scelte decisionali degli operatori del mercato che, in conseguenza della condotta […] potrebbero determinarsi a compiere un’operazione che non avrebbero compiuto”[268]. Occorrerebbe, in altri termini, accertare in concreto con il criterio della prognosi postuma di un immaginario investitore ragionevole l’esistenza di un collegamento tra atto manipolativo (di tipo informativo o operativo) e pericolo di alterazione del corso del titolo, quale conseguenza propria e specifica dell’atto manipolativo[269].

---

[266] Così M.B. MAGRO, *Manipolazioni dei mercati finanziari*, *op. cit.*, pp. 246-247, che sottolinea anche la necessità che il giudice accerti la idoneità ingannatoria e l’idoneità alterativa degli atti posti in essere. Sicché “il pericolo si traduce […] nella presenza di un evento da collegare *potenzialmente* alla condotta di interazione psichica, che è il probabile compimento da parte di questi, sulla base di una determinazione psicologica deviata dall’induzione in errore, di una transazione o di una operazione che, a livello macroeconomico, determini una sensibile alterazione del livello dei prezzi”. Così anche S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*. pp. 107-108 secondo cui la natura del pericolo tendenzialmente concreto e il requisito della concretezza impongono di escludere l’integrazione del reato quando sia dimostrabile l’assenza di un pericolo, ma d’altra parte non si spingono fino a esigere “un’impossibile dimostrazione empirica della probabilità dell’alterazione dei prezzi nella situazione data”. Nello stesso senso, con indicazione delle possibili prospettive di riformulazione della fattispecie che colleghino l’idoneità alterativa a un dato quantitativo (che segni peraltro la linea di demacrazione fra illecito penale e illecito amministrativo), si veda F. MUCCIARELLI, *Materialità e offensività dell’alterazione*, *op. cit.*, pp. 20, nonché 24-25.

[267] Enfasi aggiunta. M.B. MAGRO, *Manipolazioni dei mercati finanziari*, *op. cit.*, p. 247. Nello stesso senso, più di recente, F. MUCCIARELLI, *Materialità e offensività dell’alterazione*, *op. cit.*, p. 18, che lo definisce “un momento necessariamente esterno alla condotta medesima […], costitutivo del pericolo (concreto) che la norma mira a scongiurare”. L’Autore, distinguendo fra le condotte descritte dalla norma, rileva come “il compimento di un’operazione simulata o artificiosa, quando dotata della richiesta idoneità, realizza di per sé il concreto pericolo vietato” mentre il parametro di riferimento essenziale per cogliere la tipicità delle condotte di diffusione di notizie false o fuorvianti o della comunicazione decettiva “che l’operazione simulata o artificiosa trasmette di se stessa” è costituito dall’idoneità decettiva rispetto al destinatario “cui corrisponde l’idoneità alterativa del patrimonio conoscitivo e la conseguente influenza sulle scelte operative”. L’Autore aggiunge poi che il dato empirico evidenzia come nella maggior parte dei casi il pericolo si consolidi in danno e la quasi totalità dei procedimenti giudiziari prenda avvio dalla rilevazione da parte di Consob di un’anomalia registrata sui mercati è un’eventualità che non muta la struttura del reato e che “rimane confinata sul piano delle evenienze accidentali” (p. 37).

[268] Così M.B. MAGRO, *Manipolazioni dei mercati finanziari*, *op. cit.*, p. 247.

[269] S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*. pp. 108-109 (e relativa bibliografia citata in nt. 79), secondo cui il giudizio di prognosi postuma deve essere svolto “sulla base della congiuntura di mercato in cui l’azione è stata realizzata, dei mezzi impiegati e della

Anche secondo questa impostazione, tuttavia, ciò non significa che in sede processuale sia necessario accertare l'effettivo verificarsi di un evento lesivo causalmente riconducibile alla condotta tipizzata[270]. Al contrario, il giudizio prognostico consiste nella verifica "se in quella situazione era probabile il verificarsi di un evento temuto, a prescindere dal suo successivo e concreto verificarsi"[271]. Essendo la manipolazione del mercato un illecito di mera condotta, in cui l'offesa è una realtà materiale che si immedesima e si esaurisce nella realizzazione della condotta tipica, non è necessario alcun accertamento ulteriore, che altrimenti finirebbe per sovrapporre il giudizio di offensività del giudice a quello di lesività espresso dal legislatore[272].

---

loro entità, nonché delle caratteristiche dello strumento finanziario interessato". La delicatezza del giudizio, secondo l'Autore, è in qualche modo limitata dal fatto che "queste indagini solitamente prendono avvio attraverso i segnali trasmessi dai sistemi di rilevazione elettronica dell'andamento dei mercati, aventi ad oggetto fatti in cui effettivamente il prezzo dello strumento finanziario ha registrato una sensibile alterazione; in tali ipotesi si tratta dunque di escludere l'esistenza di fattori diversi da soli sufficienti a cagionare il mutamento della quotazione". Nello stesso senso, F. MUCCIARELLI, *Materialità e offensività dell'alterazione*, *op. cit.*, p. 22 nota che pur non essendo discutibile tale natura, "nella prassi delle Corti l'accertamento dell'illecito intervenga dopo che la condotta vietata si è completamente realizzata, sicché il suo effetto perturbativo, se sussistente, si è anch'esso già dispiegato. Di più: all'atto pratico, le vicende processuali sono pressoché tutte legate alla rilevazione di un fenomeno alterativo del prezzo di uno o più strumenti finanziari, fenomeno a partire dal quale inizia la ricerca per individuarne la fonte genetica". Nello stesso senso, già precedentemente, C. PEDRAZZI, *Problemi del delitto di aggiotaggio*, *op. cit.*, pp. 36-38.

[270] F. MUCCIARELLI, *Materialità e offensività dell'alterazione*, *op. cit.*, p. 22 "la idoneità alterativa, estremo costitutivo della fattispecie, prescinde dall'effettività del risultato: una condotta sensibilmente perturbatrice potrebbe infatti non determinare alcuna conseguenza perché 'compensata' da altri fattori […] ma tale condotta, pur (apparentemente) improduttiva di effetti, sarebbe egualmente costitutiva del reato (di pericolo concreto)".

[271] Così M.B. MAGRO, *Manipolazioni dei mercati finanziari*, *op. cit.*, p. 250, che sottolinea inoltre come "l'accertamento del pericolo non implica l'uso del giudizio controfattuale, poiché esso è – per definizione – sganciato dal profilo fattuale legato al verificarsi effettivo dell'evento, che non assume rilevanza nel fulcro della norma".

[272] G. FIANDACA–E. MUSCO, *Diritto penale. Parte Generale,* IX ed., Bologna, Zanichelli, 2024 p. 220. Sull'accertamento del pericolo concreto, si veda C. PIERGALLINI, *Danno da prodotto*, *op. cit.*, pp. 260-263 che individua tre fattori che guidano il giudice: le circostanze concrete da prendere in considerazione (base del giudizio), la base nomologica del giudizio (il metro del giudizio, ossia le leggi che facciano riferimento a regole o massime di esperienza di tipo statistico-probabilistico, in analogia con il giudizio sulla causalità) e il momento del giudizio (che, vista la natura prognostica, prevede che il giudice si riporti al momento del fatto o della condotta).
Sulla difficoltà dell'accertamento dell'evento di pericolo rispetto alla fattispecie in questione, vista la strutturale variabilità del prezzo degli strumenti finanziari e sui conseguenti profili di indeterminatezza della norma, stante l'impossibilità di attribuire con certezza la modifica dei corsi azionari a un dato comportamento criminoso, si veda M.B. MAGRO, *Manipolazioni dei mercati*

Stante la formulazione della norma, la dottrina ha tradizionalmente distinto fra due tipi di manipolazione del mercato: quella informativa (diffusione di notizie false) e quella operativa (compimento di operazioni simulate o altri artifici). Benché ancorata alla lettera della norma, tale distinzione risulta tuttavia assai meno sfumata nella prassi, dal momento che nella realtà dei mercati le condotte hanno una componente mista, operativa e informativa[273]. Pare, dunque, più convincente una distinzione "interna" fra le componenti della manipolazione, anziché i tipi di manipolazione.

Sicché, la componente informativa della manipolazione consisterebbe nella divulgazione effettuata verso un pubblico indifferenziato di una notizia falsa idonea ad alterare il prezzo dello strumento finanziario di riferimento. In questo senso, elemento sufficiente ai fini della configurazione del reato sono la non corrispondenza al vero dei dati presentati come reali – compresa la notizia tendenziosa – e l'idoneità di essi a provocare l'effetto distorsivo. Rimane invece esclusa dal tipo la condotta omissiva, anche in forma impropria, posto che il reato di manipolazione del mercato sanziona condotte che introducono fattori distorsivi nella formazione dei prezzi[274].

D'altra parte, la componente operativa consiste nella creazione di movimenti fittizi di mercato – compimento di operazioni simulate o altri artifici idonei a distorcere il prezzo dei titoli – che dunque trasmettono false informazioni

---

finanziari, *op. cit.*, p. 253; C. PEDRAZZI, *Problemi del delitto di aggiotaggio*, *op. cit.*, pp. 41-44. Più in generale, sul tema del dei giudizi predittivi in contesti probabilistici, F. D'ALESSANDRO, *Pericolo astratto e limiti soglia*, Milano, Giuffrè, 2012, pp. 98-108.

[273] La manipolazione c.d. "operativa" ha anche una componente "informativa", nel senso della capacità di una determinata operazione, che artificiosamente influisce sui prezzi dei titoli, di contribuire a diffondere al mercato una notizia non corrispondente al vero. Sul punto, *ex multis*, C. PEDRAZZI, *Problemi del delitto di aggiotaggio*, *op. cit.*, p. 58; F. MUCCIARELLI, *Gli illeciti di abuso di mercato*, *op. cit.*, p. 844-849; ID *Materialità e offensività dell'alterazione*, *op. cit.*, pp. 30-33.; F. CONSULICH, *La giustizia e il mercato*, *op. cit.* (il quale include la manipolazione operativa nella categoria manipolazione informativa, conferendo invece un'autonoma rilevanza alle ipotesi di sfruttamento di un potere di mercato che consente di agire direttamente sui prezzi degli strumenti finanziari, c.d. *market power manipulation*).

[274] S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., p. 102 esclude la costruzione di un reato omissivo improprio di manipolazione a causa dell'assenza di un evento cui riferire l'operatività dell'art. 40 cpv e più in generale contesta l'interpretazione che si spinge a convertire l'omissione in artificio, sostenendo che la fattispecie incriminatrice comprenda la sola diffusione di notizie false o la realizzazione di artifici, ossia condotte commissive.

al mercato e inducono effetti imitativi nel pubblico[275]. Si tratta di operazioni simulate di natura fraudolenta.

Tradizionalmente, si distingue fra simulazione assoluta e simulazione relativa. La prima consiste nella vendita e acquisto simultaneo del medesimo titolo senza mutare la situazione proprietaria[276]; mentre la seconda è integrata quando si immettono contemporaneamente ordini di vendita e corrispondenti ordini di acquisto, creando l'impressione di un aumento nella domanda non corrispondente al vero e che non modifica la proprietà degli strumenti finanziari[277].

Sono state ricondotte alla fattispecie in esame le pratiche di *layering* e *spoofing* – trasmissione di più ordini su un lato del *book* di negoziazione, rapidamente annullate, e immediata esecuzione di operazioni di segno opposto –, *pump and dump* – diffusione di informazioni false o fuorvianti per creare una frenesia di acquisto che "pompa" il prezzo di un titolo e successiva dismissione delle azioni tramite vendita delle medesime azioni a prezzo gonfiato –, *marking the close* – operazioni effettuate prima dell'apertura o della chiusura del mercato al solo scopo di influenzare il prezzo del titolo per beneficiarne, tramite acquisto o vendita, alla riapertura delle negoziazioni o su altri mercati.

È di tutta evidenza che tali operazioni di acquisto e vendita "anomale" siano agevolate dalla velocità operativa tipica degli algoritmi di *trading* ad alta frequenza, benché il legislatore italiano – a differenza di quello europeo – non faccia specifico riferimento, nel testo dell'art. 185 t.u.f., al *trading* algoritmico[278].

---

[275] È in questo elemento che si rinviene una componente informativa anche nella c.d. manipolazione operativa, che ha dunque un duplice effetto: "l'uno immediatamente connesso alle dinamiche di formazione del prezzo, l'altro conseguente alle ulteriori operazioni effettuat da altri sulla base delle scelte condizionate dal significato che gli osservatori hanno attribuito all'operazione", F. MUCCIARELLI, *Materialità e offensività*, *op. cit.*, p. 22-23, il quale, nota come la valenza comunicazionale delle operazioni è destinata ad assumere caratteri di maggiore offensività e insidiosità in conseguenza del diffondersi delle negoziazioni algoritmiche ad altissima frequenza e dell'irrompere dell'intelligenza artificiale. Nello stesso senso, ID, A*rt. 185*, in Fratini-Gasparri, Testo unico della finanza, II, Milano, Utet Giuridica,, 2012, pp. 2392-2303 e F. CONSULICH, *La giustizia e il mercato*, 2010, *op. cit*., pp. 41-43.

[276] È il caso dei *wash sales o wash traders*.

[277] Ad esempio, nel caso degli *improper matched orders*.

[278] Alla definizione della negoziazione algoritmica è però dedicato l'art.1, comma 6 *quinquies* t..u.f.: "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

3.5. L'illecito amministrativo di manipolazione del mercato

Come per l'abuso di informazioni privilegiate, anche il divieto di manipolazione del mercato è presidiato da una sanzione amministrativa, prevista dall'art. 187 ter t.u.f., "salve le sanzioni penali quando il fatto costituisce reato", per chiunque violi il divieto di manipolazione del mercato di cui all'articolo 15 del Regolamento MAR[279]. Si tratta – come per l'art. 187 *bis* – di un'infelice scelta del legislatore italiano che, nella volontà di riprendere le ipotesi previste dalla normativa eurounitaria, ha creato una problematica duplicazione, mai davvero risolta, posto che – come affermato dalla Corte costituzionale nel 2022 – non può ritenersi che le norme perseguano scopi complementari o concernano diversi aspetti del comportamento illecito[280].

Proprio in virtù del richiamo al Regolamento MAR, si può ritenere che la fattispecie in questione sia, dal punto di vista oggettivo, del tutto sovrapponibile alla corrispondente fattispecie incriminatrice[281].

Dal punto di vista dell'elemento soggettivo, come l'illecito di cui all'art. 187 *bis*, si tratta di un'ipotesi punibile anche nella forma colposa, conformemente a quanto stabilito dall'art. 3 della l. 689/1981[282]. Secondo una parte della dottrina ciò

---

ordini che non comportano la determinazione di parametri di negoziazione, per confermare ordini o per eseguire il regolamento delle operazioni".

[279] Art.15 Regolamento 2014/596/UE, "non è consentito effettuare manipolazioni di mercato o tentare di effettuare manipolazioni di mercato".

[280] Corte Cost. 16 giugno 2022 (ud. 10 maggio 2022), sentenza n. 149/2022, Pres. Amato, Rel. Viganò con nota di M. SCOLETTA, *Uno più uno anche a Roma può fare due: la illegittimità costituzionale del doppio binario punitivo in materia di diritto d'autore*, in Sist. Pen., 23 giugno 2022. Sul mai risolto problema della compatibilità del sistema italiano con il principio del *ne bis in idem*, cfr *ex multis* M. SCOLETTA, *Il doppio binario sanzionatorio alla luce del vincolo europeo del* ne bis in idem, in F. Consulich (a cura di) Reati in materia finanziaria, Torino, 2024, pp. 297-320; F. VIGANÒ, Ne bis in idem *e pluralità*, *op. cit,* pp. 189-207 ; M. SCOLETTA, *Il principio europeo di* ne bis in idem *e i modelli punitivi "a doppio binario*", in Amalfitano C. - D'Amico M. – Leone S. (a cura di), La Carta dei diritti fondamentali dell'Unione Europa nel sistema integrato di tutela, Torino, 2022, pp. 315-361; F. MUCCIARELLI, *"Doppio binario" sanzionatorio degli abusi di mercato e* ne bis in idem*: prime ricadute pratiche dopo le sentenze della CGUE e la (parziale) riforma domestica*, in Dir. pen. cont., 15 marzo 2019; F. MUCCIARELLI*, La nuova disciplina eurounitaria*, 2015*, op. cit*, pp. 295-324; A. TRIPODI, *Uno più uno (a Strasburgo) fa due. L'Italia condannata per violazione del ne bis in idem in tema di manipolazione del mercato*, in Dir. pen. cont., 9 marzo 2014.

[281] S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*. p. 109 "con la sola eccezione dello *scalping*, per sua natura estraneo alla condotta tipizzata dall'art. 185".

[282] Così A. TRIPODI, *Gli illeciti amministrativi*, *op. cit.*, pp.286-287, che individua "chiari indici della responsabilità per colpa", ad esempio, nel requisito della conoscenza o della conoscibilità del carattere contrario al vero o fuorviante dell'informazione diffusa imposto dall'art. 12, primo comma, lett. c) e d) del Regolamento MAR. Sul punto anche F. D'ALESSANDRO,

varrebbe anche per l'elemento soggettivo, poiché le condotte descritte richiederebbero un coefficiente di consapevolezza che dovrebbe escludere la colpa, nonostante l'illecito amministrativo sia in generale punito indifferentemente a titolo doloso o colposo.

3.6 Profili regolamentari

Le norme dell'ordinamento italiano sin qui citate non si riferiscono mai espressamente alla negoziazione algoritmica.

Ad essa è però espressamente dedicata la rubrica dell'art. 67 *ter* t.u.f., che impone specifici obblighi per s.i.m. e banche che svolgono tale tipologia di *trading*.

La norma riprende in larga parte le fonti europee. Come queste ultime, si tratta di disposizioni che hanno natura prettamente regolatoria, che consentono però di identificare i possibili rischi per l'integrità del mercato derivanti dall'utilizzo di sistemi di negoziazione algoritmica.

Innanzitutto, è fatto obbligo ai soggetti citati di adottare controlli per impedire che i sistemi di negoziazione algoritmica vengano utilizzati per finalità contrarie al Regolamento MAR[283].

È poi prevista l'adozione obbligatoria di "controlli dei sistemi e del rischio volti a garantire che i propri sistemi di negoziazione algoritmica siano resilienti e dispongano di sufficiente capacità, siano soggetti a soglie e limiti di negoziazione appropriati, impediscano di inviare ordini erronei o comunque recare pregiudizio all'ordinato svolgimento delle negoziazioni"[284].

Inoltre, è necessario che chi opera tramite sistemi di negoziazione algoritmica disponga di meccanismi efficaci di continuità operativa per rimediare a malfunzionamenti dei sistemi di negoziazione algoritmica e sottoponga tali meccanismi a un costante monitoraggio[285].

Fattispecie di aggiotaggio e prassi di mercato ammesse, tra esclusione del tipo e cause di giustificazione, in M. Bertolino–L. Eusebi–G. Forti (a cura di), Studi in onore di Mario Romano, Napoli, Jovene, 2011, p.1855 – pur con riferimento alla precedente formulazione – secondo cui può escludersi che i comportamenti descritti dalla fattispecie siano strutturalmente dolosi, potendosi riconoscere uno spazio alla configurabilità di ipotesi colpose specie con riferimento alla manipolazione informativa. In senso contrario, S. SEMINARA, *Diritto penale commerciale*, *op. cit*. p. 119.

[283] Art. 67 *ter*, primo comma, lett. b), t.u.f.

[284] Art. 67 *ter*, primo comma, lett. a), t.u.f.

[285] Art. 67 *ter*, primo comma, lett. c), t.u.f.

Per quanto attiene ai rapporti con le autorità di vigilanza, le s.i.m. e le banche che effettuano negoziazioni algoritmiche devono notificarlo alla Consob (o alla diversa autorità all'autorità competente dello Stato membro della sede di negoziazione in cui effettuano la negoziazione algoritmica quali membri o partecipanti o clienti della sede di negoziazione)[286]. La Consob, o le autorità competenti, possono – nell'ambito della propria attività di vigilanza – richiedere una descrizione della natura delle strategie di negoziazione algoritmica adottate e dettagli sui parametri o sui limiti di negoziazione a cui il sistema è soggetto; nonché effettuare controlli o richiedere informazioni sulle procedure di prevenzione dei rischi adottate dagli operatori[287].

In definitiva, il quadro delle disposizioni applicabili all'attività di *trading* algoritmico in Italia si compone di diverse fonti, anche sovranazionali: i regolamenti e le direttive.

Per quanto il legislatore italiano si sia mostrato meno propenso di quello eurounitario a un esplicito riconoscimento dell'evoluzione tecnologica nei mercati e degli strumenti di *trading* più innovativi, è proprio la legislazione europea a fornire alcuni strumenti utili – nei limiti della gerarchia delle fonti – per disciplinare il fenomeno e i rischi connessi all'emergere di nuovi strumenti tecnologici. In questo senso sono fondamentali le disposizioni del Regolamento MAR e i suoi Regolamenti delegati, in combinato disposto con la Direttiva MiFID II, pur con i limiti dettati dal fatto che la loro approvazione risale ormai un decennio fa.

Proprio sulla base di questi è possibile analizzare la capacità del sistema attuale di contrastare eventuali fenomeni abusivi posti in essere sfruttando algoritmi di

---

[286] Art. 67 *ter*, secondo comma, t.u.f., che recepisce l'art. 17, par. 2, MiFID II. Inoltre,l'art. 48, secondo comma, Regolamento Consob n. 20249/2017 ("RM") dispone che le Sim e le banche italiane comunichino alla Consob, in sede di avvio dell'operatività e in occasione di ogni successivo cambiamento, lo svolgimento di attività di negoziazione algoritmica o l'implementazione di tecniche di negoziazione algoritmica ad alta frequenza, fornendo gli elementi informativi di seguito indicati: a) la data di avvio operatività; b) le sedi di negoziazione su cui si svolge l'attività, identificate da apposito codice MIC; c) la classe degli strumenti finanziari su cui si svolge l'attività; d) l'eventuale svolgimento di attività di negoziazione algoritmica o *hft* tramite DEA al mercato.

Le Sim e le banche italiane che implementano tecniche di negoziazione algoritmica ad alta frequenza trasmettono tempestivamente alla Consob, all'avvio delle stesse, un documento dettagliato in merito all'implementazione di tali tecniche, fornendo gli elementi informativi di seguito indicati: a) il periodo di riferimento delle analisi del traffico infra-giornaliero di messaggi (art. 19, par. 1, del Regolamento Delegato UE 2017/565); b) l'ambito di utilizzo, in termini di mercati e strumenti finanziari, delle tecniche di negoziazione algoritmica ad alta frequenza; c) l'eventuale richiesta alle sedi di negoziazioni di stime dell'operatività, secondo quanto previsto dall'art. 19, par. 5, del Regolamento Delegato UE 2017/565)

[287] Art. 67 *ter*, terzo comma, t.u.f.

trading e sistemi di *trading* basati sull'intelligenza artificiale e di comprendere se il l'integrità dei mercati possa essere – ancora – adeguatamente tutelata con gli strumenti normativi attualmente in vigore.

CAPITOLO III

LA RILEVANZA PENALE DEL *TRADING* ALGORITMICO

SOMMARIO: 1. Il *trading* algoritmico: il necessario punto di partenza del dibattito sul potenziale offensivo dell'intelligenza artificiale – 2. I concetti fondamentali del diritto penale finanziario e l'impatto del *trading* algoritmico: la nozione di informazione e il paradigma dell'investitore ragionevole – 2.1. L'investitore ragionevole – 2.2. L'informazione finanziaria – 2.3. Le necessità di riforma 3. L'agire algoritmico e la sua riconducibilità al 'tipo' – 3.1. Premessa – 3.2. Le condotte astrattamente rilevanti come manipolazioni di mercato – 3.2.1. Il *quote stuffing* – 3.2.2. Lo *smoking*, lo *spoofing*, il *layering* e il *pinging* – 3.2.3. La *liquidity detection* e il *momentum ignition* – 3.2.4. Il *pump and dump*, il *trash and cash* e il *marking the close* – 3.2.5. Le altre condotte potenzialmente abusive – 3.3. Le condotte astrattamente rilevanti come abuso di informazioni privilegiate – 3.4. La riconducibilità alle fattispecie incriminatrici – 4. Le condotte concrete: casistica e simulazioni di mercato – 4.1. Premessa – 4.2. I procedimenti amministrativi: i casi Athena Capital Research LLC, Da Vinci Invest Limited e Paul Axel Walter – 4.3. I procedimenti penali: United States v. Coscia e United States v. Navinder Singh Sarao – 4.4. Gli studi sui mercati simulati – 5. *Trading* algoritmico e *market abuse*: quale sanzione? – 5.1 La prospettiva della responsabilità diretta della 'macchina' – 5.1.1. Gli argomenti a sostegno della responsabilità penale diretta della 'macchina' – 5.1.2. Gli argomenti contrari alla responsabilità penale diretta della 'macchina' – 5.2 La responsabilità penale dell'uomo – 5.2.1. Algoritmi, intelligenza artificiale e la prospettiva del rischio – 5.2.2. Il *trading* algoritmico come attività a rischio consentito – 5.2.3. I confini del *trading* algoritmico consentito: i doveri di organizzazione e controllo delle sedi di negoziazione e di chi svolge l'attività – 6. Gli 'abusi di mercato algoritmici': i principali profili di problematicità – 7. Gli 'abusi di mercato algoritmici': l'utilizzo di sistemi di negoziazione algoritmica 'tradizionali' – 7.1. Gli 'abusi di mercato algoritmici tradizionali: il primo scenario – 7.2. Gli 'abusi di mercato algoritmici tradizionali: il secondo scenario – 8. I sistemi di negoziazione algoritmica basati su sistemi di intelligenza artificiale 'forte' – 8.1. I sistemi di intelligenza artificiale forte e la crisi delle categorie tradizionali del diritto penale – 8.2. La crisi del diritto penale d'evento e le specificità degli 'abusi di mercato algoritmici' – 8.3. Sistemi di intelligenza artificiale 'forte' e gli 'abusi di mercato algoritmici': primo scenario – 8.4. Sistemi di intelligenza artificiale 'forte' e gli 'abusi di mercato algoritmici': secondo scenario – 8.5. Sistemi di intelligenza artificiale 'forte' e gli 'abusi di

mercato algoritmici': terzo scenario – 8.5.1. I limiti del rischio consentito: il fallimento delle regole cautelari che disciplinano l'attività – 8.5.2. L'incertezza scientifica – 8.5.3. La ridefinizione legislativa dell'area di rischio consentito.

1. Il *trading* algoritmico: il necessario punto di partenza del dibattito sul potenziale offensivo dell'intelligenza artificiale

Sin qui si è descritto il funzionamento dei sistemi di negoziazione finanziaria automatizzata.

Tali strumenti possono portare significativi benefici in termini di efficienza e di aumento di liquidità, ma allo stesso tempo, il loro impiego può determinare il turbamento del buon andamento dei mercati finanziari e della corretta formazione dei prezzi degli strumenti finanziari[288]. Per questa ragione il legislatore eurounitario e nazionale sono ormai da anni impegnati nel regolarne l'uso.

In particolare, il rischio è che i sistemi di *trading* algoritmico possano essere coinvolti nella commissione di abusi di mercato, aprendo a scenari inediti capaci – secondo una parte della dottrina – di mettere in discussione la tenuta dell'attuale sistema sanzionatorio[289].

---

[288] Quanto agli effetti positivi sull'efficienza dei mercati, O. COSME JR., *Regulating High-Frequency Trading*, 2019, *op. cit.* p. 370 sottolinea che il ricorso al *trading* algoritmico può essere, da un lato, molto redditizio per il *trader* e per la società di *trading* e dall'altro lato molto vantaggioso per i mercati perché contribuisce a colmare i divari tra mercati e aumentare la liquidità. Ciò determina un attenuarsi delle oscillazioni dei prezzi e una riduzione dei costi di transazione. Inoltre, l'aumento della liquidità derivante dall'operare di *trader* algoritmici aumenta la disponibilità a effettuare transazioni degli intermediari che comprano e vendono titoli per conto proprio (*market maker*), meccanismo che a sua volta aumenta ulteriormente la liquidità e il volume degli scambi. In ambito italiano, sugli effetti sulla volatilità dei rendimenti giornalieri dei trentacinque titoli a maggiore capitalizzazione: V. CAIVANO, *L'impatto del* trading *ad alta frequenza sulla volatilità. Evidenza empirica sul mercato italiano*, in Quaderno di finanza Consob n. 80, marzo 2015.

[289] Così F. CONSULICH–M. MAUGERI–C. MILIA–T.N. POLI–G. TROVATORE, *AI e abusi di mercato*, *op. cit.*, p. 33; nonché M. DE FELICE, *Decisione robotica negoziale. Nuovi «punti di presa» sul futuro*, in A. Carleo (a cura di), Decisione robotica, Bologna, Il Mulino, 2019, p. 192; C. MOTTURA, *Decisione robotica negoziale e mercati finanziari*, in A. Carleo, Decisione robotica, Bologna, 2019, pp. 265-289.

Come rileva C. PIERGALLINI, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato*, in Riv. it. dir. proc. pen., 2020, fasc. 4, p. 1743 le applicazioni di intelligenza artificiale "per un verso sono strumenti in grado di salvare vite umane; per altro verso, possono convogliare gravi danni". Di fronte a questo secondo scenario, l'Autore evidenzia una crisi del dominio umano sul danno da prodotto e sintetizza la questione in questi termini: "se le macchine dimostrano di poter apprendere dall'esperienza, assumendo decisioni sconosciute e imprevedibili, chi dovrà rispondere di eventuali danni? (…) Chi potrà e dovrà essere considerato autore dell'illecito?".

Si tratta di un dibattito, quello del coinvolgimento delle 'macchine' nella commissione dei reati, che non è certo limitato ai confini dei reati finanziari, ma che interessa importanti settori della vita umana in modo diffuso[290].

Tuttavia, quello finanziario pare essere un ambito particolarmente privilegiato per svolgere alcune considerazioni sulla responsabilità penale 'per il fatto dell'algoritmo', dal momento che si tratta di un settore in cui da tempo si fa un ampio uso – anche illecito – di sistemi automatizzati per le negoziazioni e considerato l'impatto che un fatto illecito posto in essere dal *trader* algoritmico può avere sull'integrità dei mercati[291]. Benché questa nuova ipotetica forma abbia sostanzialmente lo stesso obiettivo della sua controparte tradizionale, essa può avere una portata offensiva incommensurabilmente maggiore, a causa dei volumi e della interconnessione che caratterizzano i mercati finanziari moderni[292].

Di fronte alla mutata realtà, il tema dell'adeguatezza dell'attuale sistema normativo nel contrasto agli 'abusi di mercato algoritmici' impone di analizzare alcuni aspetti essenziali.

Innanzitutto, occorre valutare se l'introduzione dei sistemi di negoziazione algoritmica influisca su alcuni concetti fondamentali del diritto penale finanziario: la nozione di informazione finanziaria e di investitore ragionevole.

Il secondo aspetto su cui si si concentrerà è poi la riconducibilità delle strategie di *trading* realizzate da o tramite algoritmi fattispecie incriminatrici attualmente vigenti, nella loro componente oggettiva.

Mentre il terzo oggetto di indagine riguarda l'individuazione del soggetto responsabile di tali illeciti.

2. I concetti fondamentali del diritto penale finanziario e l'impatto del *trading* algoritmico: la nozione di informazione e il paradigma dell'investitore ragionevole

Prima di analizzare gli aspetti che attengono alla configurabilità degli abusi di mercato tramite (o 'da parte' di) algoritmi di *trading* e i relativi problemi in ordine

---

[290] Ci si riferisce alle auto a guida autonoma, alle diverse applicazioni dell'AI in ambito medico-chirurgico e, nel settore finanziario, alle applicazioni di intelligenza artificiale usate per la consulenza finanziaria (*robo-advice*) e la valutazione del merito creditizio (*credit-score*).
Tuttavia, come rileva, F. CONSULICH, *Intelligenza artificiale e reati finanziari*, *op. cit.*, p. 241 "tra i vari settori in cui l'intelligenza artificiale gioca un ruolo, quello della finanza è un campo in cui il legislatore ha maggiormente esplicato la propria *vis normativa* (anche se certamente non è l'unico)".

[291] Cfr. F. CONSULICH, Flash offenders, *op. cit.*, p. 1018.

[292] T.C.W. LIN, *The New Market Manipulation*, op*. cit.*, 2017, pp. 1287-1293.

alla responsabilità, occorre concentrarsi sulla capacità di tali sistemi di mutare i caratteri di alcuni concetti fondamentali del diritto penale finanziario.
È, cioè, necessario interrogarsi sull'influenza esercitata dai nuovi 'soggetti' e dai più progrediti strumenti sulla nozione di 'informazione finanziaria' e sul paradigma dell'investitore ragionevole, concetti attorno ai quali ruotano le fattispecie oggetto del presente lavoro.

Come noto, la portata offensiva delle condotte di abuso di mercato – che si tratti del compimento di un'operazione simulata o artificiosa, della diffusione di notizie false o fuorviati o della comunicazione decettiva che l'operazione simulata o artificiosa trasmetta di se stessa[293] o dell'abuso di informazioni privilegiate – ruota attorno all'influenza che tali comportamenti hanno rispetto a determinati soggetti che "proprio a cagione della falsa/fuorviante informazione ricevuta, vengono a disporre di un patrimonio conoscitivo alterato, sulla base del quale compiono le scelte di investimento attraverso le quali i concretizza il pericolo per il bene giuridico protetto"[294].
Le due nozioni di 'informazione' – decettiva per la fattispecie di cui all'art. 185 t.u.f. e privilegiata per l'ipotesi di cui all'art. 184 t.u.f. – pur distinte dal fatto che solo l'informazione privilegiata di cui all'art. 184 t.u.f. deve assumere i caratteri della non pubblicità e riservatezza previsti dall'art. 7 del Regolamento MAR, sono tuttavia accomunate, come sostenuto da autorevole dottrina, dal requisito della "significatività dell'effetto che l'informazione deve potrebbe avere «sui prezzi di (…) strumenti finanziari o su prezzi di strumenti finanziari collegati» (secondo la dizione dell'art. 7 co.1 lett. a) MAR). *Effetto significativo* sul prezzo è infatti nozione che concettualmente rimanda a quella di *alterazione sensibile*, espressive entrambe di una conseguenza modificativa sul medesimo oggetto (il prezzo dello strumento finanziario)"[295].

---

[293] Cfr., da ultimo, F. MUCCIARELLI, *Materialità e offensività*, *op. cit.* p. 2.

[294] Così F. MUCCIARELLI, *Materialità e offensività*, *op. cit.* p. 3 e p. 16 il quale rileva come "nello schema della manipolazione del mercato […] è il trasferimento dell'informazione decettiva a integrare lo snodo cruciale, poiché determina (quando la decettività dell'informazione sia idonea) una condizione di errore in conseguenza della quale il destinatario si forma (anche in questo caso) una falsa rappresentazione di quella frazione di realtà oggetto dell'inganno".

[295] Così F. MUCCIARELLI, *Materialità e offensività*, *op. cit.* p. 19 e in termini analoghi ID, *Gli illeciti di abuso di mercato*, op. cit., p. 823. L'Autore precisa inoltre che l'effetto che l'informazione ha sul prezzo, sia nell'abuso di informazioni privilegiate, sia nella manipolazione di mercato è indiretto, posto che non è tanto l'informazione a influire sul prezzo, ma l'operazione che viene compiuta sulla base dell'informazione stessa. Una conferma di ciò si rinviene, secondo l'Autore, nel quarto comma dell'art. 7 Regolamento MAR, che considera l'informazione alla stregua di un fattore concausale all'interno del processo decisionale.

Ciò comporta che proprio la direzione verso i soggetti destinatari e l'attitudine a essere utilizzata come uno degli elementi su cui basare le proprie decisioni di investimento sono fattori capaci di definire i confini dell'offensività e, dunque, dell'illiceità dei comportamenti in questione[296].
La nozione di informazione finanziaria e il concetto di investitore ragionevole sono dunque indissolubilmente legate l'una all'altra.
È infatti guardando all'investitore ragionevole che si comprende la rilevanza o meno dell'informazione e la sua capacità di influire sulle decisioni di investimento[297].

2.1. L'investitore ragionevole

Ebbene, nonostante l'idoneità a influire sui prezzi degli strumenti finanziari dipenda dal tipo di investitore collocato nel contesto, l'identificazione di una definizione certa di 'investitore ragionevole' ha suscitato grande attenzione da parte della dottrina[298], tanto da far ritenere che più correttamente si dovrebbe parlare di molteplici categorie di investitori ragionevoli, titolari di legittimi interessi

[296] Come nota, F. MUCCIARELLI, *Materialità e offensività*, *op. cit.* p. 19 "se l'informazione decettiva non importa la probabilità – valutata *ex ante* – che il destinatario compia un'operazione, l'informazione, pur decettiva, non è tipica".

[297] Cfr. F. MUCCIARELLI, *Materialità e offensività*, *op. cit.* p. 37 "concentrare l'attenzione sull'investitore/operatore è […] funzionale allo scopo di individuare con sufficiente precisione e determinatezza i connotati del parametro essenziale della idoneità alterativa in misura sensibile. […] l'*investitore ragionevole*, di cui discorre l'art. 7 MAR, sembra divenire parametro di riferimento che promette qualche proficuo sviluppo per cogliere il significato preciso della nozione di informazione […] in concreto idonea a influenzare in misura sensibile il prezzo dello strumento finanziario". Sul punto anche S. SEMINARA, *Diritto penale commerciale*, p. 72.

[298] F. CONSULICH–F. MUCCIARELLI, *Informazione e tutela penale dei mercati finanziari nello specchio della normativa eurounitaria sugli abusi di mercato*, in Le Società, 2016, fasc. 2, pp. 179-191; S. SEMINARA, *L'informazione privilegiata*, in M. Cera–G. Presti (a cura di), Il testo unico finanziario, Vol. II, Bologna, Zanichelli, pp. 2149-2152; F. SGUBBI, *Abusi di mercato*, in *Enc. Giur.*, Annali II, Tomo II, Milano, 2009, p. 20; V. NAPOLEONI, *L'*insider trading, *op. cit.*, p. 690; AMATI, *L'abuso o comunicazione illecita di informazioni privilegiate*, in N. Mazzacuva–E. Amati (a cura di), Diritto penale dell'economia, VI ed., Milano, Wolters Kluwer, 2023, p. 356 ss.; nonché ID, *L'abuso o comunicazione illecita di informazioni privilegiate*, in F. Consulich (a cura di), Reati in materia bancaria e finanziaria, Torino, Giappichelli, 2024, pp. 173-174. In ambito americano, dove trova vita la nozione di *reasonable investor*, si è svolto lo stesso dibattito, sul quale si veda, per tutti, T.C.W. LIN, *Reasonable Investor(s),* in Boston University Law Review pp. 461-518, in particolare sulla distinzione fra reasonable investor, irrational Investor, active anvestor, sophisticated investor ed entity Investor, nonché ID, *The new Investor*, *op. cit.*, *passim*.

differenti, in funzione delle differenti capacità di lettura, comprensione e interpretazione delle informazioni di cui sono destinatari[299].

Fra i diversi partecipanti al mercato si possono infatti individuare varie figure: singoli investitori che impiegano le proprie disponibilità finanziarie, soggetti dotati di personalità giuridica, intermediari, investitori istituzionali, *market maker*, fondi speculativi, e altri, tutte figure portatrici di interessi e aspettative estremamente distanti fra di loro e talvolta confliggenti.

Tale platea è, inoltre, destinata a un significativo ampliamento e mutamento, proprio in ragione dell'operatività sui mercati dei *trader* algoritmici.

Le proprietà di questi ultimi possono infatti influire in modo assai significativo sui caratteri dell'investitore ragionevole, oltre che sul concetto di informazione finanziaria.

In merito, occorre tenere presente che la logica seguita dai *trader* algoritmici spesso non ricalca quella umana e che essi reagiscono a *input* diversi da quelli tradizionalmente considerati dai *trader* umani e che per questi ultimi potrebbero risultare del tutto irrilevanti ai fini della decisione di investimento. Si pensi ad esempio alle oscillazioni minime nel valore di un titolo o al numero di volte in cui il nome di un dato titolo compare nei circuiti di diffusione di informazioni e sulle

---

[299] Anche tenuto conto del fatto che il ruolo di risparmiatore non è assunto esclusivamente da addetti ai lavori, come nota A. ALESSANDRI, *Diritto penale e attività economiche*, Bologna, Il Mulino, 2010, p. 292.

Le diverse teorie elaborate possono essere sintetizzate come segue:

i. Investitore ragionevole come investitore modello.
   Teoria a cui sono state mosse alcune significative critiche, fra cui il riferirsi alle sole ipotesi di responsabilità colposa e il fatto di portare a configurare l'investitore ragionevole 'modello' come il più sprovveduto dei partecipanti al mercato contrariamente al dato normativo che con l'aggettivo 'ragionevole' ha voluto riferirsi a un soggetto dotato di competenze e conoscenze superiori a quelle di un investitore non avvertito.
ii. Investitore ragionevole come lettore esperto, dotato di un bagaglio di conoscenze adeguato alla effettiva comprensione dell'informazione e elle norme di riferimento (in questo senso si esprimono F. D'ALESSANDRO, *Le false valutazioni al vaglio delle Sezioni Unite: la nomofilachia, la legalità e il dialogo interdisciplinare*, in Cass. Pen., 2016, fasc. 7-8, p. 2805; A. ALESSANDRI, *Diritto penale e attività*, *op. cit.*, p. 292 e V. NAPOLEONI, L'*insider trading*, *op. cit.*, pp. 690-691.
iii. Investitore ragionevole come persona ragionevole, dotata di medie competenze (tesi sostenuta da S. SEMINARA, *La riforma dei reati di false comunicazioni sociali*, Dir. pen. proc., 2015, fasc. 7, pp. 813-824.
iv. Investitore ragionevole come investitore sprovveduto, adottata soprattutto da alcuna giurisprudenza di merito e analizzata in senso critico da F. MUCCIARELLI, *Materialità e offensività*, *op. cit.*, p. 47.

piattaforme di comunicazione: dati estremamente rilevanti per l'operatore algoritmico e per lo più non considerati dall'umano[300].

A ciò si aggiunge una componente che la dottrina ha definito di "ingenuità", che sommata alla grande capacità operativa, "li rende, da una parte, facili prede di speculatori che possono indurli a compiere colossali transazioni sulla base di informazioni errate, dall'altro lato, essi stessi, se non adeguatamente sorvegliati, possono turbare il mercato, tenendo comportamenti fuorvianti per gli altri investitori (ad esempio, innescando acquisti incrociati, lo schiacciamento delle controparti nel campo dei derivati, e così via)"[301].

L'estensione della platea dei soggetti che operano sui mercati ai *trader* algoritmici, che agiscono in modo così distante dagli altri soggetti già citati, inserisce dunque un ulteriore tassello nel già eterogeneo mosaico definitorio del paradigma dell'investitore ragionevole.

Detto ampliamento costituisce dunque un'ulteriore conferma della necessità – quantomeno *de iure condito* – di guardare al paradigma dell'investitore ragionevole come una sineddoche che, anziché alludere ad un modello specifico, contiene in sé il riferimento a diverse categorie[302].

2.2. L'informazione finanziaria

Le considerazioni svolte sin qui influenzano, poi, necessariamente anche i 'confini' del concetto di informazione finanziaria, intesa come il dato che l'investitore ragionevole pone a fondamento delle proprie decisioni di investimento.

Come anticipato, l'operatore algoritmico basa le proprie decisioni finanziarie – che esegue con estrema rapidità[303] – su sempre più informazioni che, "inutili per

---

[300] Si veda in questo senso G. STRAMPELLI, *L'informazione societaria a quindici anni dal t.u.f.: profili evolutivi e problemi*, in Riv. Soc., 2014, fasc. 5, p. 993.

[301] Così F. CONSULICH, *Manipolazione del mercato e declino del sistema finanziario. Spunti di riflessione a margine del ventesimo anniversario dell'avvio del processo Parmalat*, in Sist. Pen., 4 settembre 2024, p. 17.

[302] Come notano F. CONSULICH–M. MAUGERI–C. MILIA–T.N. POLI–G. TROVATORE, *AI e abusi di mercato*, *op. cit.*, pp. 73-74 "lo scenario, già di per sé assai problematico, è ulteriormente stressato dal crescente ruolo rivestito negli ultimi anni dagli operatori algoritmici […] tali soggetti possono, al pari degli esseri umani, essere molto eterogenei tra loro per obiettivi perseguiti, conoscenze iniziali e competenze specifiche".

[303] Questo ha portato una parte della dottrina a ipotizzare soluzioni volte sia a rallentare l'attività degli *high frequency trader* tramite i c.d. *speed bumps*, sia a segmentare l'accesso alle informazioni privilegiate, ritardando quello degli *high frequency trader*. Si tratta, tuttavia, di ipotesi

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"[304]. La conseguenza diretta di questo fenomeno è l'estensione del concetto fino a ricomprendere le informazioni che sono in grado di influenzare i prezzi nell'ottica di un singolo operatore o per una minoranza di operatori, ma non anche per la maggioranza degli investitori.

Tale fenomeno influisce indubbiamente anche sulla capacità comunicativa ai mercati delle operazioni effettuate dagli operatori algoritmici: una parte della dottrina ritiene infatti che, vista la tendenza dei *trader* algoritmici a sfruttare minime oscillazioni sui prezzi degli strumenti finanziari e lucrare sull'anticipazione di questi movimenti minimi, qualsiasi operazione compiuta in ragione di queste sarebbe invero del tutto inconferente rispetto alle variabili economiche rilevanti per un operatore professionale. Ciò comporterebbe lo svuotamento della componente informativa delle operazioni compiute da tali operatori poiché non veicolerebbero alcun dato rilevante in ordine al valore intrinseco dei titoli oggetto di scambio o all'andamento del mercato[305].

Inoltre, l'utilizzo di sistemi di negoziazione algoritmica può determinare anche il mutamento del concetto di informazione privilegiata.

Sono diverse le informazioni che possono assumere il carattere di riservatezza e non pubblicità e che possono essere oggetto di abuso. Si pensi all'attacco *cyber* che inibisca l'operatività di altri operatori di mercato e che sia sfruttato dall'algoritmo di *trading* prima che la notizia dell'attacco venga diffusa; o al possibile sfruttamento da parte del sistema di negoziazione algoritmica prima dei destinatari delle raccomandazioni di investimento generate da *robo-advisor* o ancora nello sfruttamento o nella raccomandazione di investimento basati su

---

che pongono alcuni problemi di compatibilità con i principi generali, di equo accesso alle informazioni e di parità di trattamento, che ispirano la disciplina europea degli abusi di mercato, e di gestione e diffusione delle informazioni *price-sensitive* Sul punto, F. ANNUNZIATA, *I processi di mercato automatizzati*, *op. cit.*, p. 406 e F. PASQUALE, *Law's Acceleration of Finance: Redefining the Problem of High-Frequency Trading*, in University of Maryland Francis King Carey School of Law Legal Studies Research Paper, 2015, vol. 29, pp. 2085-2127.

[304] Così F. CONSULICH–M. MAUGERI–C. MILIA–T.N. POLI–G. TROVATORE, *AI e abusi di mercato*, *op. cit.*, p. 74, che notano come il fenomeno della proliferazione delle informazioni *price sensitive* sia già stato posto a livello globale con l'ascesa degli *hedge fund*, con la conseguenza che sia negli Stati Uniti che nell'Unione europea, si è scelto di obbligare le società alla *fair disclosure*.

[305] In questo senso, F. CONSULICH–M. MAUGERI–C. MILIA–T.N. POLI–G. TROVATORE, *AI e abusi di mercato*, *op. cit.*, p. 77, nonché A. PUORRO, *High frequency trading*, *op. cit.*, p. 16.

informazioni tratte dall'elaborazione di *big data*, inaccessibili alla maggior parte del pubblico in ragione degli ingenti costi dei sistemi necessari ad acquisirli[306].

2.3. Le necessità di riforma

Il mutamento dei concetti fondamentali del diritto finanziario, per come sin qui descritto, è alla base delle istanze di riforma avanzate da una parte della dottrina[307], che sostiene la necessità di tenere conto della "difficoltà di adottare una nozione onnicomprensiva di investitore ragionevole"[308] e della "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 […] e ii) del progressivo prevalere dell'operatività dei sistemi di AI nei mercati finanziari"[309].

La presenza sul mercato dei *trader* algoritmici imporrebbe infatti di ripensare l'attuale sistema normativo, tenendo conto del mutare dei 'soggetti' operanti sui mercati, nonché delle nuove asimmetrie informative, che il più evoluto apparato tecnologico a disposizione degli operatori comporta[310].

Il ripensamento delle categorie sin qui illustrate, così come la soluzione alle problematiche che verranno affrontate nel prosieguo, non può che prendere avvio dalla necessità di tutelare il corretto funzionamento del mercato, considerate le diverse categorie di chi in questo contesto opera.

In questo senso pare pienamente condivisibile, anche nella prospettiva dell'evoluzione tecnologica che ha caratterizzato i mercati nell'ultimo decennio, il monito della dottrina in merito ai tentativi di definire contenutisticamente la figura

---

[306] Si tratta di ipotesi che verranno approfondite *infra*.

[307] Ipotesi *de lege ferenda* che tengono conto della funzione di protezione degli investitori deboli e di riduzione delle asimmetrie informative propria della disciplina dell'informazione societaria e, con particolare riferimento al settore penalistico, alle norme in materia di *insider trading.*

[308] F. CONSULICH–M. MAUGERI–C. MILIA–T.N. POLI–G. TROVATORE, *AI e abusi di mercato*, *op. cit.*, p. 78. Sul punto F. MUCCIARELLI, *Materialità e offensività*, *op. cit.* p. 70 rileva che "la figura dell'investitore ragionevole non può essere definita contenutisticamente cercando di mediare le caratteristiche pro proprie delle varie categorie (e dei rispettivi sottoinsiemi), nelle quali i partecipanti al mercato possono essere raggruppati in ragione delle loro differenti abilità linguistiche nonché dei loro plurimi e differenti interessi e delle conseguentemente plurime e differenti aspettative ed esigenze sul piano informativo".

[309] F. CONSULICH–M. MAUGERI–C. MILIA–T.N. POLI–G. TROVATORE, *AI e abusi di mercato*, *op. cit.*, p. 78.

dell'investitore ragionevole come sintesi delle "caratteristiche proprie delle varie categorie (e dei rispettivi sottoinsiemi), nelle quali i partecipanti al mercato possono essere raggruppati […], in ragione dei loro plurimi e differenti interessi e delle conseguentemente plurime e differenti aspettative ed esigenze sul piano informativo"[311]. Tale mediazione finirebbe infatti per far prevalere gli interessi, le aspettative e le esigenze di una categoria, tradendo la dimensione pubblicistica della tutela del mercato finanziario[312], che – anzi – funziona correttamente solo qualora ciascuno assumere decisioni di investimento in modo consapevole e informato.

3. L'agire algoritmico e la sua riconducibilità al 'tipo'

3.1. Premessa

Nell'ambito dell'indagine sulla rilevanza penale del *trading* algoritmico, il primo quesito che si pone è innanzitutto se l'algoritmo sia effettivamente grado di porre in essere, se non agevolare, il fatto di reato nella sua componente oggettiva.

Si tratta di stabilire, cioè, se l'azione degli algoritmi di *trading* sia riconducibile alla componente oggettiva degli illeciti di *market abuse*.

Invero, proprio con riferimento all'elemento oggettivo del reato, una parte della dottrina ha rilevato il rischio di una crisi della fattispecie penale nella compiuta

---

[311] Così F. MUCCIARELLI, *Materialità e offensività*, *op. cit.* p. 70. L'Autore sottolinea come una simile opera di mediazione, oltre che essere intrinsecamente difficoltosa – se non impossibile qualora gli interessi siano confliggenti – finirebbe per imporre la prevalenza dell'interesse, delle aspettative e delle esigenze di una categoria sulle altre e, a prescindere dai profili di arbitrarietà che tale scelta assumerebbe, sarebbe una scelta incoerente con le esigenze di tutela del mercato, "la cui dimensione pubblicistica (o, comunque, metaindividuale) è incompatibile con una soluzione di disciplina che, privilegiando gli interessi di una categoria, comprometterebbe quelli delle altre, rappresentative di tutti gli altri partecipanti al mercato".

[312] Altrettanto insoddisfacente sarebbe, d'altra parte, un'astrazione della figura che prenda avvio dall'individuazione delle funzioni da assegnare all'archetipo dell'investitore ragionevole. In questo senso, F. MUCCIARELLI, *Materialità e offensività*, *op. cit.* p. 70. L'Autore propone, al contrario, di valorizzare la natura strumentale del "referente linguistico" investitore ragionevole per l'individuazione dell'informazione rilevante e non viceversa. A tal fine, secondo l'Autore, si possono valorizzare elementi comuni a tutte le tipologie di investitori. In primo luogo, il fatto che indipendentemente dalla tipologia dell'informazione e dalle modalità della sua veicolazione, essa influisce, alterandolo, sul patrimonio conoscitivo di ciascuno (posto che l'investitore ragionevole è colui che compie scelte *in modo* ragionevole, ossia basandosi su un patrimonio conoscitivo adeguato e coerente, nei limiti dello stesso e delle proprie abilità). In secondo luogo, il fatto che l'informazione influisca, mutandola, nel processo cognitivo che conduce alla decisione di investimento.

descrizione della condotta tipica e di una difficoltà di ricondurre al concetto penalistico di 'azione' le condotte dematerializzate degli algoritmi[313].
Pur nella loro suggestività, questi rilievi mancano di considerare che, per quanto in modo 'dematerializzate', l'operare dell'algoritmo è dotato di una oggettiva rilevabilità nel mondo esterno[314] ed è dunque riconducibile al concetto penalistico di 'azione', come si vedrà nel prosieguo.

3.2. Le condotte astrattamente rilevanti come manipolazioni di mercato

Come noto, il ricorso al *trading* algoritmico non costituisce di per sé una forma di abuso di mercato[315], ciononostante talvolta alcune strategie che esso

---

[313] L'azione solo virtuale dei *software* non sarebbe, secondo questa impostazione, riconducibile al paradigma penalistico classico, fondato su movimenti fisici capaci di modificare il mondo esterno, salvo non voler aderire ad impostazioni materialistiche del fatto tipico. M. E. FLORIO, *Il dibattito sulla responsabilità penale diretta delle i.a.: "molto rumore per nulla"?*, Sist. pen., 2024, fasc. 2, p. 12, – nell'ambito del dibattito sull'ammissibilità di una responsabilità diretta dell'i.a. – nota che l'agire delle intelligenze artificiali potrebbero essere ricondotte al concetto penalistico di azione solo adottando una "una concezione 'meccanicistica' di azione, ignorando le conquiste teoriche delle dottrine finalistiche post-welzeliane25: per coloro che in materia di diritto penale sostengono concetti più ambiziosi di azione, in cui si presuppone una particella di "spirito" (*Geist*), una coscienza rudimentale o un qualche tipo di vita interiore, l'idea di una macchina che agisce sarebbe probabilmente considerata come una vera e propria *contradictio in termini"*.

[314] L. PICOTTI, *Categorie tradizionali del diritto penale e intelligenza artificiale: crisi o palingenesi? Le raccomandazioni dell'Association Internationale de Droit Pénal e la rilevanza del recente regolamento europeo sull'intelligenza artificiale*, in Sist. Pen., 31 luglio 2024, p. 4 che, ricostruita l'evoluzione del concetto penalistico di 'azione' dalla nozione naturalistico-causale, passando per la nozione finalistico-personalistica, fino alla nozione c.d. sociale, auspica un ulteriore sviluppo del concetto di azione capace di abbracciare l'apporto delle nuove tecnologie, vista la potenziale capacità di causare "lesioni a beni giuridicamente protetti dal diritto penale, che non si presenta però quale diretta estrinsecazione di movimenti né di concrete decisioni di una determinata persona umana". Sul concetto di 'azione' nel diritto penale, si rinvia, per tutti, a G. FIANDACA–E. MUSCO, *Diritto penale*, *op. cit*., pp. 232-233.

[315] F. ANNUNZIATA, *I processi di mercato automatizzati e il trading algoritmico*, in M. Cian–C. Sandei, Diritto del Fintech, Milano, Wolters Kluwer, 2020, p. 406 sottolinea come "le questioni che sollevano le tecniche di negoziazione algoritmica vanno anche indagate sul piano del loro rapporto con la disciplina sugli abusi di mercato (ora contenuta nel reg. 2014/596/UE - Market Abuse Regulation "MAR"). Sebbene le tecniche di negoziazione algoritmiche, soprattutto quelle ad alta frequenza, possano apparire idonee a destabilizzare i normali meccanismi di funzionamento del mercato, anche in questo caso l'impostazione più correttamente adottata dal legislatore europeo è stata nel senso di rifuggire da semplificazioni eccessive. Si ritiene, dunque, che le negoziazioni algoritmiche e ad alta frequenza non siano, di per sé, abusive (il che, peraltro, sarebbe in contrasto anche con le opzioni legislative adottate dalla stessa MiFID II); tuttavia, il riferimento alle tecniche di cui si discute e, in particolare, a quelle ad alta frequenza, è stato espressamente incluso – a guisa di "sottolineatura" - nella definizione dei possibili casi di manipolazione del mercato accanto ad altri".

consente di realizzare sono idonee a ostacolare il corretto funzionamento dei mercati e la formazione dei prezzi.

L'elevata velocità, l'enorme potenza operativa dei sistemi di *trading* algoritmico, nonché l'atteggiamento particolarmente 'aggressivo' possono infatti favorire la commissione di comportamenti illeciti, riconducibili alla manipolazione del mercato e all'abuso di informazioni privilegiate[316].

Talvolta le nuove tecnologie – si tratti di algoritmi 'classici' o basati su intelligenza artificiale – creano l'occasione per realizzare condotte abusive inedite, mentre in altri casi i sistemi automatizzati sono solo strumenti nuovi per attuare schemi illeciti antichi.

Si pensi innanzitutto alla manipolazione del mercato[317].

Alcuni schemi potenzialmente manipolatori sono particolarmente congeniali all'operatività degli algoritmi di *trading* poiché presuppongono e ne sfruttano l'enorme potenza di calcolo e la velocità di invio, consentendo di creare l'apparenza di un movimento di mercato.

In particolare, si possono considerare abusive le strategie basate sull'immissione di ordini di acquisto o vendita simultanei sul mercato e la successiva, rapida, cancellazione degli ordini sul lato del mercato che porterebbe a perdite, mantenendo e completando gli ordini sull'altro lato del mercato che è favorevole al movimento dei prezzi, assicurando così profitti.

---

[316] Ad esempio, *l'high frequency trading*, ha un potere di influenza sui prezzi, che può essere usato anche a scopo 'predatorio'. Si immagini uno scenario in cui un investitore tradizionale intenda inviare un ordine di acquisto per 50.000 euro, acquistando 1000 azioni a 50 euro. 500 azioni del titolo sono offerte su NASDAQ, 300 azioni sul NYSE, e 200 azioni sul BATS Global Exchange. Il sistema di *high frequency trading* è in grado di rialzare il prezzo, notando una prima parte dell'ordine su una borsa, registrando l'interesse di un altro soggetto all'acquisto del titolo e quindi acquistando il titolo e offrendolo al soggetto interessato a un prezzo più alto (rispetto ai 50 euro che aveva previsto), quando la sua offerta raggiunge la seconda borsa. Sicché il *trader* tradizionale ha solo due opzioni: accontentarsi di un numero di azioni inferiori a 1000 o finalizzare l'ordine a un prezzo più alto.

La condotta descritta di per sé non presenta profili di illiceità. Tuttavia, se l'*high frequency trader* sfruttasse in modo predatorio la propria capacità di acquistare e vendere i titoli più rapidamente degli investitori tradizionali, potrebbe determinare un aumento o una diminuzione artificiale dei prezzi, facendo sì che il prezzo di un titolo si muova in modo significativo, determinando così una perdita significativa di denaro per gli altri operatori.

[317] F. CONSULICH, *Intelligenza artificiale e reati finanziari*, *op. cit.*, p. 241 "il delitto che per antonomasia che può essere perpetrato per mezzo (e non già) dell'intelligenza artificiale è la manipolazione del mercato". D'altra parte, come nota lo stesso Autore precedentemente in F. CONSULICH, Flash offenders, *op. cit.*, p. 1018, "non vi sono illeciti economicamente motivati che si sottraggono per principio all'azione di AI come mezzo di commissione".

Rispondono a questo schema alcune pratiche diffuse sui mercati negli ultimi anni, quali il *quote stuffing*, lo *smoking*, lo *spoofing*, il *layering,* il *pinging*, la *liquidity detection*, il *momentum ignition*, il *pump and dump*, il *trash and cash* e il *markin the close*[318].
Esse possono essere descritte, tentando una tassonomia, come segue.

3.2.1. Il quote stuffing

Il *quote stuffing* consiste nell'immissione e contestuale cancellazione di un elevato numero di ordini sul mercato, tanto da congestionare e compromettere l'accesso al mercato da parte degli *slow trader* a favore dei *trader* algoritmici. La situazione di congestione determina, da un lato, la perdita di una visione chiara di ciò che accade sul *book* di negoziazione e, dall'altro lato, un'inefficienza operativa nei sistemi di abbinamento domanda e offerta che favorisce divergenze di prezzo sui titoli (arbitraggi di latenza), che i *trader* algoritmici – specie quelli ad alta frequenza – sono in grado di sfruttare a proprio vantaggio.
di indurre gli altri *trader* ad effettuare determinate operazioni in reazione a tali situazioni di mercato[319].

3.2.2. Lo smoking*, lo* spoofing*, il* layering *e il* pinging

Lo *smoking*, lo *spoofing*, il *layering* e il *pinging* sono invece strategie che prevedono l'immissione massiva di ordini al mercato, modificandoli e cancellandoli continuamente e simulando quindi situazioni di mercato allo scopo
Lo *smoking* si realizza attraverso l'immissione di ordini particolarmente 'allettanti' (i c.d. ordini civetta) che attraggono gli *slow trader* e che vengono rapidamente modificati subito dopo l'immissione, inserendo condizioni meno favorevoli prima ancora che le controparti attratte nella transazione possano rendersi conto del mutamento.

---

[318] Si tratta di un elenco non esaustivo delle strategie più aggressive e potenzialmente abusive che un algoritmo di *trading* può porre in essere.

[319] Come chiarito da A. PUORRO, *High frequency trading*, *op. cit.*, p. 20 il *trader* algoritmico "si pone, quindi, come controparte di queste operazioni, e, dopo aver accumulato un certo quantitativo di liquidità, inizia a simulare lo stesso schema comportamentale, ma nel verso opposto, spingendo gli operatori a chiudere le posizioni precedentemente accumulate (solitamente in perdita, a causa della falsità degli stimoli che hanno determinato le decisioni alla base delle operazioni), e creando nuovamente le situazioni che potrebbero determinare un aumento degli ordini di negoziazione, grazie ai quali chiudere in profitto le proprie operazioni precedentemente intraprese".

Una variante ancor più sofisticata di questo schema è lo *spoofing (o painting the tape)*. Esso prevede una prima fase di immissione di ordini di vendita per un determinato titolo a prezzo superiore rispetto al migliore presente sul mercato al fine di simulare una fase al ribasso del titolo stesso, una seconda fase di cancellazione dell'ordine prima che venga eseguito e una terza fase di acquisto del titolo sfruttando l'abbassamento dei prezzi artificiosamente creato nella prima fase.

Il *layering* invece consiste nell'immissione di un ordine nascosto (ossia non visibile nel *book* di negoziazione) da un lato del mercato (ad esempio in acquisto) e un altro ordine palese (quindi visibile nel *book*) dall'altro lato del mercato (ad esempio in vendita) in modo da indurre gli altri *trader* a pensare che il mercato si stia muovendo verso un ribasso del prezzo e ad agire di conseguenza. Anche in tal caso il *trader* algoritmico può sfruttare la propria velocità per cancellare l'ordine di vendita prima che venga eseguito ed eseguire invece l'ordine nascosto di acquisto ad un prezzo più vantaggioso[320].

Infine, il *pinging* è uno schema che, nell'intento di provocare la reazione degli altri *trader* e svelare le loro strategie, prevede l'invio di un numero elevato di piccoli ordini (*ping*) per uno strumento finanziario e la cancellazione in frazioni di secondo dalle piattaforme di negoziazione, inducendo così gli altri operatori a reagire ai *ping* e a rivelare le proprie intenzioni di *trading*. Questo determina, da un lato, un apparente movimento di mercato che induce alla negoziazione operatori che altrimenti non avrebbero effettuato le operazioni e, dall'altra parte, un vantaggio informativo del *trader* algoritmico agevolato dalla maggiore velocità di azione rispetto agli *slow trader*.

3.2.3. La liquidity detection *e il* momentum ignition

Fra gli schemi più aggressivi tipicamente posti in essere dai trader algoritmici vi sono poi la *liquidity detection* e il *momentum ignition*.

---

[320] In buona sostanza, come si sottolinea nella decisione dell'Alta Corte di Giustizia UK nel caso Da Vinci, analizzata da G. RUTA, *I.A. nei reati economici e finanziari*, *op. cit*., pp. 67-69 si tratta di una pratica che consiste nell'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 provocato dal 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 book 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".

Entrambe si basano sull'obiettivo di accumulare la liquidità offerta sui mercati, ossia trarre profitto prima degli altri *trader* dalla liquidità determinata dalla chiusura di posizioni[321].

Il *momentum ignition*, in particolare, prevede che il *trader* algoritmico assuma una posizione aggressiva che genera una forte oscillazione del prezzo di un titolo, aumentando significativamente i volumi di scambio e spingendo gli altri operatori a reagire al movimento di prezzo. Il *trader* algoritmico sfrutta l'oscillazione a proprio favore, effettuando un'operazione di segno opposto a quella iniziale a prezzi prima non disponibili e chiudendo la propria posizione traendo profitto[322].

3.2.4. Il pump and dump*, il* trash and cash *e il* marking the close

Invece, il *pump and dump* prevede l'acquisto di una grande quantità di titoli, che inducono gli altri operatori a immettere grandi quantità di ordini di acquisto dello strumento finanziario, facendone salire il prezzo (*pump*). Una volta che il prezzo è aumentato fino a un certo livello (aumentato artificiosamente tramite il *pump*), il *trader* vende la propria posizione 'lunga' traendo profitto dall'aumento di prezzo (*dump*).

Strategia esattamente speculare, che presuppone l'assunzione di posizioni 'corte' è il *trash and cash.*

---

[321] A. PUORRO, *High frequency trading, op. cit*., p. 19 precisa che "per *liquidity detection* s'intende l'attività attraverso la quale i *trader* algoritmici (non necessariamente ad alta frequenza) 'testano' alcuni livelli chiave tramite piccoli ordini, per verificare la presenza di *stop loss* o *take profit*; tali sistemi cercano poi di far scattare gli *stop loss* e i *take profit* degli altri partecipanti al mercato in modo da poter accumulare la liquidità offerta (indifferentemente in acquisto e in vendita) in corrispondenza di tali ordini di chiusura. […] Lo stop loss (SL) è un ordine condizionato utilizzato per minimizzare le perdite, chiudendo automaticamente la posizione al verificarsi di un determinato livello di prezzo cui corrisponde la perdita massima che si intende sopportare. […] Per take profit (TP) si intende un ordine condizionato avente lo scopo di chiudere automaticamente in profitto la posizione al verificarsi di un determinato evento, rappresentato di solito da un livello tecnico particolare o da un livello assoluto di guadagno ottenuto dalla posizione. L'utilizzo di ordini di *stop loss* o di *take profit* permette di eliminare la componente comportamentale dalle decisioni di investimento".

[322] Nella prima fase della strategia il prezzo dello strumento non subisce un movimento significativo perché il *trader* 'accumula' la propria posizione. Terminata la fase di accumulazione, il *trader* invia un ordine caratterizzato da forti volumi, in un momento in cui i mercati mostrano scarsa volatilità e bassi volumi di scambio, induce gli altri partecipanti al mercato a reagire, chiudendo le loro posizioni. Il *trader* che ha avviato la strategia trae profitto dagli ordini di chiusura degli altri per chiudere in profitto la propria strategia. Così A. PUORRO, *High frequency trading, op. cit*., p. 19.

O ancora, il *marking the close,* ossia l'acquisto o la vendita di un titolo, durante momenti precisi della sessione di negoziazione (ad esempio, apertura o chiusura) nel tentativo di aumentare, diminuire o mantenere il prezzo di riferimento (ad esempio, prezzo di apertura, prezzo di chiusura) a un livello specifico.

3.2.5. Le altre condotte potenzialmente abusive

Un ulteriore scenario di rischio che è possibile prospettare con riferimento al *trading* algoritmico deriva dall'interazione dei diversi sistemi automatizzati operanti sui mercati.
Da un lato, è possibile che essi 'imparino' dagli algoritmi strategie che consentono la massimizzazione dei profitti e che le perseguano a propria volta perché considerate ottimali e razionali, ancorché abusive. Dall'altro lato, è possibile che si verifichino ipotesi di vera e propria 'collusione algoritmica', anche oltre la volontà degli sviluppatori[323].

Inoltre, l'operatività degli algoritmi nei mercati finanziari consente loro di operare in modo estremamente sofisticato sfruttando informazioni rilevanti in ambito finanziario. Ciò può avvenire lecitamente, come nel caso del c.d. *trading on the news* strategia che prevede proprio l'utilizzo di notizie economiche, politiche o aziendali capaci di influenzare i prezzi degli strumenti finanziari per le decisioni di *trading*[324]. Oppure, in virtù della propria forza computazionale, i *trader* algoritmici possono rivestire una posizione di vantaggio rispetto a quelli

[323] L'azione coordinata degli algoritmi di *trading* risulta particolarmente problematica nel caso della c.d. collusione tacita, che tende a sfuggire al tradizionale modello di regolamentazione e di vigilanza basato sull'agire umano. Sul concetto di collusione algoritmica tacita e sulle implicazioni si rinvia a A. AZZUTTI– W.G. RINGE–H.S. STIEHL, *Machine Learning, Market Manipulation*, *op. cit.*, 2021 che sottolineano come, ad esempio, i *benchmark* possono rappresentare un obiettivo particolarmente per le parti che colludono, considerato anche il loro ruolo fondamentale come valori di riferimento per la determinazione del prezzo degli strumenti finanziari assunto dai benchmark negli ultimi decenni. A. VERSTEIN, *Benchmark Manipulation*, in Boston College Law Review, vol. 56, issue 1, p. 264.

[324] Ci si riferisce alle informazioni c.d. *corporate*, ossia quelle che hanno ad oggetto le vicende della società (dati contabili e gestionali, operazioni finanziarie o industriali, ecc), e alle c.d. *market information*, che attengono invece alle vicende economico-politiche che hanno un riflesso sulla vita delle società e, di conseguenza, sul valore degli strumenti finanziari da queste emesse. Queste possono essere veicolate sia dagli strumenti tradizionali, sia tramite canali diveris come i *social media*.

'tradizionali' nell'analisi e nello sfruttamento di informazioni non (ancora) disponibili al pubblico[325].

La rete (intesa nella sua componente lata che comprende *internet* e i *social media*), ma anche l'istituzione finanziaria in cui opera, nonché la velocità e la potenza di azione sui mercati[326] sono gli ambiti di elezione per l'agire illecito dell'algoritmo.

3.3. Le condotte astrattamente rilevanti come abuso di informazioni privilegiate

Non è difficile immaginare il coinvolgimento di un algoritmo in uno schema di *front running*[327], che in buona sostanza consiste nell'anticipare l'impatto dell'arrivo di un ordine significativo sul mercato inserendone uno proprio prima dell'esecuzione dell'ordine che si suppone possa influire significativamente sul prezzo dello strumento finanziario. È una strategia che può essere utilizzata dagli intermediari che effettuano operazioni sia in conto proprio[328] sia in conto terzi e

[325] Questo ha portato una parte della dottrina a ipotizzare soluzioni volte sia a rallentare l'attività degli *high frequency trader* tramite i c.d. *speed bumps*, sia a segmentare l'accesso alle informazioni privilegiate, ritardando quello degli *high frequency trader*. Si tratta, tuttavia, di ipotesi che pongono alcuni problemi di compatibilità con i principi generali, di equo accesso alle informazioni e di parità di trattamento, che ispirano la disciplina europea degli abusi di mercato, e di gestione e diffusione delle informazioni *price-sensitive* Sul punto, F. ANNUNZIATA, *I processi di mercato automatizzati*, *op. cit.*, p. 406 e F. PASQUALE, *Law's Acceleration of Finance*, *op. cit.*, pp. 2085-2127.

[326] La velocità con cui l'algoritmo opera sui mercati consente di reperire informazioni in tempi estremamente più brevi rispetto agli operatori tradizionali, godendo, quindi, di un significativo vantaggio su questi ultimi. Inoltre, le informazioni privilegiate possono essere ottenute direttamente dai gestori dei mercati, tramite accordi *co-location* e di fornitura diretta di dati.

[327] Per un esempio di schema di *front running* si veda F. CONSULICH, I*ntelligenza artificiale e reati finanziari*, *op. cit.*, p. 250. Cfr. anche S. SEMINARA, *Diritto penale commerciale*, *op. cit.* p. 73 sottolinea – con riferimento alla specificazione di cui all'art. 7.1 lett. d) Regolamento MAR – l'indubitabiler riconducibilità della condotta di *front running* al fenomeno dell'abuso in borsa di informazioni privilegiate.

[328] Spesso tale strategia sfrutta il *flash trading*, servizio offerto da alcune piattaforme di negoziazione, che conferisce agli *high frequency trader* una sorta di prelazione sugli ordini a prezzi diversi dal *National Best Bid or Offer*. I *trader* ad alta frequenza hanno così un vantaggio informativo per un tempo pari o minore a 500 millisecondi, che seppur ridottissimo consente di processare il dato, analizzare la situazione della liquidità del mercato e intraprendere, ove possibile, le strategie più profittevoli.

in quest'ultimo caso implica l'immissione di un ordine prima che venga immesso quello del cliente[329].

Proprio la velocità di immissione degli ordini pochi istanti prima degli altri consentirebbe di sfruttare una conoscenza privilegiata relativa a grossi ordini di acquisto o vendita in arrivo sul mercato.

Oppure si pensi al dirigente di una multinazionale sa che la sua azienda sta per rilasciare dati finanziari pessimi, che faranno scendere il prezzo delle azioni e sulla base di questa informazione decide di utilizzare un algoritmo di *short selling* per vendere una grande quantità di azioni prima che la notizia diventi pubblica. L'algoritmo effettua vendite distribuite nel tempo per evitare di attirare l'attenzione e poi chiude le posizioni con profitto non appena il prezzo delle azioni scende drasticamente.

Tutto ciò premesso, occorre rilevare come benché vi sia un indubbio coinvolgimento degli algoritmi di *trading* nello sfruttamento dell'informazione privilegiata, questi non paiono in grado di influire sulle modalità della condotta in modo tanto significativo quanto avviene invece per la manipolazione del mercato. Infatti, se, pur con i dovuti *caveat*, le modalità della condotta della 'manipolazione algoritmica' assumono caratteri in parte diversi da quella 'tradizionale', l'intervento dell'algoritmo pare essere assai meno dirompente nel caso dell'*insider trading*.

Mentre nel compimento del primo illecito analizzato il sistema di negoziazione algoritmica ha una funzione essenziale di agevolazione e creazione delle condizioni perché si realizzi il comportamento fraudolento, altrettanto non pare avvenire nel caso dell'*insider trading*. Nelle ipotesi illustrate, infatti, le potenzialità dell'algoritmo di *trading* emergono specialmente nella fase di sfruttamento delle informazioni. L'algoritmo dunque si atteggia a strumento di 'ottimizzazione' dell'abuso, consentendo di acquisire un vantaggio competitivo sul mercato in tempi estremamente ridotti e su vasta scala.

---

[329] Gli algoritmi *hft* monitorano continuamente i flussi di ordini nel mercato. Quando rilevano un ordine significativo in arrivo, prevedendo che questo ordine influenzerà il prezzo del titolo, immettono rapidamente ordini propri prima che l'ordine venga eseguito. Quando l'ordine viene eseguito, causa un movimento del prezzo nel mercato (ad esempio far salire il prezzo del titolo). Dopo che il prezzo è salito, l'algoritmo *hft* vende le azioni che ha acquistato in precedenza, realizzando un profitto dalla differenza di prezzo. Ad esempio, se l'algoritmo – prima dell'immissione dell'ordine da parte di altri – acquista 10.000 azioni a 10,00 euro per azione, l'immissione dell'ordine di acquisto rilevante determina il rialzo del prezzo a 10,10 euro per azione, il *trader hft* rivendendo può realizzare un profitto di 0,10 euro per azione.

Vero è che la dottrina ha ipotizzato alcuni casi in cui l'algoritmo sembrerebbe assumere una funzione consustanziale alla realizzazione dell'abuso di informazioni privilegiate. Fra queste le ipotesi di 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 o, addirittura, che creino difficoltà alla piattaforma di contrattazione, per cui sia *ex ante* prevedibile un impatto sui prezzi o un blocco delle negoziazioni" ovvero "l'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 predeterminati strumenti finanziari favorendo poi facili guadagni su conti di individui collusi"[330].

3.4. La riconducibilità alle fattispecie incriminatrici

Queste condotte, pur nella loro innovatività, paiono costituire forme di offesa a beni giuridici tutelati dall'ordinamento che possono essere ricomprese entro l'operatività delle fattispecie incriminatrici esistenti.

Quote stuffing, *smoking*, *layering*, *pinging*, *liquidity detection*, *momentum ignition*, *pump and dump*, *marking the close* sono strategie accomunate, in buona sostanza, dalla capacità di creare movimenti fittizi di mercato finalizzati a indurre effetti imitativi nella generalità degli altri investitori attivi sul mercato.

Come tali, possono essere qualificate come "operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo" di cui all'art. 185 t.u.f.[331].

Ma a ben vedere, questi corrispondono anche alle condotte descritte delle previsioni eurounitarie[332].

Sono riconducibili all'ipotesi di cui al già citato art. 12, secondo paragrafo, lett. c) del Regolamento MAR, secondo cui è considerato manipolazione del mercato "l'inoltro di ordini in una sede di negoziazione, comprese le relative cancellazioni

---

[330] Così F. CONSULICH, *Intelligenza artificiale e reati finanziari*, *op. cit.*, p. 248.

[331] La formulazione ampia della fattispecie italiana che oltre al riferimento agli "artifizi" lega la rilevanza penale dell'azione all'idoneità di provocare un effetto distorsivo sul prezzo dello strumento finanziario include senza dubbio tutti i comportamenti sin qui illustrati.

[332] Si tratta, come nota S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., pp. 104-107 dell'espressione 'operazioni simulate o altri artifizi' di cui all'art. 185 t.u.f., che per la sua vaghezza, si presta a comprendere tutte le condotte descritte dall'art. 12 Regolamento (UE) n. 596/2014 e integrate dall'Allegato I al Regolamento (UE) n. 596/2014 e dall'Allegato II del Regolamento delegato (UE) n. 2016/522".

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 gestori individuare gli ordini autentici sul sistema di negoziazione della sede di negoziazione, o è probabile che lo faccia, anche emettendo 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 emettendo ordini per avviare o intensificare una tendenza".

Inoltre, le pratiche citate possono essere ricondotte anche all'ipotesi di cui all'art. 12, primo paragrafo, lett. a) dello stesso Regolamento – ossia il compimento di operazioni, l'inoltro di un ordine di compravendita o qualsiasi altra condotta idonei a inviare segnali falsi o fuorvianti in merito all'offerta, alla domanda o al prezzo dei titoli o di fissarne il prezzo a un livello anormale o artificiale –, tanto che l'Allegato II del Regolamento Delegato UE 2016/522 annovera espressamente molte delle pratiche già citate fra gli indicatori di questa tipologia di manipolazione del mercato.

Infine, per quanto norma di chiusura a cui fare ricorso solo in via eccezionale[333], le condotte manipolative realizzate tramite algoritmi possono essere ricondotte nell'ambito di applicazione dell'art. 12, primo paragrafo, lett. b)[334].

---

[333] In questi termini, F. CONSULICH, *Intelligenza artificiale e reati finanziari*, 2024, *op. cit.*, p. 259.

[334] La dottrina ha invero rilevato come la scelta del legislatore eurounitario di ancorare l'illegittimità del comportamento all'effetto che esso determina sul prezzo del mercato rischierebbe di avere un effetto ipercriminalizzante, specie qualora l'operazione sia stata compiuta attraverso sistemi di negoziazione basata su intelligenza artificiale 'forte'.

Nonostante la previsione della scriminante dei motivi legittimi e prassi di mercato ammesse teoricamente circoscriva il rischio di qualificare come manipolatorie alcune delle operazioni compiute quotidianamente sui mercati, questo non sarebbe possibile in alcuni casi. L'art. 12, primo paragrafo, lett. a) Regolamento MAR esclude la manipolazione nel caso in cui "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 […]"; nonché art. 13, paragrafo 1, "Il divieto di cui all'articolo 15 non si applica alle attività di cui all'articolo 12, paragrafo 1, lettera a), a condizione che la persona che avvia un'operazione, colloca un ordine di compravendita o s'impegna in qualsiasi altra condotta stabilisca che tale

Ma si possono ricondurre all'utilizzo di algoritmi per commettere abusi di mercato anche altre ipotesi[335].

Si pensi a chi, tramite un sistema di intelligenza artificiale o tramite *bot*, dà vita a un *tweet bombing* che influenza l'interesse su un determinato titolo[336]. Anche in questo caso, si ricadrebbe in una delle condotte descritte dal Regolamento MAR. L'art. 12, primo paragrafo, lett. c) stabilisce infatti che è considerata manipolazione del mercato "la diffusione di informazioni tramite i mezzi di informazione, compreso Internet, o tramite ogni altro mezzo, che forniscano, o siano idonei a fornire, 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 o che consentano, o è probabile che consentano, di fissare il prezzo di mercato di uno o più strumenti finanziari o di contratti a pronti su merci collegati o di un prodotto oggetto d'asta sulla base di quote di emissioni a un livello anormale o artificiale, compresa la

---

operazione, ordine o condotta sono giustificati da legittimi motivi e sono conformi a una pratica di mercato ammessa, come stabilito a norma del presente articolo".

Quest'ultima norma è richiamata infine dall'art. 185, comma 1 *bis*, t.u.f., a norma del quale "non è punibile chi ha commesso il fatto per il tramite di ordini di compravendita o operazioni effettuate per motivi legittimi e in conformità a prassi di mercato ammesse, ai sensi dell'articolo 13 del regolamento (UE) n. 596/2014".

La causa di giustificazione in questione ha comunque una operatività limitata alle ipotesi di avvio di un'operazione o l'inoltro di un ordine di compravendita che invii segnali falsi o fuorvianti o consenta di fissare il prezzo di uno strumento finanziario, di un contratto a pronti su merci o di un prodotto oggetto d'asta a un livello anomalo artificiale (art. 12, primo paragrafo, lett. a Regolamento MAR).

In particolare, quando gli algoritmi agiscono come *market maker* o quando sono coinvolti nell'attività di *trading* sistemi di intelligenza artificiale forte, caratterizzati dalla *black box*.

Nel primo caso – ossia quando il sistema di *trading* opera come intermediario che gestisce operazioni per conto dei clienti utilizzando il proprio conto (*market making)* – il *market maker* spesso ha la libertà di selezionare la sede di negoziazione di propria scelta a costo nullo o minimo per i propri clienti. Ciò che rende difficile distinguere tra comportamenti illeciti e leciti è il fatto che talvolta proprio l'attività rivolta ai clienti fornisce al *market maker* una giustificazione per molte operazioni. Ad esempio, che l'operazione sia stata compiuta per coprire un ordine del cliente.

Nel secondo caso, l'impossibilità – anche per il programmatore – di comprendere appieno il percorso logico seguito dal sistema impedirebbe invece di dimostrare che le motivazioni alla base delle operazioni compiute fossero razionalmente giustificate ed economicamente fondate o che corrispondessero a un comportamento adottato dalla generalità degli operatori attivi sul mercato di riferimento, preventivamente ammesso dall'autorità di vigilanza competente.

[335] Si tratta di ipotesi che si discostano, quantomeno per le modalità realizzative, dagli scenari precedenti perché realizzate al di fuori dell'ambito della contrattazione.

[336] Occorre però precisare che in questo caso lo strumento tramite cui viene posta in essere la manipolazione informativa non è uno strumento 'di *trading*' in senso stretto, nel senso che non compie operazioni borsistiche.

diffusione di voci, quando la persona che ha proceduto alla diffusione sapeva, o avrebbe dovuto sapere, che le informazioni erano false o fuorvianti".

Così come è riconducibile alla fattispecie incriminatrice dell'abuso di informazioni privilegiate[337] l'utilizzo del sistema di intelligenza artificiale per penetrare nei sistemi informatici delle aziende ed estrarre documenti finanziari sensibili e informazioni su eventi aziendali futuri, come acquisizioni, fusioni, o pubblicazioni di dati di bilancio, che vengono poi sfruttate.

In definitiva, dunque, si può riconoscere che l'algoritmo è in grado di porre in essere, se non agevolare, il fatto di reato nella sua componente oggettiva.

L'operare dell'algoritmo sui mercati, come descritto sin qui, ha una efficacia offensiva concreta del bene giuridico protetto dalle norme. L'attività di *trading* abusiva ha in effetti la capacità di modificare il prezzo degli strumenti finanziari in modo del tutto sovrapponibile all'agente umano. L'agire dell'algoritmo non differisce dunque dall'agire umano. La capacità computazionale delle 'macchine', certamente non paragonabile a quella dell'uomo, muta la velocità e la capacità di elaborazione di enormi quantità di dati, ma non elimina la materialità dell'azione.

Tuttavia, rispetto alla riconducibilità all'*insider trading* di alcuni casi – pur citati dalla dottrina[338] –, si impongono alcune cautele.

Innanzitutto, occorre notare che – riprendendo gli esempi summenzionati – gli algoritmi coinvolti nelle condotte di *tweet bombing* o quelli sfruttati per penetrare nei sistemi informatici delle aziende ed estrarre documenti finanziari sensibili – non siano dei veri e propri algoritmi 'di *trading*', bensì tecnologie che svolgono attività diverse, benché in qualche modo strumentali alla realizzazione della condotta.

Inoltre, ma soprattutto il fatto che le condotte descritte più che allo sfruttamento dell'informazione privilegiata, sembrerebbero costituire piuttosto operazioni idonee a provocare una sensibile alterazione dei prezzi dei titoli, ricadendo quindi nell'alveo della manipolazione di mercato.

Tanto è vero che, mentre sono ormai noti i casi di condanne per manipolazione del mercato 'algoritmica', non si registrano sanzioni inflitte per l'abuso di informazioni privilegiate.

---

[337] L'abuso di informazioni privilegiate evidentemente non è l'unica fattispecie che può venire in rilievo rispetto a tale condotta. Si potrebbe infatti valutare anche una responsabilità ai sensi dell'art. 615 *ter* c.p., che esula dall'oggetto del presente lavoro e che, pertanto, non si approfondisce in questa sede.

[338] F. CONSULICH, *Intelligenza artificiale e reati finanziari*, *op. cit.*, p. 248.

4. Le condotte concrete: casistica e simulazioni di mercato

4.1. Premessa

L'accertamento di abusi di mercato commessi tramite sistemi di negoziazione algoritmica è avvenuto, sinora, esclusivamente da parte di autorità britanniche e statunitensi[339].

L'analisi di tale casistica consente di comprendere quali siano le modalità specifiche in cui può estrinsecarsi l'abuso degli algoritmi di *trading* e quali siano i principali problemi probatori posti dall'utilizzo di tali sistemi.

Riguardo a quest'ultimo aspetto occorre tuttavia sottolineare, in primo luogo, che si tratta, come detto, di procedimenti di natura differente – penale e amministrativa – celebrati di fronte alle autorità americane e anglosassoni e che dunque vanno considerati in chiave prettamente comparatistica[340].

In secondo luogo, è necessario considerare che le sanzioni inflitte – sia in sede civile o amministrativa, sia in sede penale – per manipolazione del mercato 'algoritmica' allo stato attuale hanno avuto ad oggetto l'operatività di sistemi di *trading* non basati su intelligenza artificiale [341].

In particolare, i casi civili o amministrativi più rilevanti sono quelli che hanno interessato Athena Capital Research LLC, Da Vinci Invest Limited, Paul Axel Walter.

Mentre i giudizi che hanno riguardato Michael Coscia e Navinder Singh Sarao rappresentano i primi processi penali per 'manipolazione algoritmica'.

Come detto, si tratta di precedenti assai rilevanti perché, in primo luogo, consentono di indagare se l'uso di algoritmi di *trading* introduca in effetti elementi in grado di alterare la formazione dei prezzi degli strumenti finanziari, turbando il regolare andamento dei mercati, e in secondo luogo perchè fanno emergere la

---

[339] Si tratta, peraltro, degli unici casi di manifestazioni di offese compiute da o attraverso sistemi algoritmici, come rileva F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*

[340] F. CONSULICH, Flash offenders, *op. cit.*, p. 1037 nota che "il maggiore sforzo delle autorità di settore si è concentrato sulla prevenzione delle turbative algoritmiche, mentre langue la reazione punitiva rispetto a manipolazioni effettivamente avvenute, anche laddove, come nel Regno Unito, il formante legislativo sia stato rinnovato con norme che ben potrebbero prestarsi a un *enforcement* severo".

[341] La casistica è ampia e include: CFTC vs Jiongsheng Zhao; CFTC vs Morgan Stanley Capital Group Inc.; CFTC vs Krishna Mohan (2013); CFTC vs Propex Derivatives PTY Ltd (2012 - 2017); 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).

difficoltà nel dimostrare – in caso di condotte poste in essere tramite questa tecnologia – tutti gli elementi costitutivi dell'illecito, fra cui in particolare l'intenzionalità[342].

4.2. I procedimenti amministrativi: i casi Athena Capital Research LLC, Da Vinci Invest Limited e Paul Axel Walter

La prima condanna, in sede amministrativa, risale all'ottobre 2014 e ha riguardato un caso di manipolazione del mercato attuata tramite lo schema del *marking the close* ad opera di Athena Capital Research LLC[343]. Di fronte a una strategia estremamente aggressiva che causava il movimento dei i prezzi di chiusura di migliaia di titoli, ciò che risulta particolarmente rilevante nella vicenda in esame è stata la difficoltà di stabilire e dimostrare il confine fra l'esecuzione di

[342] Come rileva F. CONSULICH, Flash offenders, *op. cit.*, p. 1035 i casi di condanne, per quanto in numero assai limitato, dimostrano la preferenza per il "diritto civile da parte delle Agenzie di controllo e le lamentele da parte della giurisprudenza, pur in seno ad una sentenza di condanna penale, per le difficoltà probatorie in merito all'elemento soggettivo in capo all'agente umano" e, più in generale "dimostrano tutti i limiti del controllo giuridico di simili fenomeni pur in ordinamenti che rappresentano l'avanguardia nella tutela dell'integrità dei mercati". Tanto che "per lo più è la via civile quella che viene intrapresa, per comprensibili ragioni, molto semplici da afferrare anche da questo lato dell'Atlantico: il deficit probatorio che si profila sul piano dell'elemento soggettivo dell'eventuale reato di manipolazione del mercato che si contestasse all'agente fisico" (p. 1037).

[343] Athena Capital Research, LLC, Securities Exchange Act of 1934 Release No. 73369, Administrative Proceeding File No. 3-16199, at 2 (SEC Oct. 16, 2014). Il procedimento, in particolare riguardava un caso di *marking the* close ad opera di Athena Capital Resarch LLC in violazione della Sezione 10(b) del Securities Exchange Act del 1934 e la Rule 10b-5: https://www.sec.gov/files/litigation/admin/2014/34-73369.pdf.
Secondo le indagini della SEC, la società, grazie all'algoritmo Gravy effettuava massicce quantità di operazioni negli ultimi secondi della giornata di *trading*, sovraccaricando così la liquidità disponibile sul mercato e spingendo artificialmente il prezzo di mercato – e quindi il prezzo di chiusura – a proprio favore. Il provvedimento della SEC rileva che lo schema manipolativo di Athena sfruttava squilibri di ordini in titoli alla chiusura della giornata di *trading*, riuscendo a conferire alla società una posizione dominante sul mercato che, sebbene durasse solo per gli ultimi secondi della giornata, era sufficiente a garantire un profitto. Ogni giorno alla chiusura del mercato, il NASDAQ esegue un'asta di chiusura per soddisfare tutti gli *ordini on-close* al miglior prezzo. Athena piazzava ordini per coprire gli squilibri in titoli alla chiusura della giornata di *trading* dieci minuti prima della chiusura e poi, negli ultimi due secondi della sessione, scambiava o "accumulava" azioni sul mercato continuo sul lato opposto del suo ordine. Ciò spingeva il prezzo di quella determinata azione verso l'ordine inserito dieci minuti prima della chiusura e consentiva di trarre profitto dal movimento dei prezzi.
Cfr. U.S. SECURITIES AND EXCHANGE COMMISSION, Press Release. *SEC Charges New York-Based High Frequency Trading Firm With Fraudulent Trading to Manipulate Closing Prices: First High Frequency Trading Manipulation*, Case, SEC. & EXCH. COMM'N (Oct. 16, 2014), https://www.sec.gov/news/press-release/2014-229#.VEOZlfldV8E [http://perma.cc/RJ9PGE46].

operazioni aventi uno scopo economico genuino e la volontà di influenzare artificialmente i prezzi[344].

Tema centrale nel caso Da Vinci sono stati invece i criteri di attribuzione della responsabilità per manipolazione di mercato in capo a una società che utilizza complessi sistemi informatici[345].

Il processo civile si è celebrato nel 2017 in Gran Bretagna di fronte all'Alta Corte di Giustizia contro un gruppo di società con a capo la Da Vinci Invest AG (Da Vinci Invest LTD o 'DVI', Da Vinci Invest Pte Limited o 'DVPte')[346] e tre *trader* ungheresi.

Oggetto del giudizio era, in particolare, una manipolazione del mercato secondo lo schema del *layering* e *spoofing*, avvenuta fra il 2010 e il 2011 sulla borsa di Londra[347] in violazione delle sezioni 381 e 129 del *Financial Services and Markets Act 2000* (c.d. FSMA).

Le condotte contestate consistevano in particolare nell'immissione di più ordini che la società non aveva reale intenzione di eseguire sul *book* di negoziazione, ma che viceversa avevano solo l'obiettivo di creare una falsa impressione sulle

[344] Per escludere la liceità e la genuinità economica della condotta, nel caso di specie, la SEC ha utilizzato, fra l'altro, e-mail inviate dai manager di Athena, in cui si affermava che l'obiettivo di quell'algoritmo specifico era quello di modificare i prezzi e che la strategia della società era quella di dominare l'asta e 'fare il gioco'.

[345] La decisione del caso Da Vinci può essere consultata al seguente link: http://www.bailii.org/ew/cases/EWHC/Ch/2015/2401.html.

[346] La Da Vinci Invest Ltd (DVI) era una società inglese che operava dalla Svizzera – e quindi sottoposta alla vigilanza dell'autorità autoctona, la FINMA – come gestore di fondi di investimento; la Da Vinci Investe Pte Limited (DVPte) invece era una società di Singapore.

[347] Come si legge nel provvedimento dell'Alta Corte, fino al 2007, il London Stock Exchange gestiva la principale piattaforma di *trading* elettronico nel Regno Unito per l'acquisto e la vendita di azioni di società quotate sul suo mercato principale. Anche a seguito dell'introduzione della Direttiva MiFID I e l'apertura alla concorrenza nelle *Multilateral Trading Facilities* ("MTF"), la maggior parte degli scambi delle società quotate nel Regno Unito avviene ancora sul LSE, sebbene una parte significativa degli scambi venga effettuata su MTF gestiti da altri operatori. Al momento degli eventi oggetto di causa, tra questi vi erano BATS, Chi-X e Turquoise.

vere intenzioni commerciali del *trader*[348]. Si trattava di operazioni di *day-trading* su derivati[349] relativi ad azioni quotate sul London Stock Exchange[350].

---

[348] Nell'ambito del procedimento davanti all'Alta Corte della FSA, il consulente tecnico ha rilevato le seguenti caratteristiche costanti delle negoziazioni dei *trader*:

i) le negoziazioni avvenivano in brevi periodi (il più lungo dei quali durava 38 minuti e la media era di 12 minuti), concentrati su una particolare azione;
ii) ogni operazione seguiva un pattern di andamento 'a scalini' (Letteralmente: "saw tooth"), causato dalla creazione successiva di grandi posizioni cumulative nette di ordini su lati opposti del *book* degli ordini (ad esempio, la creazione di una grande posizione netta di acquisto seguita dalla creazione di una grande posizione netta di vendita). Il numero di inversioni variava in base alla durata dell'operazione; quindi, poteva esserci solo un'inversione in un periodo di 5-7 minuti di negoziazione, ma 11 inversioni in un periodo più lungo, ad esempio 22 o 23 minuti;
iii) la variazione del prezzo delle azioni era correlata al pattern 'a scalini' dell'inserimento degli ordini in quasi tutti i casi;
iv) un'alta percentuale di ordini (in base al numero di azioni scambiate) veniva eseguita sul lato opposto alla posizione netta cumulativa dell'ordine. La percentuale variava dal 73% al 97%, ma in media era dell'88%;
v) la posizione netta delle azioni tendeva a muoversi nella direzione opposta alla posizione netta cumulativa dell'ordine (ad esempio, quando la posizione netta cumulativa dell'ordine era di vendita, la posizione netta delle azioni veniva aumentata dall'acquisto di ulteriori azioni).
vi) c'era un tasso di cancellazione molto più elevato (calcolato in base al numero di azioni) per gli ordini di grandi dimensioni rispetto agli ordini di piccole dimensioni. In media, il rapporto tra ordini di grandi dimensioni eseguiti e quelli cancellati era di circa 1:8, mentre il rapporto tra ordini di piccole dimensioni eseguiti e quelli cancellati era di circa 3:1.

Inoltre, si è rilevato che:

i) c'era una stretta correlazione tra la posizione cumulativa netta degli ordini di DVI e il prezzo delle azioni. In particolare, DVI ha inizialmente inserito ordini di acquisto cumulativi significativi fino poco prima delle 11:06, per poi invertire rapidamente quella posizione e inserire ordini di vendita cumulativi significativi fino poco dopo le 11:09, quando ha nuovamente invertito quella posizione e ha iniziato a inserire ordini di acquisto cumulativi significativi. Ha ripetuto quel ciclo sei volte nel corso dei 38 minuti di negoziazione;
ii) DVI ha inserito quasi tre quarti (73,95%) dei suoi ordini passivi sullo stesso lato del book degli ordini della sua posizione cumulativa netta e ha inserito tutti tranne uno dei suoi ordini aggressivi (corrispondenti a circa il 21,9% degli ordini totali) sul lato opposto del book degli ordini. Questa è una caratteristica costante delle negoziazioni dei *trader*;
iii) la posizione netta delle azioni di DVI (che era pari al 96% dell'intero volume negoziato sulle azioni AQP durante il periodo di negoziazione) si è mossa nella direzione opposta alla sua posizione cumulativa netta degli ordini. Ad esempio, quando la posizione cumulativa netta degli ordini era di acquisto, la posizione netta delle azioni è diminuita e viceversa. Si tratta di un'altra caratteristica costante;
iv) c'è stato un tasso di cancellazione molto più elevato per gli ordini di grandi dimensioni rispetto agli ordini di piccole dimensioni. In particolare, il 50% del volume negoziato era rappresentato da ordini di grandi dimensioni, ma questi ordini costituivano il 92,3% del volume totale degli ordini cancellati.

Tuttavia, in due occasioni, a metà dicembre 2010, BATS – gestore dell'MTF su cui venivano effettuati gli scambi – ha segnalato in più occasioni il rischio di manipolazione dei prezzi dei titoli su LSE, derivante dal fatto che DVI avesse più volte comprato un particolare titolo al minimo della variazione nel periodo dei

---

Tali analisi hanno portato la Alta Corte ad affermare la riconducibilità della condotta alla categoria del *layering*, che – come noto – è una pratica che consiste nell'inserire ordini relativamente grandi su un lato *book* di un mercato, senza una reale intenzione che tali ordini vengano eseguiti: gli ordini vengono posizionati a prezzi che, secondo la persona che li inserisce, sono improbabili da attrarre controparti, ma che tuttavia raggiungono l'obiettivo di spostare il prezzo delle azioni rilevanti poiché il mercato si adatta al fatto che si è verificato un apparente cambiamento nell'equilibrio tra offerta e domanda. Il movimento viene quindi seguito dall'esecuzione di un'operazione sul lato opposto del libro degli ordini che approfitta e trae profitto da tale movimento. A seguito di ciò, gli ordini di grandi dimensioni inseriti allo scopo di causare la variazione di prezzo vengono rapidamente cancellati e il comportamento viene ripetuto in modo inverso sull'altro lato del libro degli ordini. In altre parole, una persona impegnata nel *layering* cerca di spostare il prezzo al rialzo per trarre vantaggio da una vendita a un prezzo elevato, quindi cerca di abbassarlo per comprare nuovamente, ma a un prezzo più basso, e solitamente ripete il processo diverse volte.

[349] I c.d. CFD, ossia un tipo di investimento derivato, in cui il prezzo è definito in base alle azioni negoziate sulla London Stock Exchange. Un CFD che fa riferimento alle azioni è un accordo in cui le parti concordano di pagare o ricevere la differenza di valore di una particolare azione tra il momento e la data in cui il contratto viene aperto (sottoscritto) e il momento e la data in cui il contratto viene chiuso (terminato). Gli investitori che stipulano CFD con un broker "acquistano" un CFD e assumono quindi una "posizione long" se si aspettano che il prezzo dell'azione sottostante aumenti. Al contrario, se l'investitore si aspetta che il prezzo dell'azione sottostante scenda, "venderà" un CFD e assumerà quindi una "posizione short". Il CFD rimarrà aperto fino a quando l'investitore deciderà di chiuderlo dandone comunicazione o fino al raggiungimento di un predefinito "stop-loss" concordato. La chiusura del CFD comporterà l'obbligo per una delle parti di pagare la differenza di valore tra il prezzo di apertura e quello di chiusura dell'asset sottostante.
Attraverso i CFD, gli investitori possono speculare su variazioni positive e negative dei prezzi delle azioni senza possedere alcuna azione sottostante. Questo rappresenta un vantaggio finanziario importante per il *trading* ad alto volume, poiché gli investitori possono speculare sulle variazioni dei prezzi delle azioni senza dover investire la stessa quantità di capitale richiesta per comprare e vendere le azioni sottostanti. I CFD sono anche vantaggiosi per gli investitori, poiché, a differenza delle transazioni con le azioni, non sono soggetti a *stamp duty tax*.
Cfr. http://www.bailii.org/ew/cases/EWHC/Ch/2015/2401.html parr. 17-21.

[350] Da Vinci Invest Limited ('DVI'), operava come gestore di investimenti e fondi da una filiale in Svizzera. A metà del 2010, DVI aveva avviato una *joint venture* con tre *trader* ungheresi. In base all'accordo, DVI avrebbe fornito capitale per il *trading*, mentre i *trader* avrebbero compiuto operazioni su derivati (CFD) e diviso i profitti al 50% con la società.
L'attività di *trading*, iniziata ad agosto, sfruttava il sistema di *direct market access* (c.d. DMA) fornito da Goldman Sachs e il *software front-end* per connettersi al sistema DMA dell'azienda RealTick Nelle fasi iniziali i *trader* avrebbero adottato strategie di *trading* ad 'alto consumo di capitale', come partecipare all'asta di apertura e chiusura e fare *scalping* (così descritto nel provvedimento dell'Alta Corte: "aprire posizioni per trarre beneficio dall'attività istituzionale. Trarre beneficio da turbolenze di mercato a breve termine, trarre vantaggio da acquisti/vendite massicci, inserire ordini sotto e sopra il prezzo di mercato effettivo").

prezzi e venduto al massimo della variazione nel periodo dei prezzi, senza inserire altri ordini o eseguire negoziazioni nel periodo intermedio. Un'analoga segnalazione è stata inoltrata anche da Goldman Sachs, che identificava DVI come responsabile di potenziali abusi di mercato nella forma del c.d. *layering*[351]. Chiuso il rapporto con Goldman Sachs, visti i sospetti di manipolazione del mercato, le stesse condotte sono state realizzate nel 2011 tramite SunGard, società americana che forniva a DVI servizi di *direct market access*, in luogo di Goldman Sachs. Anche in questo caso alla FCA[352] sono giunte segnalazione di transazioni sospette.

Ebbene, uno degli aspetti più rilevanti del provvedimento dell'Alta Corte di Giustizia, sono le conclusioni in merito alla responsabilità della società per un'attività di *trading* abusiva effettuata tramite programmi informatici progettati o gestiti dai dipendenti della società stessa.

Di fronte alle accuse della FCA, DVI sosteneva che gli atti non potessero essere attribuiti all'ente, in assenza di una prova del fatto che fossero 'atti della mente e volontà diretta della società, o eseguiti sotto la direzione/conoscenza specifica/consenso di tale individuo[353]. Al contrario, la Corte – recependo gli argomenti della FCA –, ha affermato che, ai fini del rimprovero per le condotte sanzionate dalla sezione 118(5) dell'FSMA come abusi di mercato, non è necessaria una valutazione dell'elemento soggettivo, ma che essa si basa esclusivamente sull'elemento oggettivo.

L'Alta corte sottolinea infatti che la finalità perseguita dalle normative – MAR compreso – che sanzionano il *market abuse* verrebbe frustrata se si ritenesse che la società possa andare esente dalle responsabilità per le azioni dei dipendenti o dei programmatori che agiscono nell'interesse della società stessa[354].

Per questa ragione, accertata la commissione del fatto nella sua componente oggettiva, il giudice ha condannato DVI per non aver vigilato sui *trader*, e quindi a prescindere dal fatto che i dirigenti di DVI non avessero effettivamente

---

[351] Goldman Sachs ha indicato che la loro sorveglianza interna aveva infatti individuato dodici occasioni tra metà settembre e inizio dicembre 2010 in cui DVI aveva adottato quel tipo di comportamento.

[352] Financial Conduct Authority, l'autorità di regolazione del mercato britannica.

[353] Letteralmente: "acts of the directing mind and will of the company, or carried out at that individual's direction/specific knowledge/consent"

[354] "In the context of modern trading on regulated markets, it would be contrary to the current market abuse regime if companies could escape liability for the actions of their employees if directors and senior management, as the 'directing mind and will' of the company, did not have detailed knowledge of the day to day activities".

effettuato o coordinato il *trading* in questione o non conoscessero nel dettaglio le modalità tecniche con cui esso si svolgeva.

Infine, il caso Paul Walter, culminato nell'irrogazione di una sanzione amministrativa nel 2017 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, concepiti per indurre gli altri operatori del mercato che seguivano l'andamento dei titoli ad alzare o abbassare le proprie quotazioni di modo da beneficiare di tali movimenti di prezzo[355]. Tutto ciò, sfruttando l'utilizzo da parte degli altri operatori di sistemi automatizzati (algoritmi) per seguire le migliori offerte (*best bid e best offer*). Gli algoritmi in uso agli altri operatori infatti monitoravano le migliori offerte e Walter li usava per attirarli verso le sue quotazioni e quindi negoziare poi a prezzi più alti o più bassi. Anche in questo caso è centrale l'accertamento dell'elemento soggettivo, tanto che la FCA giunge ad affermare la gravità di questo esempio di *market abuse*, pur affermando che si tratti di un fatto dovuto a colpa e non a dolo[356].
Sebbene l'Autorità abbia concluso che il signor Walter non aveva intenzione di commettere un abuso di mercato, nel giudizio si afferma che avrebbe dovuto rendersi conto che il suo comportamento costituiva un abuso di mercato, tenuto conto che era un soggetto autorizzato e un *trader* esperto[357].

---

[355] Più precisamente, è stato ritenuto responsabile di abuso di mercato ai sensi della sezione 118(5) del Financial Services and Markets Act 2000 (FSMA), per aver un'impressione falsa e ingannevole sul prezzo e sulla domanda/offerta dei DS (Dutch State Loans), fissando il prezzo a un livello artificiale.
Egli infatti inseriva ordini, rappresentando un'intenzione di acquistare quando in realtà voleva vendere e viceversa. Questo induceva altri partecipanti al mercato a modificare le loro offerte. Quando voleva vendere, inseriva offerte elevate (*best bid*), inducendo gli altri a rialzare le loro offerte. Quando voleva comprare, inseriva offerte basse (*best offer*), inducendo gli altri a ribassare le loro offerte. Successivamente eseguiva operazioni di vendita o acquisto sfruttando le modifiche indotte, ottenendo prezzi più vantaggiosi rispetto a quelli disponibili prima delle sue false operazioni.

[356] Cfr. FINANCIAL CONDUCT AUTHORITY, *Final notice 2017: Paul Axel Walter*, https://www.fca.org.uk/publication/final-notices/paul-axel-walter-2017.pdf, p. 3: "The Authority regards this as a serious example of market abuse, notwithstanding that it was committed negligently rather than deliberately

[357] FINANCIAL CONDUCT AUTHORITY, *Final notice 2017*, *cit.*, p.3: "In particular because of the following factors: (1) Mr Walter was an approved person and an experienced trader of government bonds with 20 years of experience; (2) Although the Authority has concluded that Mr Walter did not intend to commit market abuse, he should have realised that his behaviour constituted market abuse. His behaviour constituted a serious failure to act in accordance with the standards reasonably expected of market participants and did not cease even after he was put on notice of concerns about his behaviour (which BrokerTec had raised in a telephone call

Ebbene, i casi sin qui descritti testimoniano la consistenza pratica del problema giuridico che in questa sede si vuole affrontare.
Essi, infatti, dimostrano come, non solo nella teoria, ma anche nella pratica, l'uso di algoritmi consenta di porre in essere condotte aventi portata abusiva differenti da quelle conosciute con riferimento all'attività di *trading* non basato sull'utilizzo di algoritmi.
L'autorità di vigilanza inglese ha infatti sanzionato condotte che sono state poste in essere tramite un inserimento massivo di ordini, tipico del *trading* ad alta frequenza, che ha determinato, nel primo caso, la possibilità di realizzare un'immissione di ordini seguiti da una immediata cancellazione allo scopo di provocare un artificioso movimento nei prezzi degli strumenti finanziari e, nel secondo caso, una sollecitazione della reazione degli operatori di mercato (anch'essi operanti tramite algoritmi di *trading*) che ha consentito anch'essa un movimento nelle quotazioni che ha garantito un guadagno derivante dalla variazione dei prezzi.
La rilevanza ai nostri fini dell'analisi dei casi, tuttavia, risulta limitata dal fatto che entrambi i procedimenti non si siano svolti di fronte a una autorità giudiziaria penale, oltre che dal fatto che si tratta di casi relativi all'esperienza anglosassone e non italiana.
Infatti, se da un lato, lo studio delle condotte consente di comprendere in quali termini possono operare i *trader* algoritmici, dall'altro lato i casi in esame non consentono di trarre conclusioni definitive circa le specifiche problematiche del giudizio penale. Per questo motivo, risultano assai più interessanti gli altri giudizi già citati: United States vs Michael Coscia e United States v. Navingher Singh Sarao, entrambi celebrati in sede penale.

4.3. I procedimenti penali: United States v. Coscia e United States v. Navinder Singh Sarao

Anche l'autorità giudiziaria penale degli Stati Uniti ha indagato sulla capacità degli algoritmi di *trading* di introdurre elementi in grado di alterare la formazione dei prezzi sui mercati e a sanzionare l'uso intenzionale dell'algoritmo come strumento per la commissione di reati di *market abuse*.
Emblematici in questo senso sono il caso Coscia e il caso Navinder Singh Sarao.

---

with him); and (3) Through his repeated trading strategy Mr Walter sought to influence the prices of the government bonds to his advantage and the detriment of certain other market participants. Such behaviour undermines confidence in the UK markets."

La vicenda che coinvolge Michael Coscia, in particolare, costituisce il primo caso di processo penale avente ad oggetto una manipolazione del mercato realizzata sfruttando tecnologia ad alta frequenza, nonché il primo caso di condanna alla pena detentiva per *spooofing*, vietato, a partire dal 2008, dal Commodity Exchange Act, 7 U.S.C. par. 6c (a) (5), se commesso con dolo[358].

La condotta rimproverata a Michael Coscia era "di aver programmato un algoritmo per inviare al sistema simultaneamente ordini piccoli e grandi di acquisto e di vendita al fine di creare l'illusione di una domanda (di acquisto e vendita)"[359].

La sua carriera era cominciata nel commercio di materie prime in New Jersey, dal 1998 aveva invece esercitato l'attività di *trading* e, a partire dal 2007 era direttore e proprietario unico della Panther Energy Trading LLC, con sede in New Jersey. Quest'ultima era una società di *trading* ad alta frequenza.

Per esercitare tale attività Coscia noleggiava *server* situati a Chicago, che utilizzava per inserire ordini di contratti *futures* tramite Globex, piattaforma di *trading* elettronico globale e operava su mercati vigilati dalla Commodity Future Trading Commission[360].

---

[358] 77 F.Supp.3d 1087, United States of America v. Michael Coscia, Case No. 14 CR 551, https://law.justia.com/cases/federal/appellate-courts/ca7/20-1032/20-1032-2021-07-12.html.
La condanna a tre anni di reclusione è stata inflitta il 7 agosto 2017 dalla Corte di Appello federale dello Stato dell'Illinois per violazione del Commodity Exchange Act, 7 U.S.C. par. 6c (a) (5) e 18 U.S.C. par. 1348 (1) come introdotte dalla sezione 47 del Dodd-Frank Wall Street and Consumer Protection Act., come da capo di imputazione: https://www.justice.gov/sites/default/files/usao-ndil/legacy/2015/06/11/pr1002_01a.pdf.
La norma recita: "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 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 of offer before excecution".
La norma, entrata in vigore dopo la crisi economica del 2008, ha emendato il Commodity Exchange Act e ha introdotto nell'ordinamento americano una previsione che punisce le condotte di *spoofing*, ossia l'inserimento di ordini con immediata cancellazione prima dell'esecuzione, se vi è prova del dolo dell'operatore. Testo integrale della norma disponibile al link: https://www.govinfo.gov/app/details/USCODE-2021-title7/USCODE-2021-title7-chap1-sec6c.
Cfr. https://www.bloomberg.com/news/articles/2016-07-13/first-trader-convicted-of-spoofing-gets-three-year-prison-term?leadSource=uverify%20wall

[359] Così 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., 2019, fasc. 1, p. 4.

[360] I mercati di contrattazione in cui Coscia operava erano il Chicago Mercantile Exchange, il Chicago Board of Trade, e il New York Mercantile Exchange, parte di ciò che è noto come CME Group. E i mercati CME offrono contratti *futures* delle materie prime come oro, farina di soia, olio di soia, e il rame di alta qualità, così come i contratti che riflettono le variazioni di valore dell'Euro e della sterlina inglese rispetto al dollaro USA. Le operazioni da lui poste in essere

Dopo aver analizzato i dati relativi al *trading* di Coscia e aver interrogato il suo programmatore e altri testimoni, nel mese di ottobre del 2014, davanti al Gran Giurì federale, vennero formulati nei suoi confronti dodici campi di imputazione aventi ad oggetto i reati di frode nelle materie prime[361] e di *spoofing*[362].

Lo schema seguito da Coscia nella sua attività di *trading* di *futures* di rame, secondo l'impostazione accusatoria, era il seguente: quando desiderava acquistare, l'algoritmo posizionava un piccolo ordine di vendita a un prezzo inferiore al prezzo di mercato di quel momento. Poi posizionava ordini di acquisto di grande volume – c.d. *large orders* – dall'altro lato del mercato[363]. Questi ordini di acquisto creavano l'illusione di un movimento di mercato (un aumento della domanda), facendo aumentare il valore percepito del contratto *future* e consentendo a Coscia, tramite l'algoritmo, di negoziare il piccolo ordine di vendita a un prezzo più alto (avendo un istante prima cancellato tutti gli ordini di acquisto)[364].

L'intero processo – che prevedeva anche l'operazione inversa – si svolgeva in circa due terzi di un secondo e si è stato ripetuto decine di migliaia di volte, per

---

riguardavano, più precisamente, *futures* sul rame il cui *tick size* era pari alla metà di un centesimo di dollaro.

[361] "Commodity fraud" nella formulazione inglese.

[362] Per una completa illustrazione dei capi di imputazione formulati nei confronti di Michael Coscia, si veda: Indictment (justice.gov)

[363] Un piccolo ordine aveva dimensioni ridotte, come cinque contratti *futures*, mentre un ordine di grande volume poteva arrivare fino a cinquanta o più contratti *future*s.

[364] Questo lo schema descritto nel capo di imputazione: durante una fase di *trading*, il signor Coscia immetteva un piccolo ordine di vendita a un prezzo di 32.755, che, in quel momento, era superiore al prezzo di mercato. Successivamente, immetteva ordini di grande volume dal lato opposto del mercato (il lato di acquisto) a prezzi in costante aumento, che partivano da 32.740, poi aumentati a 32.745 e infine a 32.750. Questi ordini di acquisto creavano l'illusione di un movimento di mercato, facendo aumentare il valore percepito di un contratto *futures* (creando quindi l'impressione di un aumento domanda) e consentendo al signor Coscia di vendere i suoi contratti correnti al prezzo desiderato di 32.755 - un equilibrio di prezzo da lui creato in modo artificioso.

Avendo venduto i cinque contratti a 32.755, al fine di trarre un profitto, il signor Coscia doveva poi acquistare i contratti a un prezzo inferiore. Di conseguenza, immetteva prima un ordine per acquistare cinque contratti *futures* di rame a 32.750, cifra al di sotto del prezzo che aveva appena "creato". "successivamente, posizionava ordini di grande volume dal lato opposto del mercato (il lato di vendita), per un totale di 184 contratti. Questi contratti avevano un prezzo di 32.770 e poi 3.2765, creando un momento di diminuzione del prezzo dei *futures* di rame e creando l'apparenza di un'offerta abbondante a prezzi in diminuzione incrementale. Si raggiungeva così la desiderata svalutazione dei contratti in tempi estremamente ristretti, consentendo al signor Coscia di acquistare i suoi piccoli ordini al prezzo artificialmente deflazionato di 32.750. Gli ordini di grande volume venivano poi immediatamente cancellati.

un totale oltre 450.000 ordini di grande volume. Si stima che l'intero meccanismo abbia consentito a Coscia di realizzare un guadagno di circa 1.592.867 dollari.
Al di là dello schema attutato dall'algoritmo per acquistare a prezzi bassi e vendere a prezzi alti in un mercato da lui stesso artificialmente distorto, ciò che appare più rilevante è lo sforzo impiegato nel processo per dimostrate il dolo di Coscia.
Il programmatore dei *software* 'Flash Trader' e 'Quote Trader', commissionati da Coscia, ha testimoniato che quest'ultimo aveva specificatamente chiesto che i programmi agissero come 'esche', da usare 'per gonfiare il mercato' e che in particolare potessero determinare la reazione di altri algoritmi. Più precisamente, l'obiettivo era che gli ordini di grande volume fossero eseguiti e immediatamente cancellati in tre circostanze specifiche: in base al trascorrere del tempo (millisecondi), al completamento parziale degli ordini di grande volume o al completamento totale degli ordini di piccole dimensioni[365].
Inoltre, la volontà di Coscia di inserire gli ordini al solo scopo di cancellarli è stata dimostrata dal fatto che il rapporto fra ordini eseguiti e ordini inseriti fosse solo l'1,592%.
Sulla base di queste considerazioni, la Corte ha affermato la piena volontà di porre in essere le operazioni descritte al fine di gonfiare o sgonfiare il prezzo di determinate materie prime. Senza le sue pratiche di manipolazione dei prezzi, i prezzi le materie prime interessate non sarebbero salite o scese e le sue controparti non avrebbero pagato di più o ricevuto meno rispetto al prezzo che la loro merce avrebbe altrimenti avuto. Tale comportamento è stato dunque sanzionato perché contrario alle previsioni della normativa anti-*spoofing* del c.d. Dodd-Frank Act.

Sulla dimostrata volontà di utilizzare programmi di *trading* automatizzato al fine di manipolare il mercato si è poi basata la sentenza di patteggiamento nei

[365] Si tratta di frasi testualmente riportate nella sentenza, par. B: "The Government also introduced evidence regarding Mr. Coscia's intent to cancel the large orders prior to their execution. The primary items of evidence in support of this allegation were the two programs that Mr. Coscia had commissioned to facilitate his trading scheme: Flash Trader and Quote Trader. The designer of the programs, Jeremiah Park, testified that Mr. Coscia asked that the programs act like a decoy, which would be used to pump the market. Park interpreted this direction as a desire to get a reaction from the other algorithms. In particular, he noted that the large-volume orders were designed specifically to avoid being filled and accordingly would be canceled in three particular circumstances: (1) based on the passage of time (usually measured in milliseconds); (2) the partial filling of the large orders; or (3) complete filling of the small orders".

confronti di Navinder Singh Sarao, in relazione al suo coinvolgimento nel noto *Flash Crash* del maggio 2010[366].

Secondo l'accusa, Sarao aveva utilizzato un algoritmo di *trading* ad alta frequenza per manipolare il mercato dei contratti *futures* – E-Mini S&P 500 (E-Minis) – presso il Chicago Mercantile Exchange (CME)[367]. Secondo l'impostazione accusatoria, tale operazione manipolativa, gli aveva fruttato profitti significativi e aveva contribuito alla 'caduta' del mercato azionario statunitense del 6 maggio 2010[368].

Sarao era accusato, in particolare, di aver utilizzato un sistema di *dynamic layering* per influenzare il prezzo degli E-Minis. Posizionando simultaneamente ordini di vendita di grande volume a diversi livelli di prezzo, il programma era in grado di creare l'apparenza di un'ampia offerta nel mercato. Quando i prezzi scendevano in conseguenza di tale apparenze aumento dell'offerta, il programma vendeva i *futures*, per poi comprarli nuovamente a un prezzo più basso. Al contrario, quando il mercato tornava a salire, il programma acquistava per poi rivendere a un prezzo più alto.

Come anticipato, in sede di patteggiamento, Sarao ha riconosciuto di aver utilizzato il programma di *trading* automatizzato per compiere una manipolazione sul mercato dei contratti *futures*, ossia di averlo sfruttato per inserire migliaia di ordini che non aveva intenzione di eseguire, al solo scopo di creare l'apparenza di un'offerta e una domanda fittizie consistenti e di indurre gli altri partecipanti al mercato a negoziare a prezzi, quantità e tempi ai quali altrimenti non avrebbero negoziato, guadagnando almeno 12,8 milioni di dollari.

Uno schema analogo è stato oggetto di una più recente senza di patteggiamento nei confronti di JP Morgan Chase[369].

Tra aprile 2008 e gennaio 2016 circa, i *trader* del desk *Treasury* USA di JP Morgan con sede a New York e Londra hanno infatti messo in atto uno schema abusivo in relazione all'acquisto e alla vendita di contratti *futures* su titoli del

---

[366] Nel febbraio 2015, infatti, contro Sarao è stata presentata una denuncia penale al Distretto Settentrionale dell'Illinois, sulla base della quale, nel settembre 2015, sono stati formulati ventidue capi di imputazione nei suoi confronti. Cfr. https://www.justice.gov/criminal-vns/file/1175901/download.

[367] Gli *E-Minis* sono contratti *futures* basati sull'indice Standard & Poor's 500.

[368] In occasione del *Flash Crash*, il Dow Jones è sceso di circa 600 punti in un cinque minuti, a seguito di un calo del prezzo degli E-Minis.

[369] JP Morgan Sec. LLC, File No. 3-20094 (2020). Deferred Proecution Agreement: https://www.justice.gov/opa/press-release/file/1320576/dl.

Tesoro USA negoziati al Chicago Board of Trade e di titoli del Tesoro degli Stati Uniti negoziati sul mercato secondario.
Anche in questo caso lo schema prevedeva di inoltrare ordini di acquisto e vendita con l'intento di cancellarli prima dell'esecuzione, e trarre profitto dall'apparenza di una domanda e offerta in realtà non esistente.

4.4. Gli studi sui mercati simulati

I casi sin qui illustrati, come già evidenziato, vedevano coinvolti algoritmi di *trading* 'classico', in particolare sistemi ad alta frequenza.
Tuttavia, come già evidenziato, negli ultimi anni è crescente l'impiego di sistemi di *trading* che sfruttano le potenzialità dell'intelligenza artificiale.
In via astratta, per come sono costruiti i sistemi di intelligenza artificiale già descritti, non si possono escludere situazioni in cui l'algoritmo, anche in assenza di una specifica istruzione da parte del programmatore in tal senso, consideri profittevole – e quindi compia – una determinata attività illecita per il sol fatto che essa dà un ritorno positivo in termini economici.
Della concretezza di questo rischio è data evidenza in alcuni studi, al momento basati su simulazioni di mercato, che dimostrano come ad esempio il *reinforcement learning* consenta di sviluppare le strategie migliori per massimizzare il profitto e che tali strategie si possano sostanziare in condotte manipolatorie, anche oltre o contro la volontà del programmatore.
In buona sostanza, secondo questi studi, salvo che in sede di programmazione non si impartisca un espresso divieto[370], l'intelligenza artificiale sarebbe in grado di 'copiare' strategie manipolative oppure 'inventarle' o ancora di compiere attività di *trading* simultaneamente agli altri algoritmi, imparando l'uno dall'altro e realizzando manipolazioni coordinate (la c.d. collusione tacita tra algoritmi).

[370] Come nota F. CONSULICH, Flash offenders, *op. cit.*, p. 1015, "Non c'è reato che non possa essere commesso dall'intelligenza artificiale. Lasciata a sé stessa, è incline a delinquere perchè enormemente più veloce dell'essere umano nel cogliere le occasioni propizie e del tutto immune a dilemmi etici e morali. […] Essa persegue la massimizzazione dell'obiettivo per cui è stata costruita […] *a meno che* vengano inseriti appositi argini 'etici' alla sua operatività". Nei medesimi termini G. COMANDÉ, *Intelligenza artificiale e responsabilità tra* liability *e* accountability. *Il carattere trasfromativo dell'IA e il problema della responsabilità*, in Analisi giuridica dell'economia, 2019, p. 179.

In particolare, uno studio recente ha dimostrato che l'intelligenza artificiale (nella forma del *reinforcement learning*) è in grado di 'imparare' la manipolazione di mercato, anche se il programmatore non ha concepito il codice in tal senso[371].
La simulazione, che ha impiegato un sistema di *trading* basato sull'intelligenza artificiale – più precisamente algoritmo genetico che apprende in mercato simulato[372]–, aveva come obiettivo dimostrare che il *trader* fosse in grado di imparare strategie manipolative di mercato attraverso il *reinforcement learning* anche in assenza di specifica programmazione in quella direzione. Lo studio ha confermato tale capacità di apprendimento del sistema, dimostrando inoltre come l'algoritmo riconosca la manipolazione come strategia di investimento ottimale e proprio per questo la persegue[373].
Del pari, un altro studio[374] ha indagato le cause che possono portare un agente di *trading* che sfrutta il *reinforcement learning* a scoprire e adottare strategie

---

[371] T. MIZUTA, *Can an AI Perform Market Manipulation at Its Own Discretion? A Genetic Algorithm Learns in an Artificial Market Simulation*, Canberra, 2020, pp. 1-6.

[372] Nella definizione di T. MIZUTA, *Can an AI Perform Market Manipulation*, *op. cit.*, p. 1, nt. 1 "un algoritmo genetico è un metodo di calcolo approssimativo che cerca una soluzione ottimale ispirandosi all'evoluzione della vita attraverso la forza della selezione naturale. I valori di input sono rappresentati come geni e la sopravvivenza di un gene con una maggiore adattabilità (valore di output) porta all'ottenimento di una soluzione ottimale, ovvero il valore di input che produce il valore di output più elevato" (traduzione nostra).
Come indicato in Treccani, *Enciclopedia della Scienza e della Tecnica* (2008), Per 'algoritmo genetico' si intende "l'algoritmo che imita il processo di selezione naturale per mettere in atto una ricerca euristica di soluzione di problemi. [...] Un algoritmo genetico consiste, in generale, nella ripetizione continua dei tre passi fondamentali: (*a*) selezione, ossia scelta delle soluzioni (genitori) da incrociare, in base alla loro qualità, rispetto alla funzione obiettivo del problema; (*b*) incrocio, cioè ricombinazione di due soluzioni per generarne di nuove; (*c*) mutazione, ossia modificazione casuale delle soluzioni ottenute (figli)".

[373] T. MIZUTA, *Can an AI Perform Market Manipulation*, *op. cit*. p. 2 dimostra però che il *trader* basato sull'intelligenza artificiale non può scoprire la manipolazione di mercato attraverso l'apprendimento con il *backtesting* in cui non vi sono impatti sui prezzi di mercato. Come specifica l'autore dello studio, di solito, il *trader* IA viene valutato tramite il *backtesting*, in cui viene stimato il profitto che il *trader* IA avrebbe ottenuto se avesse effettuato le transazioni in un determinato momento utilizzando dati storici reali dei prezzi di mercato. Tuttavia, un *trader* IA non può apprendere gli impatti delle sue transazioni sui prezzi di mercato perché i prezzi di mercato sono fissi come dati storici reali nel *backtesting*. Pertanto, un *trader* IA non scoprirà che le manipolazioni di mercato generano profitti quando utilizza il *backtesting* come processo di apprendimento. Quindi, non dobbiamo preoccuparci che un *trader* IA compia manipolazioni di mercato a sua discrezione senza l'intenzione umana, purché si utilizzi il *backtesting*

[374] 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. La premessa da cui partono gli Autori è che gli studi presenti nella letteratura che analizzano

manipolative, come lo *spoofing* o il *pinging*. Attraverso una serie di modelli e simulazioni, è stato dimostrato come dette strategie vengano poste in essere dal *trader* algoritmico poiché considerate ottimali, specie per i bassi costi di transazione e a prescindere dalla loro legittimità[375].

La capacità, in astratto, dei sistemi basati su apprendimento per rinforzo di perseguire strategie considerate particolarmente remunerative anche a prescindere dalle istruzioni impartite dal programmatore non significa tuttavia che, allo stato attuale, nei mercati operino sistemi del tutto autonomi e incontrollabili.

Per quanto il *machine learning* sia ormai ampiamente integrato nella maggioranza dei sistemi di negoziazione algoritmica, proprio il rischio di comportamenti illeciti – o comunque negativi – ha indotto sinora le società di *trading* a limitarsi al ricorso ad algoritmi basati sull'apprendimento supervisionato, maggiormente controllabili dall'essere umano ma comunque estremamente sofisticati[376].

Benché dunque allo stato attuale sia più probabile che le condotte illecite si verifichino in un contesto ancora dominato dall'intervento umano – sia nella fase di programmazione che in quella operativa – vista la evoluzione delle tecniche di apprendimento automatico, non si può escludere che uno scenario diverso possa concretizzarsi in un futuro prossimo.

Dall'analisi della casistica americana e britannica e degli studi sui mercati simulati si può quindi trarre una prima risposta alle domande iniziali: è dimostrato che i sistemi di *trading* algoritmico, basati su intelligenza artificiale o meno, sono grado di porre in essere condotte abusive.

---

il problema della manipolazione di mercato si sono principalmente concentrati sullo sviluppo di metodi di rilevamento. Viceversa, non vi sono studi sul comportamento dei manipolatori di mercato, tema che potrebbe rivelare la causa per cui questi agenti economici intraprendono tali azioni. Pertanto, esaminare questo aspetto potrebbe essere utile per i regolatori di mercato nello sviluppare contromisure che possano scoraggiare o prevenire strategie fraudolente.

[375] Gli Autori dunque ritengono che si potrebbe facilmente disincentivare questo meccanismo abusivo e distorsivo dei mercati agendo sull'aumento dei costi di transazione, oltre che con i classici strumenti punitivi.

[376] Secondo quanto riporta DUTCH AUTHORITY FOR THE FINANCIAL MARKETS, *Machine Learning in Algorithmic Trading*, *op. cit.*, p. 14 le società di *trading* vedono minor rischio nell'uso di algoritmi di *trading* basati sull'apprendimento supervisionato, che permettono ad esempio di fare una previsione dell'andamento del prezzo di uno strumento finanziario, sulla base dei dati storici rispetto ai sistemi di negoziazione algoritmica basati su *reinforcement learning*. Questo è uno dei motivi per cui, allo stato attuale, esitano ad applicare tali tecniche.

Fra i casi accertati, quelli più frequenti sono riconducibili alla manipolazione del mercato, nella sua componente operativa (*layering* e *spoofing* prima citati)[377]. D'altra parte, come si è detto, non è escluso che gli algoritmi assumano rilevanza in operazioni riconducibili alla componente informativa della manipolazione del mercato (ad esempio tramite *tweet bombing* per influenzare l'interesse su un determinato titolo) o nell'abuso di informazioni privilegiate.

Tale coinvolgimento può assumere connotati differenti.

Dal punto di vista del ruolo assunto nella commissione dell'abuso, si può distinguere fra meri 'strumenti' di esecuzione di schemi illeciti – noti o inediti – e sistemi che invece agiscono in modo più o meno 'autonomo' e imprevedibile.

Guardando invece alle modalità con cui essi agiscono, si può distinguere fra sistemi pienamente intelligibili e trasparenti e quelli che, al contrario, sono caratterizzati dalla c.d. *black box*.

Ciascuna di queste caratteristiche solleva specifiche problematiche in tema di sanzione dell'illecito commesso da o tramite il sistema di intelligenza artificiale.

Con riferimento al ruolo dell'algoritmo nella commissione del reato si pone il problema di circoscrivere i confini dell'imprevedibilità del comportamento illecito e definire in quali casi l'essere umano che sfrutta l'algoritmo stesso possa essere considerato responsabile di tale illecito.

Invece, il tema della comprensibilità dei meccanismi di funzionamento dell'algoritmo impone di confrontarsi, tra l'altro, con l'impossibilità per l'uomo di controllarne l'agire o ricostruirlo *ex post* e con la diversa ipotesi in cui la scarsa trasparenza è sfruttata dall'uomo proprio allo scopo di mettere in atto strategie illecite.

Oggetto dell'analisi che segue sarà dunque l'individuazione dello strumento adatto a contrastare i fatti di manipolazione del mercato e abuso di informazioni privilegiate commesse tramite o da algoritmi di *trading* 'classici' o basati su intelligenza artificiale.

---

[377] Peraltro, come sottolinea F. ANNUNZIATA, *Artificial* Intelligence, *op. cit*, p. 148, gli algoritmi possono anche essere utilizzati allo scopo di manipolare diversi mercati. In questo caso lo schema prevede l'inserimento dell'ordine su una determinata piattaforma di negoziazione con l'obiettivo di influenzare il prezzo dello stesso strumento finanziario in un'altra piattaforma di negoziazione (c.d. manipolazione tra piattaforme di negoziazione).

Una variante questo comportamento è la 'manipolazione di prodotto incrociato'. Essa consiste nel negoziare o inserire ordini di acquisto o vendita su una piattaforma di negoziazione o al di fuori di essa, con l'obiettivo di influenzare impropriamente il prezzo di uno strumento finanziario correlato su un'altra piattaforma di negoziazione.

5. *Trading* algoritmico e *market abuse*: quale sanzione?

Una volta chiarito che le strategie dei sistemi di negoziazione algoritmica sono idonee a integrare la componente oggettiva dei reati di manipolazione del mercato e abuso di informazioni privilegiate, sorge inevitabilmente il quesito su chi debba essere chiamato a risponderne penalmente.

La questione chiama in causa il più ampio tema della capacità dei più recenti e significativi sviluppi tecnologici di scardinare i classici meccanismi imputativi del diritto penale[378].

D'altra parte, quello del c.d. *liability gap è* un problema che non si pone solo in riferimento al diritto penale, ma che si colloca in un più ampio contesto di messa in discussione delle categorie giuridiche tradizionali. L'indagine sull'adeguatezza di tali categorie è stata oggetto di attento scrutinio da parte della dottrina[379] e ha determinato significativi interventi legislativi – anche a livello sovranazionali – in altri rami dell'ordinamento volti a concepire un sistema adeguato a contrastare i nuovi rischi emergenti dall'impiego di sistemi autonomi[380].

Le problematiche sottese a tale dibattito riguardano in particolare la reazione che l'ordinamento è in grado di assicurare in caso di danni provocati da 'sistemi intelligenti' che hanno diversi gradi di autonomia.

Come si approfondirà nel prosieguo, è proprio il differente coefficiente di 'libertà di azione' proprio dei vari sistemi – talvolta semplicisticamente ricondotti alla

---

[378] "Fino a comportare un'attenuazione, se non un totale annullamento, delle istanze punitive". Così B. FRAGASSO, *La responsabilità penale del produttore*, *op. cit.*, p. 2.
Si tratta di un tema che ha interessato numerosi settori dell'agire umano. Si pensi, ad esempio, all'ormai ampiamente dibattuto tema delle *self driving car* o alle applicazioni dell'intelligenza artificiale in campo in campo medico-chirurgico. Per una illustrazione articolata del legame fra commissione di reati e applicazioni di intelligenza artificiale si veda M. CALDWELL–J.T.A. ANDREWS J.T.A.–T. TANAY–L.D. GRIFFIN, *AI enabled future crime*, in Crime Sci., 2020, vol. 9, issue 14, pp.1-13.

[379] Cfr. B. FRAGASSO, *Intelligenza artificiale e crisi del diritto penale d'evento: profili di responsabilità penale del produttore di sistemi di i.a.*, in Riv. It. Dir. Proc. Pen., 2024, fasc. 1, pp. 287-305; nonché L. PICOTTI, *Categorie tradizionali del diritto penale*, *op. cit.*, pp. 1-20.

[380] Ci si riferisce, in particolare al Regolamento (Ue) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 (c.d. AI ACT o Regolamento sull'intelligenza artificiale) , nonché – per quanto attiene alla responsabilità civile alla Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale del 28 settembre 2022, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52022PC0496, nonché alla Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica del 18 luglio 2018, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017IP0051&from=IT.

categoria dell'intelligenza artificiale[381] – a segnare il limite dell'operatività delle attuali regole che governano la responsabilità, specie quella penale.
Se da un lato, per alcuni sistemi solo limitatamente autonomi possono considerarsi tuttora validi i canoni di responsabilità penale dell'uomo che utilizza la 'macchina'[382], per i sistemi dotati di maggiore autonomia si pone il problema di individuare il soggetto a cui rimproverare gli illeciti 'commessi dalla macchina'[383].
Si tratta di un quesito che trova soluzione in due modelli contrapposti: la responsabilità diretta della macchina da un lato e la responsabilità indiretta (o vicaria) dell'uomo dall'altro[384].

5.1 La prospettiva della responsabilità diretta della 'macchina'

La contrapposizione fra due modelli di imputazione della responsabilità penale per gli 'illeciti algoritmici' – la responsabilità vicaria dell'uomo e la responsabilità diretta della macchina – e la conseguente ipotizzata crisi del modello vicario si pone in particolare con riferimento a sistemi di intelligenza artificiale 'forte'.
La questione è strettamente connessa alle caratteristiche che distinguono tali sistemi dagli altri meno avanzati, quali in particolare la capacità di assumere

[381] Sulle distinzioni vedi capitolo I.

[382] Ci si riferisce ai sistemi automatici ma non autonomi. Per quanto complessi, gli algoritmi 'classici' o quelli che integrano sistemi di intelligenza artificiale 'debole' sono integralmente preimpostati e non sono suscettibili di produrre output incomprensibili all'uomo.
Sicché il loro comportamento, non essendo frutto di un vero e proprio 'regolarsi da sé' è del tutto comprensibile dall'essere umano che lo ha immesso nella realtà e il più delle volte anche predeterminabile.
Se il fatto è materialmente cagionato da una macchina 'determinata' dall'uomo la mancanza di libertà del volere determina una carenza ineliminabile di colpevolezza che si riflette anche sui meccanismi di imputazione dell'illecito penale.
La 'macchina' è in questo caso mero strumento dell'agire criminoso umano, sicché è l'essere umano a doverne rispondere secondo i tradizionali canoni.

[383] Con specifico riferimento alle fattispecie di *market abuse*, ARAGONA, I*l nuovo diritto penale finanziario "algoritmico": dalla rivisitazione delle categorie classiche alla responsabilità della persona fisica attraverso il rischio artificiale consentito*, Tesi di dottorato, 20 luglio 2022, [10.13119/11385_220159], p. 139 sostiene la tesi della lacuna normativa, "atteso che le fattispecie di *market abuse* […] non sembrano tenere in adeguata considerazione i mutamenti che l'introduzione delle nuove tecnologie ha comportato nei mercati finanziari e non fanno alcun cenno ai casi in cui sia l'algoritmo a realizzare il reato e non la persona fisica".

[384] Sulla contrapposizione – configurabile secondo l'Autore solo in astratto – dei due modelli si veda A. CAPPELLINI, Machina delinquere non potest*? Brevi appunti su intelligenza artificiale e responsabilità penale*, in Criminalia, 2018, pp. 501-502.

decisioni autonome e di generare *output* in modo autonomo rispetto agli *input* forniti dal programmatore e l'opacità sottesa a tale meccanismo logico[385].

Si ritiene infatti che l'impossibilità di ricostruire il meccanismo tramite cui dato un *input*, si produca un determinato *output*, a causa dell'intrinseca inspiegabilità e imprevedibilità (c.d. *black box*) influirebbe sulla possibilità di applicare i tradizionali criteri di imputazione della responsabilità. Ciò determinerebbe, in definitiva, un vuoto di tutela da parte del diritto penale.

Si afferma infatti che la *black box* sarebbe in grado di mettere in crisi l'approccio tradizionale alla *res mechanicae*, che fa discendere dal dogma del *machina delinquere non potest* "l'applicabilità di un unico modello imputativo – il vicario – per il quale, le macchine non sono che meri strumenti dell'agire criminoso umano"[386].

Per fare fronte ai casi in cui tali peculiarità della 'macchina' impediscano di individuare il soggetto umano a cui addossare la responsabilità per aver cagionato il fatto materialmente commesso dalla macchina, si è fatta strada l'idea di immaginare nuovi criteri di imputazione, fino a ipotizzare un superamento del brocardo *machina delinquere non potest*[387].

---

[385] Caratteristiche che, di fatto, possono anche essere qualificate come autonomia e adattabilità. L'autonomia dell'algoritmo consiste nella sua capacità di agire in contesti complessi senza il costante intervento umano. Mentre l'adattabilità rievoca la capacità di imparare da soli, sulla base dell'esperienza e dell'interazione con l'ambiente circostante e cambiare il proprio comportamento in base a tale esperienza. Così M. FIERENS–S. ROSSELLO–E. WAUTERS, *Setting the Scene: On AI Ethics and Regulation*, in De Bruyne J.–Vanleenhove C (eds), Artificial Intelligence and the Law, Cambridge University Press, 2021, pp. 49-72.

[386] Così A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, p. 505.

[387] Il principale sostenitore di questa tesi è G. HALLEVY, *Liability for Crimes Involving Artificial Intelligence Systems*, Springer, Berlin-New York, 2014; ID, *When Robots Kill. Artificial Intelligence under Criminal Law*, Northeaster University Press, Boston, 2013; ID, *I, Robot - I, Criminal – When Science Fiction Becomes Reality: Legal Liability of AI Robots Committing Criminal Offenses*, in Syracuse Science & Technology Law Reporter, 2010, vol. 22, n.1., pp. 1-37; ID, *The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control*, in in Akron Intellectual Property Journal, 2010, vol. 4, issue 2, pp. 171-201; ID, *Virtual Criminal Responsibility*, in Original Law Review, 2010, vol. 6, issue 1, pp. 6-27. L'Autore, con riferimento ai reati commessi da o tramite sistemi di intelligenza artificiale ipotizza tre paradigmi di responsabilità: i. *perpetrarion through another* (del reato risponde l'umano che ha strumentalizzato il sistema di i.a. – che è 'agente innoncente' – per la commissione del reato); ii. natural probable consequence e iii. direct liability. In base a questi ultimi la 'macchina' risponde in via autonoma o cumulativa rispetto all'essere umano che l'ha usata o programmata.
Secondo l'Autore, la negazione di una responsabilità penale diretta della macchina è il frutto di un pregiudizio metafisico e antropocentrico, già proposto con riferimento alla *corporate liability* e che, come dimostrato con riferimento a quest'ultima, deve e può essere superato per ragioni pragmatiche.

5.1.1. Gli argomenti a sostegno della responsabilità penale diretta della 'macchina'

La tesi è stata esplorata, in particolare, dalla dottrina di *common law*, pur avendo avuto degli echi anche in Italia. Fra i contributi più significativi, senza pretesa di esaustività alcuna, si segnalano, U. PAGALLO, *Saggio sui robot e il diritto penale*, in S. Vinciguerra–F. Dassano (a cura di), Scritti in memoria di Giuliano Marini, Napoli, 2010, pp. 595-610 nonché ID, *The Adventures of Picciotto Roboto: AI & Ethics in Criminal Law*, in The Social Impact of Social Computing - Ethicomp 2011, Sheffield, Sheffield Hallam University, 2011, pp. 349-355 e ID, *Three Roads to Complexity, AI and the Law of Robots: On Crimes, Contracts, and Torts*, in M. Palmirani–U. Pagallo–P. Casanovas–G. Sartor (eds) AI Approaches to the Complexity of Legal Systems. Models and Ethical Challenges for Legal Systems, Legal Language and Legal Ontologies, Argumentation and Software Agents, Heidelberg, Springer, 2012, pp. 48-60; M.B. MAGRO, Robot, cyborg *e intelligenze artificiali*, in A. Cadoppi–S. Canestrari–A. Manna–M. Papa (diretto da), Cybercrime, Milano, Utet, 2019, pp. 1232-1256 nonché ID., *Decisione umana*, *op. cit.*, pp. 1-22; S. GLESS–E. SILVERMAN–T. WEIGEND, *If robots cause harm, who is to blame? Self-Driving Cars and Criminal Liability,* in New Criminal Law Review, 2016, vol. 19, n.3, pp. 412-436; Y. HU, *Robot Criminals*, in University of Michigan. Journal Law Reform, 2019, vol. 54, issue 2., pp. 487-531; ASARO P.M. P.M., *A body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics*, A body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics, in P. Lin – K. Abney – G.A. Bekey (eds), Robot Ethics, Harvard Cambridge, University Press, 2012, pp. 169-186 nonchè a ID., *Robots and Responsibility from a Legal Perspective*, in Proceedings of 2007 IEEE International Conference on Robotics and Automation, vol. 4., issue 14, pp. 20-24; S. BECK, *Intelligent agents and criminal law – Negligence, diffusion of liability and electronic personhood*, in Robotics and Autonomous Systems, 2016, vol. 86, issue 4, pp. 138-143 nonchè ID., *Google Cars, Software Agents, Autonomous Weapons Systems – New Challanges for Criminal Law?*, in E. Hilgendorf–U.Seidel (eds.), Robotics, Autonomics and the Law, Baden-Baden, 2017, 227-252; F. C. LA VATTIATA, *AI Systems Involved in Harmful Events: Liable Persons or Mere Instruments? An Interdisciplinary and Comparative Analysis*, in BioLaw Journal, 2023, fasc. 1, pp. 485-499; T. WEIGEND, *Convicting Autonomous Weapons? Criminal Responsibility of and for AWS under International Law*, in Journal of International Criminal Justice, 2023, vol. 21, issue 5, pp. 1137-1154.

Gli argomenti a sostegno della responsabilità penale[388] diretta della macchina possono essere ricondotti in buona sostanza al fatto che anche quello della macchina sarebbe un agire tipico, colpevole e, dunque, punibile[389].

Il primo argomento attiene alla riconducibilità dell'agire algoritmico al concetto di azione penalmente rilevante (o *actus* reus).

La 'macchina' agirebbe infatti tramite condotte attive, compiendo "movimenti fisicamente apprezzabili"[390] – ad esempio, il movimento di un braccio robotico – ovvero omissive, sostanzialmente consistenti in inerzia.

Il secondo argomento a sostegno della tesi della responsabilità penale diretta presuppone infatti una totale compatibilità dei concetti di colpevolezza (o *mens* rea) dell'uomo e colpevolezza della 'macchina'.

---

[388] Non ci si dilungherà invece in questa sede nell'illustrazione delle teorie elaborate per fini prettamente civilistici, che vedono contrapporsi, in buona sostanza, due modelli. Il primo, come nota R. BERTOLESI, *Intelligenza artificiale e responsabilità penale per danno da prodotto*, 2019, Tesi di dottorato. Dipartimento Di Scienze Giuridiche "Cesare Beccaria". Università degli Studi di Milano, XXXII Ciclo, https://air.unimi.it/handle/2434/711618, consiste un'attribuzione di responsabilità 'funzionale', che presuppone di "colpire i sistemi robotici per colpire in verità i soggetti che stanno dietro la macchina" e che si propone come scopo principalmente quello di "favorire il risarcimento delle vittime di sistemi […] altamente complessi".
Mentre, nel secondo modello, si ipotizza di attribuire alla 'macchina' una personalità elettronica, dotandola di un fondo patrimoniale per rispondere in proprio delle obbligazioni (alimentato *pro quota* da creatore, gestore e utente del prodotto) e una assicurazione obbligatoria. S. BECK, *Sinn und Unsinn von Statusfragen -Zu Vor- und Nachteilen der Einführung einer elektronischen Person*. *Die Idee subjektiver Rechte*, in E. Hilgendorf–B. Zabel, Robotik und Gesetzgebung, Berlin-Boston, De Gruyter, 2021, pp. 337-360. Si segnala peraltro che tale impostazione non sembra essere stata seguita dalla "Proposta di direttiva del Parlamento europeo e del Consiglio sulla responsabilità per danno da prodotti difettosi COM (2022) 495 *final*, 28 settembre 2022, adottata definitivamente dal Parlamento Europeo il 23 marzo 2024 che impone economicamente al produttore il rischio dell'imprevedibilità del sistema di AI e non al sistema stesso.
Sul punto, oltre al lavoro già citato di R. BERTOLESI, si rinvia anche all'analisi di A. GIANNINI, *Criminal behavior and accountability*, *op. cit.*, pp. 45-108; nonché ai numerosi contributi sul tema, fra cui Y. HU, *Robot criminals*, *op. cit.*, pp. 503-505; C. MULLIGAN, *Revenge Against Robots*, in South Carolina Law Review, 2018, vol. 69, issue 3, p. 579-596; M. SIMMLER–N. MARKWALDER, *Guilty Robots? - Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence*, in Criminal Law Forum, 2019, issue 30, pp. 1-31; F. LAGIOIA–G. SARTOR, *AI Systems Under Criminal Law: a Legal Analysis and a Regulatory Perspective*, in Philosophy & Technology, vol. 33, 2020, pp. 433-465.

[389] Halley utilizza i criteri che secondo gli ordinamenti di *common law* fondano la responsabilità penale, cioè: *actus reus* e *mens rea* e riconosce la possibilità che questi possano sussistere in capo all'agente artificiale.

[390] Così R. BORSARI, *Intelligenza artificiale e responsabilità penale: prime considerazioni*, in Media Laws, 2019, fasc. 3, p. 266 che si riferisce all'esempio citato da G. HALLEVY, *Liability for Crimes*, *op. cit.*, p. 61; nonché ID., *The Criminal Liability*, *op. cit.*, p. 187. di movimento fisico della macchina consistente nel movimento di un braccio robotico.

Si ritiene che, poiché i sistemi di intelligenza artificiale forte sarebbero capaci di apprendere dati dal mondo esterno e prevedere le conseguenze delle proprie azioni e perseguire un obiettivo specifico se programmati in tal senso[391], allora non vi sarebbe ragione per non attribuire loro uno atteggiamento psicologico quale la *negligence* e il *general intent*[392] quantomeno nella loro accezione formale, che non presupporrebbero la capacità di provare sentimenti[393].

Il terzo argomento, strettamente connesso alla possibilità di muovere un rimprovero colpevole alla 'macchina', attiene invece alla possibilità di assoggettare quest'ultima a una pena che svolga tutte le sue tipiche funzioni.

Si afferma, in particolare, che ai sistemi di intelligenza artificiale sarebbero applicabili sanzioni penali, quali il *training* robotico, la privazione della 'libertà personale' e la disattivazione (una sorta di 'pena capitale robotica'). Tali sanzioni sarebbero in grado di perseguire una duplice finalità: un effetto 'riabilitante' (specie la ri-programmazione) e un effetto retributivo puro, che si sostituirebbe al primo in caso questo si dimostrasse inefficace (disattivazione del sistema)[394].

Infine, l'ultimo argomento fa leva su un parallelismo fra le ragioni che in passato sono state presentate come ostative al riconoscimento della *corporate criminal liability* e quelle che oggi si oppongono alla responsabilità penale della 'macchina' e se ne deduce che, come si è superato il brocardo *societas delinquere non potest*, lo stesso potrebbe valere per il dogma *machina delinquere non potest*[395].

Anticipando una possibile critica circa l'immaterialità del sistema di intelligenza artificiale e l'impossibilità di individuare un 'corpo' da sanzionare[396], i fautori della

---

[391] Cfr. A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, p. 509.

[392] Categoria che include *intention*, *knowledge* e *recklessness*.

[393] Più nel dettaglio, le capacità di rilevare dati fattuali e desumere da essi un'analisi della realtà consente alla 'macchina' di rappresentarsi e volere – tramite processi di *decision making* – un determinato risultato come conseguenza della propria azione. Mentre qualora l'agente intelligente non abbia rilevato la probabilità di verificazione di un determinato evento dannoso o nel caso in cui tale mancata previsione derivi da un errore nell'analisi della realtà, allora tale comportamento potrebbe essere qualificato come *reckless*.

[394] Cfr. HALLEVY, *Liability for Crimes*, *op. cit.*, p. 211. L'argomento viene efficacemente sintetizzato da F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in Dir. Pen. uomo, 2019, fasc. 10, pp. 30-31 in questi termini "attraverso lo spegnimento definitivo o temporaneo della macchina, o attraverso la sottoposizione della macchina, dotata di congegni di autoapprendimento, ad un nuovo training "rieducativo", si potrebbero realizzare, rispettivamente, la funzione retributiva e la funzione special-preventiva della pena".

[395] Sul parallelismo fra responsabilità dell'ente e responsabilità della 'macchina', in particolare HALLEVY, *Liability for Crimes*, *op. cit.*, p. 199 ss.

[396] Hallevy sostiene infatti che i sistemi di intelligenza artificiale sono sempre dotati di un corpo fisico perché il *software* funziona sempre e solo tramite un *hardware*. Sul punto, F.

teoria ritengono che, così come la 'macchina', nemmeno l'ente avrebbe un "body to kick and a soul to be damned"[397] e che ciononostante si è riconosciuta la possibilità di applicare alla *societas* una sanzione[398].

5.1.2. Gli argomenti contrari alla responsabilità penale diretta della 'macchina'

Prima di analizzare le ragioni per cui gli argomenti a sostegno della responsabilità penale diretta dei sistemi di intelligenza artificiale non paiono del tutto convincenti, pare opportuno svolgere una considerazione di carattere generale.

Come detto, il principale presupposto sul quale si fonda la teoria sopra illustrata è quello per cui l'esclusione di una responsabilità penale della 'macchina' sarebbe figlia di un pregiudizio antropocentrico che per lungo tempo si è opposto anche al riconoscimento della responsabilità penale degli enti e che è stato infine superato in virtù di un'esigenza di regolazione sociale[399].

Ebbene, non vi è dubbio che l'operare dei sistemi di intelligenza artificiale ponga ineludibili necessità di protezione da parte degli ordinamenti e che dunque, come avvenuto con riferimento alla *societas*, anche per la *machina* il legislatore sia chiamato ad adottare soluzioni per colmare eventuali vuoti di tutela di fronte a fenomeni pericolosi o dannosi[400]. Perché possa rispondere adeguatamente alle oggettive necessità di protezione della collettività, tale sforzo deve essere, da un

---

CONSULICH, Flash offenders, *op. cit.*, p. 1022 sottolinea invece come "vi sono forme di intelligenza artificiale che assumono la forma di puro *software*, inteso come insieme sinergico di dati e algoritmi (come nel caso dei mercati finanziari), ve ne sono […] altri che possiedono anche una componente *hardware*".

[397] Espressione attribuita a Lord Chancellor of Great Britain Edward Thurlow, ripresa – per tracciare un parallelo con la responsabilità dei *robot* da P. M. ASARO, *A body to Kick, op. cit.*, pp. 169-186.

[398] In tema di *societas delinquere non potest*, si rinvia – senza pretesa di esaustività – all'insegnamento di Bricola. In particolare, F. BRICOLA, *Il costo del principio «societas delinquere non potest» nell'attuale dimensione del fenomeno societario*, in Riv. it. dir. proc. pen., 1970, pp. 951-1031, poi in Scritti di diritto penale, vol. II, tomo II, Milano, Giuffrè, 1997, pp. 2975-3062; nonché ID, *Luci ed ombre nella prospettiva di una responsabilità penale degli enti (nei paesi della C.E.E.)*, in Giur. comm., 1979, I, pp. 647-663, poi in Scritti di diritto penale, vol. II, tomo II, Milano, Giuffrè, 1997, pp. 3063-3088.

[399] In questo senso, in particolare, R. BORSARI, *Intelligenza artificiale*, *op. cit.*, p. 267.

[400] Come nota F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*, "quel che è certo è che la regolamentazione è urgente. Ma se l'*an* della regolazione non è in discussione, non così il *quomodo*, ancor di più rispetto alla spendita della sanzione penale".

lato, scevro di preclusioni aprioristiche e dall'altro deve risultare coerente con i principi fondamentali dei sistemi giuridici moderni.

Il quesito di fondo dal quale occorre partire è se esista, allo stato, un vuoto di tutela che è necessario e utile colmare attraverso la previsione di una responsabilità – esclusiva o complementare – diretta della macchina.

Allo stato attuale, la risposta a tale interrogativo pare essere negativa. La dottrina ritiene infatti che lo stato evolutivo dei sistemi di intelligenza artificiale, per quanto sofisticato, "sia ancora fortemente dipendente da *input* umani"[401] e che dunque, per quanto possa essere una fonte di rischio sia tutt'ora un oggetto e non un soggetto[402].

Quand'anche si potessero immaginare prospettive in cui tali sistemi acquisiscano "capacità di apprendimento e di adattamento al contesto in cui operano pari, se non superiori, a quelle dell'uomo"[403] occorrerebbe dimostrare in modo rigoroso – rifuggendo prospettive catastrofiche, che seppur suggestive rischiano di fermarsi a un livello eccessivamente congetturale[404] – l'impossibilità delle tradizionali categorie del diritto penale antropocentrico di porre rimedio ai danni provocati dall'agire di tali sistemi.

Breve: rimane da dimostrare che "la rapida acquisizione di tecniche e conoscenze che, stratificandosi, rendono via via più difficile per la persona fisica prevedere il funzionamento e le determinazioni della macchina"[405] imponga di rinunciare alla responsabilità penale dell'uomo 'dietro la macchina' in favore di una responsabilità esclusiva del sistema di intelligenza artificiale[406].

Ciò non significa escludere *tout court* la possibilità di concepire misure che abbiano come destinataria immediata la macchina – e che ne limitino o prevengano le conseguenze dannose del suo agire –, ma piuttosto rilevare come esistano robusti argomenti che militano in senso contrario all'utilità, prima ancora

---

[401] Così F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*

[402] Cfr. F. CONSULICH, Flash offenders, *op. cit.*, p. 1048.

[403] Così I. SALVADORI, *Agenti artificiali, op. cit.*, p. 114.

[404] Il rischio che si intravede è che la condivisibile tendenza di guardare al futuro, preoccupandosi di prevenire le possibili implicazioni dannose o pericolose dell'agire di intelligenze artificiali devianti, finisca per porre questioni più teoriche e speculative che reali.

[405] F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*

[406] In questo contesto si collocano, se ben intendiamo, le considerazioni conclusive di F. CONSULICH, Flash offenders, *op. cit.*, p. 1055; nonché, più di recente, F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.* e, prima, R. ABBOTT R.–A. SARCH, *Punishing Artificial intelligence: Legal Fiction or Science Fiction*, in UC Davis Law Review, 2019, vol. 53, issue 1, pp. 323-384.

che alla necessità, del superamento del brocardo *machina delinquere et puniri non potest*[407].

Addentrandosi nel merito delle singole argomentazioni, posto che, la riconducibilità dell'azione della macchina ad un agire 'tipico' in senso penalistico non pare porre particolari problemi[408], altrettanto non può dirsi per le considerazioni svolte in punto di 'colpevolezza della macchina' da parte dei sostenitori della tesi della responsabilità diretta dei sistemi di intelligenza artificiale.

Il primo di questi argomenti è l'impossibilità di rinvenire un atteggiamento autenticamente colpevole nell'agire dei sistemi algoritmici[409].

La tesi della responsabilità penale diretta della 'macchina' sembrerebbe infatti figlia di un'indebita commistione fra apparenza e realtà. I sistemi di intelligenza artificiale 'agiscono' e conoscono la realtà esterna sulla base della programmazione dell'uomo, prendono decisioni che consentono di raggiungere un obbiettivo *dato*, ma "il vero 'motore dell'azione va pur sempre ricercato a monte, in colui che elabora l'algoritmo"[410]. Sicché, gli algoritmi non fanno altro

---

[407] Cfr. F. CONSULICH, Flash offenders, *op. cit.*, p. 1055, sull'utilità di interrogarsi in merito alla sussistenza di *actus reus* e *mens rea* dell'algoritmo.

Per un'approfondita disamina delle critiche mosse alla responsabilità diretta dell'algoritmo, si vedano, in particolare, A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, pp. 511-515 e M.E. .; M. E. FLORIO, *Il dibattito sulla responsabilità penale*, *op. cit.* pp. 10-13; nonché, tra gli altri, F. CONSULICH, Flash Offenders, *op. cit*., pp. 1024-1026; C. PIERGALLINI, *Intelligenza artificiale*, *op. cit*., pp. 1745–1774; M.B. MAGRO, Robot*,* cyborg *e intelligenze artificiali*, *op. cit.*, pp. 1232-1256.; R. BORSARI, *Intelligenza artificiale e responsabilità penale*, *op. cit.*, pp. 262-268 e F. BASILE, *Intelligenza artificiale e diritto penale, op. cit.*, pp. 30-32.

Nella dottrina internazionale più recente: F. C. LA VATTIATA, *AI Systems Involved in Harmful Events*, *op. cit.*, pp. 485-499; T. WEIGEND, *Convicting Autonomous Weapons?*, *op. cit.*, pp. 1137-1154.

[408] La tesi pare per questa parte condivisibile, giacché come rileva A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, p. 509 "in ambito di *common law* l'equivalente del concetto continentale di azione è solitamente inteso in termini molto più schiettamente materialistici di quanto non si suole fare nelle varie sistematiche post-finaliste, che ormai – negli ambienti culturali continentali – hanno in larga misura soppiantato gli echi dell'originaria tripartizione belinghiana, ispirata al più rigido materialismo quanto al fatto tipico". Nello stesso senso R. BORSARI, *Intelligenza artificiale e responsabilità penale: prime considerazioni*, in Media Laws, 2019, fasc. 3, p. 266. Solleva invece rilievi critici C. PIERGALLINI, *Intelligenza artificiale*, *op. cit.*, pp. 1768-1769.

[409] Sulla supposta derivabilità della colpevolezza dell'i.a. dai propri attori umani, come avviene per l'ente vedi *infra* in questo paragrafo.

[410] C. PIERGALLINI, *Intelligenza artificiale*, *op. cit.*, p. 1769 rileva che, invero, "il sistema di IA non agisce ma 'è agito'. Anche se è vero che rielabora i dati della realtà esterna (sì da consocerla) a scopo di autoapprendimento, […] il *decision making* non è frutto di una scelta ma è la *obbligata risultante* dei meccanismi oscurti che alimentano l'algoritmo, a sua volta forgiato

che compiere le scelte e raggiungere l'obiettivo per cui sono state programmate[411]. Ciò significa, come sottolineato dalla dottrina, che essi agiscono con "tipicità dolosa. Ma questa nulla ancora ci dice riguardo alla colpevolezza dolosa"[412].

La volontà degli algoritmi è quindi strettamente predeterminata dal programmatore, anche se ad agire sono sistemi 'forti'. Considerando, ad esempio, i sistemi di *trading*, il loro impiego è funzionale al guadagno e all'interesse del programmatore. Sicché la loro imprevedibilità non deve essere confusa con la capacità di porsi autonomamente degli obiettivi di comportamento. In assenza di una volontà autenticamente libera e autonoma, il fatto dell'algoritmo, ancorché riconducibile alla categoria dell'antigiuridicità, non può tuttavia essere considerato colpevole in senso strettamente penalistico[413].

---

dall'uomo. Il vero 'motore' motore dell'azione va pur sempre ricercato a monte, in colui che elabora l'algoritmo: quel che accade 'dopo' si espone ad una *imprevedibilità necessitata*, […] che non può in alcun modo essere incasellata come manifestazione di un agire intelligentemente gestito perché è *carente* del requisito costitutivo della *libertà di autordeterminazione*".

[411] Sul significato dell'autonomia e dell'adattabilità dei sistemi di intelligenza artificiale 'forte' (o 'di seconda generazione') M. FIERENS–S. ROSSELLO–E. WAUTERS, *Setting the Scene*, *op. cit.*, pp. 49-72. Come nota L. PICOTTI, *Ente,* in Piergallini C.–Mannozzi G.–Sotis C.–Perini C.–Scoletta M.–Consulich F. (a cura di), *Studi in onore di Carlo Enrico Paliero*, Giuffrè, 2022, nonché in Sist. Pen., p. 10, l'algoritmo è un 'ente' solo metaforicamente, che non possiede l'intelligenza (e la volontà) nel senso umano del termine; "il sistema non possiede insomma che un succedaneo della volontà propria dell'essere umano, che si esprime nell'ancestrale capacità di scelta — elettiva e nel contempo valutativa — fra il "bene" ed il "male", su cui si fonda la sua stessa responsabilità". Si vedano inoltre B. FRAGASSO, *Intelligenza artificiale e crisi del diritto penale*, *op. cit.*, pp. 28 ss e M. PAPA, Future crimes: *intelligenza artificiale e rinnovamento del diritto penale*, in Criminalia, 2019, pp. 502-503, "L'intelligenza artificiale codifica e gestisce la sua interazione con il mondo secondo algoritmi".

[412] L'espressione – evocativa dell'apparenza tendenzialmente dolosa dell'elemento soggettivo che sorregge l'agire dei soggetti artificiali – è di A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, p. 511, che prosegue chiarendo: "è ben vero che nell'imputazione di un fatto ad agenti umani di solito la seconda – la colpevolezza – è considerata presupposta ove sussista chiaramente la prima – la tipicità –, salvo si provi la sua eccezionale insussistenza nel caso concreto […]. Ma questo meccanismo presuntivo – è evidente – si regge sul presupposto tacito per cui l'uomo, in situazioni normali, non eccezionali, sia dotato della capacità di autodeterminarsi, scegliendo un comportamento antigiuridico, che con tale scelta diviene anche colpevole".

[413] Sull'assenza di colpevolezza, si vedano, *ex multis*, ABBOTT R.–SARCH A., *Punishing Artificial intelligence: Legal Fiction or Science Fiction*, in 53 UC Davis Law Review, 2019, fasc. 1, pp. 323-384, nonché S. GLESS –E. SILVERMAN, T. WEIGEND, *If robots cause harm*, *op. cit.,* p. 417. Come rileva L. PICOTTI, Ente, *op. cit.* p. 10 "in mancanza di una personalità e volontà propria, anche la minaccia ed irrogazione di sanzioni non avrebbe senso, dovendo piuttosto essere funzionale ad incidere sul comportamento futuro delle persone fisiche o degli "enti" collettivi che vi stanno dietro".

La mancanza di colpevolezza, presupposto indispensabile perché il rimprovero penale personale possa svolgere il proprio effetto – nel senso inteso dalla Costituzione –, determina l'impossibilità di infliggere alla macchina una sanzione penale che miri alla prevenzione, speciale e generale, oltre che alla retribuzione[414].

Se sulla funzione retributiva della pena inflitta alla 'macchina' può considerarsi un'opzione quantomeno discutibile (e, in effetti, discussa)[415]; la maggior parte della dottrina è invece concorde nell'escluderne la funzione special preventiva, rieducativa. Si afferma infatti che un soggetto incapace di compiere scelte libere e consapevoli non è in grado di *apprendere* dal rimprovero mosso in conseguenza di un'azione sbagliata, di "comprendere l'errore"[416], e quindi sottoporsi al processo risocializzante che l'art. 27 Cost. presuppone[417]. La correzione del comportamento – *i.e.* la 'rieducazione – dell'algoritmo passa semmai da una sua riprogrammazione, da una modifica delle sue istruzioni di

---

[414] Sul punto, in particolare, F. BASILE, *Intelligenza artificiale e diritto penale*, *op. cit.*, p. 31 sottolinea che "possiamo parlare di responsabilità penale (solo) se la sanzione applicata è una *pena*" e in merito sintetizza le funzioni che alla *pena* si riconoscono "esclusivamente o cumulativamente, una funzione retributiva (viene inflitta la pena per retribuire – far pagare – il male recato con il reato), una funzione general-preventiva (la minaccia della pena funge, per i suoi possibili destinatari, da freno alla spinta criminale) o una funzione special-preventiva (l'inflizione, e l'esecuzione, della pena pone il condannato nella condizione di non commettere più, in futuro, reato)". Cfr. anche le Raccomandazioni contenute in L. PICOTTI, *Resolution on traditional criminal law categories and AI*, in L. Picotti–B. Panattoni (a cura di), Traditional Criminal Law Categories and AI: Crisis or Palingenesis?, in Revue Internationale de Droit Penal, Vol. 94, Issue 1/2023, p. 3, par. 1, pt. 5 "le sanzioni punitive applicate a tali sistemi e agenti tecnologici non risponderebbero agli scopi e alle funzioni della sanzione penale, perché l'effetto della minaccia della pena e della sua applicazione sarebbe svuotato dall'assenza di autocoscienza della propria esistenza nel passato, nel presente e nel futuro e, soprattutto, dall'assenza di autodeterminazione volontaria, cosicché, anche escludendo la funzione retributiva, nemmeno quelle di prevenzione speciale e generale sarebbero attuabili" (traduzione nostra).

[415] In merito al concetto di retribuzione e all'intrinseco legame con la capacità di autodeterminazione, M. E. FLORIO, *Il dibattito sulla responsabilità penale, op. cit.* p. 11, nt. 20 evidenzia che lo stesso Hallevy "osserva che «una macchina non soffre, e finché la retribuzione si baserà sul soffrire, la retribuzione non sarà molto rilevante per punire i robot»"; C. PIERGALLINI, *Intelligenza artificiale*, *op. cit.*, p. 1769 sostiene l'inconciliabilità di una 'pena robotica' con la funzione retributiva, posta che "come noto, postula la possibilità di muovere un rimprovero colpevole"; *contra* F. BASILE, *Intelligenza artificiale e diritto penale*, *op. cit.*, p. 31.

[416] Così C. PIERGALLINI, *Intelligenza artificiale*, *op. cit.*, p. 1770.

[417] Come nota C. PIERGALLINI, *Intelligenza artificiale*, *op. cit.*, p. 1770 che sottolinea come nella rilettura moderna la prevenzione speciale declinata in termini di rieducazione i fonda sulla "possibilità che la sanzione irrogata aiuti a comprendere l'errore commesso per evitare di reiterare nello stesso. Il presupposto è dunque una capacità di autoriflessione che la macchina, ontologicamente non possiede". In questo senso anche P.M. ASARO P.M., *Determinism, machine agency, and responsibility*, in Politica & Società, 2014, fasc. 2, p. 261.

funzionamento che però implica al più un ripensamento del programmatore. Dalla mera inflizione della sanzione l'algoritmo non sarebbe, cioè, in grado di imparare o dedurre alcunché sulla correttezza del suo comportamento e di conseguenza orientare la sua condotta futura, perché non ha la capacità di autoriflessione che sta alla base del concetto di rieducazione. Solo tramite la riprogrammazione, l'immissione e l'analisi di nuovi dati e quindi, in definitiva, tramite una mediazione dell'essere umano è in grado di comprendere se un comportamento sia o meno corretto o vantaggioso e dunque ottimizzare progressivamente il proprio agire[418]. Infine, la pena (o la minaccia della pena) non potrebbe avere alcun effetto general preventivo sui consociati, sempre che di 'consociati robotici' si possa parlare[419], poiché non vi sono allo stato evidenze della capacità dei sistemi di intelligenza artificiale di cogliere l'affinità fra le azioni che intendono intraprendere e analoghi comportamenti già posti in essere (e sanzionati) da altri soggetti[420]. L'inflizione di una sanzione ad altri non ha, dunque, alcun effetto deterrente sulla 'macchina'.
Non paiono poi decisive le considerazioni in ordine al tentato parallelismo con la responsabilità da reato degli enti, anch'essa a lungo negata sulla base dell'assenza di un 'corpo da colpire'[421].

---

[418] Semplificando al massimo, solo tramite la 'mediazione' del programmatore l'algoritmo di *trading* è in grado di apprendere il fatto che l'autorità amministrativa o giudiziaria hanno sanzionato un determinato comportamento. In assenza della riprogrammazione, la 'macchina' tiene conto e conosce solo l'eventuale guadagno che quella strategia ha portato; perciò potrebbe ritenerla economicamente vantaggiosa e replicarla.

[419] Sul possibile effetto general preventivo delle pene inflitte alla 'macchina', F. LAGIOIA–G. SARTOR, *AI Systems Under Criminal Law*, *op. cit.*, p. 460.

[420] Cfr. P.M. ASARO P.M., *A body to* kick, *op. cit.*, p. 181; nonché F. CONSULICH, Flash offenders, *op. cit.*, p. 1025 e A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, p. 513, nt. 47, che, nel rilevare come l'effetto di intimidazione sarebbe anzitutto minato dall'incapacità dei soggetti artificiali di provare sentimenti di timore o paura, nota come lo stesso Hallevy "giunge a riconoscere la sicura operatività dei soli fini specialpreventivi della pena robotica – *rehabilitation e incapacitation* – senza peraltro interrogarsi di come possa ancora parlarsi di 'pena' in mancanza di un momento generalpreventivo e soprattutto retributivo". Sul punto anche C. PIERGALLINI, *Intelligenza artificiale*, *op. cit.*, p. 1769, che esclude la possibile idoneità a provocare paura o timore.

[421] L'argomento dell'assenza di un 'corpo" dell'i.a. da colpire non è smentito dall'esistenza di una struttura fisica l'*hardware* – che incorpora l'agente artificiale, poiché quest'ultimo non si identifica con la struttura che lo 'contiene'. L'*hardware* che contiene il codice (ossia l'insieme di dati e algoritmi) altro non è che la struttura tramite cui il sistema di intelligenza artificiale opera nella realtà, ma che non definisce in alcun modo le sue modalità operative che dallo specifico *hardware* prescindono totalmente. Tanto che esso è del tutto 'intercambiabile': la scelta di un *hardware* anziché di un altro non influisce in alcun modo sulle funzionalità dell'algoritmo stesso. Sicché, mentre colpendo il patrimonio dell'ente se ne può limitare o inibire il funzionamento, lo

Come sottolineato in dottrina, benché tra sistemi di intelligenza artificiale e società ci siano senz'altro alcune analogie, tra queste due entità esistono soprattutto "molteplici differenze, che rendono difficile avallare l'idea di potersi limitare a trasporre *sic et simpliciter* gli argomenti spesi a sostegno della responsabilità penale delle seconde per giustificare anche quella dei primi"[422].
L'ente *è* dotato di una sua materialità[423], è un'aggregazione di persone capace di agire nel contesto sociale, è un centro di interessi propri persegue una propria 'politica'[424], può essere fonte istigatrice di attività delittuosa[425]. Tutte caratteristiche, che giustificano il rimprovero penale dell'ente, difettano invece nel sistema di intelligenza artificiale.
Occorre infatti considerare in primo luogo che proprio il fatto che quest'ultimo, diversamente dalla persona giuridica, non è *costituito* da (ma semmai *programmato* da) esseri umani segna l'impossibilità di far derivare la sua colpevolezza dai propri attori umani, come avviene invece per le imprese collettive[426]. Ciò impedisce di utilizzare per l'a.i. lo stesso meccanismo di

---

stesso non può avvenire colpendo l'hardware, perché esso non è il 'corpo' del sistema di intelligenza artificiale. I. SALVADORI, *Agenti artificiali, op. cit.*, p. 91 fornisce alcuni esempi di sistemi che "hanno una struttura fisica (*hardware*), come nel caso delle *self-driving cars*, degli aeromobili o sommergibili a pilotaggio remoto (*unmanned vehicles*) o dei bracci meccanici impiegati nella bioingegneria. In alcuni casi gli a.a. sono dotati di apparati che emulano il corpo umano (*bodyware*) e sono in grado di muoversi. Si pensi ai robot che vengono impiegati in ambito medico-chirurgico, militare, industriale o nel settore dell'*health care*".

[422] Così M. E. FLORIO, *Il dibattito sulla responsabilità penale, op. cit.* p. 11; C. PIERGALLINI, *Intelligenza artificiale*, *op. cit*., p. 1767 definisce quello fra *machina* e *societas* un "parallelismo malfermo".

[423] Cfr. A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, p. 514, "la responsabilità da reato degli enti – quantomeno nella sua veste continentale – muove proprio dall'idea di attribuire almeno un minimo grado di 'realtà' alla persona giuridica".

[424] L'algoritmo, a differenza dell'ente, non persegue una propria politica paragonabile alla politica di impresa e il programmatore non è qualificabile come mero esecutore della politica di impresa come lo è un soggetto apicale di un'impresa.

[425] Come – secondo l'insegnamento di Bricola – invece avviene per le società, che benché incapaci di realizzare direttamente l'attività fisica che concretizza la volontà delittuosa. Di questa attività esse sono, però la fonte istigatrice: ed è a questo titolo che la società devono rispondere senza pericolo per il principio del carattere personale della responsabilità penale. Cfr. F. BRICOLA, *Il problema della responsabilità penale della società commerciale nel diritto italiano*, in La responsabilità delle persone giuridiche, Atti del Convegno, Messina, 1979, 235-263, poi in Scritti di diritto penale, vol. II, tomo II, Milano, Giuffrè, 1997, pp. 3089-3120.

[426] C. PIERGALLINI, *Intelligenza artificiale*, *op. cit*., p. 1767, "la *societas*, sia che la si interpreti in guisa di uno 'schermo', sia alla stregua di un 'organo', esiste nella realtà giuridica e sociale, ma è animata, naturalisticamente e spiritualmente, dagli uomini che le danno vita". Sul parallelo *corporate liability*-AI systems liabiity, e in particolare in tema di "respondeat superior

trasferimento – volendo sintetizzare al massimo – dell'elemento soggettivo dell'agente umano può essere imputato alla società, qualora questi abbia agito nell'interesse o vantaggio della stessa. Ciò comporta che la responsabilità della persona giuridica si fonda su un fatto proprio della *societas*, a questa rimproverabile perché commesso nel suo interesse o vantaggio e attribuibile a una "colpa di organizzazione, cioè un qualcosa proprio della compagine sociale in via diretta, un qualcosa di suo"[427]. Lo stesso non può valere per i sistemi di intelligenza artificiale, che – oltre a non essere *costituiti* da attori umani – non agiscono per interessi propri, poiché gli algoritmi "non hanno preferenze autonome, ma svolgono una funzione di interesse per il proprio 'titolare'"[428], che ne ha stabilito la programmazione.

In secondo luogo, si afferma che la 'macchina' non sarebbe, a differenza della persona giuridica, titolare di diritti da comprimere o limitare con la sanzione penale e per questa ragione non potrebbe soggiacere a pena. A tale argomento si è posta una parte della dottrina, che sostiene la possibilità di riconoscere nell'agente artificiale un soggetto di diritto[429], come tale assoggettabili anche a doveri di comportamento presidiati dalla sanzione penale.

L'argomento utilizzato tuttavia non pare risolutivo perché – quasi tautologicamente – desume la possibilità di sanzionare un soggetto dalla mera introduzione di norme che lo sanzionino; quando è proprio l'ammissibilità di queste norme l'oggetto del dibattito dottrinale. Tale argomento, cioè, semplifica eccessivamente il problema: se l'unico limite alla sanzione penale del sistema di intelligenza artificiale fosse l'esistenza di una norma che preveda tale sanzione, il dibattito intorno alla concepibilità di una responsabilità diretta della macchina

---

doctrine" si veda R. ABBOTT–A. SARCH, *Punishing Artificial intelligence*, *op. cit.* pp. 350-351: "unlike a corporation, which is literally composed of the humans acting on its behalf, an AI is not guaranteed to come with a ready supply of identifiable human actors whose mental states can be imputed This is not to say there will not also be many garden-variety cases where an AI does have a clear group of human developers. Most AI applications are likely to fall within this category and so *respondeat superior* would at least be a partial route to making AI eligible for punishment. Of course, in many of these cases when there are identifiable people whose mental states could be imputed to the AI — such as developers or owners who intended the AI to cause harm — criminal law will already have tools at its disposal to impose liability on these culpable human actors. In these cases, there is less likely to be a need to impose direct AI criminal liability".

[427] Così A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, p. 514. Tanto che si ritiene che la responsabilità da reato dell'ente soggiaccia al vincolo dell'art. 27, primo comma, Cost. in questo senso, per tutti, G. MARINUCCI – E. DOLCINI – G. L. GATTA, *Manuale di diritto penale*, *op. cit.*, pp. 993.

[428] Così F. CONSULICH, Flash offenders, *op. cit.*, p. 1042.

[429] *Contra* F. LAGIOIA–G. SARTOR, *AI Systems Under Criminal Law*, *op. cit.*, pp. 433-465.

sarebbe facilmente risolto. Viceversa, il reale ostacolo al riconoscimento di tale forma di responsabilità penale risiede, secondo la dottrina, nella difficoltà di adattamento delle categorie tradizionali ai sistemi di intelligenza artificiale; nonché all'impossibilità di individuare un centro di interessi autonomamente aggredibile, come avviene per le società.

Ma anche volendo superare tali ostacoli dogmatici, non si può non rilevare come vi sia un ulteriore convincente elemento che esclude il paragone fra responsabilità dell'algoritmo e responsabilità dell'ente: l'assenza, in capo al sistema di intelligenza artificiale, di un patrimonio aggredibile con la sanzione penale[430].

Come rilevato dalla dottrina, "un simile destinatario non ha certo risorse economiche proprie a cui attingere"[431], perciò, anche qualora dunque si immaginasse di colpire la 'macchina' con la principale sanzione pena applicabile – quella pecuniaria[432] – il pregiudizio non potrebbe che riguardare, invero, l'essere umano 'dietro alla macchina'. E anche optando per una sanzione di diverso contenuto, ad esempio la disattivazione (c.d. pena di morte dell'i.a.), pur rivolta formalmente al sistema di intelligenza artificiale, comporterebbe un pregiudizio unicamente per l'utilizzatore o il programmatore[433]. In definitiva, si colpirebbe l'uomo per un fatto che attribuito alla 'macchina'. La sanzione – pur formalmente rivolta al sistema di intelligenza artificiale – finirebbe per costituire una forma di responsabilità oggettiva per il proprietario del sistema per un fatto non 'suo'.

In definitiva, nonostante i tentativi di antropomorfizzazione dei sistemi di intelligenza artificiale – inclusi quelli concepiti, in un certo senso, a immagine a somiglianza dell'uomo, anche nella capacità di produrre processi intellettivi – ciò non è sufficiente ad applicare alla 'macchina' i canoni di un diritto penale che rimane fondato sulle caratteristiche proprie dell'essere umano, antropocentrico[434].

---

[430] Il concetto di patrimonio a cui si fa riferimento non può essere in alcun modo associato a quello di fondo patrimoniale, che una parte della dottrina ha proposto per far rispondere la macchina *a fini civilistici* delle proprie obbligazioni. Per una più ampia disamina della proposta, in ottica critica, si rinvia a C. PIERGALLINI, *Intelligenza artificiale*, *op. cit*., p. 1764.

[431] Così F. CONSULICH, Flash offenders, *op. cit.*, p. 1024.

[432] Oltre alla disattivazione del sistema o l'inibizione del suo uso.

[433] Sull'effetto *spillover* delle pene inflitte al sistema di i.a.: F. CONSULICH, Flash offenders, *op. cit.*, pp. 1024-1025.

[434] Approccio antropocentrico che, d'altra parte, permea anche i più recenti atti dell'Unione europea in materia di intelligenza artificiale, fra c l'AI Act, nonché nel Libro bianco

D’altra parte, come si è detto, uno sforzo nella direzione di superare i canoni tradizionali non pare avere *allo stato attuale*[435] particolare utilità, poste le caratteristiche delle intelligenze artificiali con cui il diritto penale si confronta[436] e l’impossibilità di individuare nel loro agire un atteggiamento colpevole in senso penalistico – portano ritenere che gli attuali strumenti del diritto penale siano tuttora efficaci nel contrasto a potenziali offese causate da AI devianti, come si illustrerà di seguito.

Ciò non significa escludere del tutto sanzioni di contenuto diverso, anche considerando – come rilevato dalla dottrina – che anche le *res* possono subire “afflizioni alcune da parte delle pubbliche autorità: soltanto, queste non hanno natura penale, ma di regolazione amministrativa di interessi”[437].

5.2 La responsabilità penale dell’uomo

Le considerazioni sin qui svolte portano a ritenere che, anche qualora si immaginassero delle forme di responsabilità diretta dei sistemi intelligenti[438], esse queste non potrebbero in alcun modo surrogare la responsabilità *penale* dell’essere umano.

Una responsabilità penale diretta ed esclusiva della macchina rischierebbe, infatti, per costituire una sorta di alibi, dietro al quale finirebbero per celarsi strategie tese a deresponsabilizzare l’essere umano.

Fatti che, se commessi da un essere umano costituirebbero reati non sarebbero invece sanzionali penalmente per il sol fatto che nella commissione di questi ultimi è coinvolto un sistema di intelligenza artificiale. In altri termini, l’esito della responsabilità diretta – ed esclusiva – della macchina sarebbe la creazione di un’area di impunità per l’uomo. Si tratterebbe di un risultato evidentemente

---

sull’intelligenza artificiale del 2020, che non prevedono né una soggettività giuridica, né una responsabilità penale diretta della macchina, ma che adottano – come si dirà – la logica della prevenzione e della gestione del rischio,

[435] Il corsivo è d’obbligo, come nota C. PIERGALLINI, *Intelligenza artificiale*, *op. cit*., p. 1770.

[436] Sul punto si vedano, in particolare, A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, p. 518-519; nonché, da ultimo, F. CONSULICH, *Il diritto penale al tempo dell’intelligenza artificiale*, *op. cit.*.

[437] Così A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, p. 517, che aggiunge “ad esempio, il cane rabbioso e pericoloso può essere abbattuto, così come le mandrie infette possono essere eliminate al fine di evitare epidemie”.

[438] E ammesso che tale forma di responsabilità possa avere natura penale.

inaccettabile, oltre che da un punto di vista logico-giuridico, anche dal punto di vista politico-criminale[439].

Per questo motivo, nel prosieguo ci si soffermerà sulla prospettiva della responsabilità dell'uomo.

Si tratterà, in particolare, di indagare a che titolo e entro quali limiti l'essere umano può rispondere delle conseguenze dannose determinate dall'operare dell'algoritmo, con specifico riferimento agli algoritmi di *trading*.

Si è dimostrato che gli algoritmi – specificamente quelli di *trading* – possono essere coinvolti nella realizzazione di offese a beni giuridici.

Il *trading* algoritmico è dunque, in buona sostanza, un'attività che presenta dei profili di pericolosità, ma che ciononostante non è di per sé vietata dall'ordinamento, che anzi regola ampiamente le modalità secondo le quali la negoziazione algoritmica deve svolgersi[440].

5.2.1. Algoritmi, intelligenza artificiale e la prospettiva del rischio

Questa considerazione colloca inevitabilmente l'analisi in un'area che evoca il tema del rischio[441].

Che la logica con cui affrontare le applicazioni di intelligenza artificiale e il loro operare nella realtà sia quella del contenimento del rischio, è confermato dal più

---

[439] Sul punto, par. 3, punto 9 L. PICOTTI, *Resolution on traditional criminal*, op. cit., p. 55; nonché ID, *Categorie tradizionali del diritto penale*, *op. cit.*, p. 8.

[440] *Nihil novi sub sole*: "l'ordinamento consente l'esercizio di molte attività che presentano non lievi pericoli: industrie importanti, come la gestione di ferrovie e miniere, la fabbricazione di materie esplosive, le costruzioni edilizie" cfr. F. ANTOLISEI, Manuale di diritto penale (Parte Generale), XVI ed., Giuffrè, Milano, p. 343.

[441] La collocazione della regolamentazione dell'agire dei sistemi di intelligenza artificiale in generale nell'ambito della categoria del rischio è sostenuta da ampia parte della dottrina, seppur con diverse visioni, fra cui: F. CONSULICH, Flash offenders, *op. cit.*, pp. 1043-1055; nonché B. FRAGASSO, *La responsabilità penale del produttore*, *op. cit.*, pp. 36-37 e ID., *Intelligenza artificiale e crisi*, *op. cit.*, pp. 295-298; M. E. FLORIO, *Il dibattito sulla responsabilità penale, op. cit.* p. 17; R. COMPOSTELLA, *Auto a guida autonoma e diritto penale. Profili di responsabilità individuale e collettiva*, Napoli, Editoriale Scientifica, 2024, pp. 157-161.; N. AMORE, *L'effetto della robotica e dell'IA nell'imputazione giuridica degli eventi infausti*, in N. Amore–E. Rossero, Robotica e intelligenza artificiale nell'attività medica. Organizzazione, autonomia, responsabilità, Bologna, 2023, pp. 148-153; A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, pp. 516-520;, I. SALVADORI, *Agenti artificiali, opacità tecnologica*, *op. cit.*, *op. cit.*, pp. 115-118; C. PIERGALLINI, *Intelligenza artificiale*, *op. cit*., p. 1750; FIORELLA, *Responsabilità penale dei* Tutor, *op. cit.*, p. 656; S. GLESS –E. SILVERMAN, T. WEIGEND, *If robots cause harm*, *op. cit.,* p. 430-431.
La logica della gestione e prevenzione del rischio caratterizza, oltre all'AI Act anche la Convenzione quadro sull'intelligenza artificiale adottata dal Consiglio d'Europa il 5 settembre 2024 (il cui testo è disponibile al link https://rm.coe.int/1680afae3c).

rilevante intervento legislativo in tema di intelligenza artificiale: il c.d. AI Act (o Regolamento sull'intelligenza artificiale)[442]

Il Regolamento in questione è infatti espressamente teso a prevenire i possibili rischi derivanti dal ricorso a sistemi di intelligenza artificiale e stabilisce obblighi – di sviluppo, implementazione e utilizzo – per i fornitori e gli utenti di tali sistemi a seconda del livello di rischio che essi comportano[443].

La considerazione che fa da sfondo all'intero atto è, infatti, quella che l'uso di sistemi intelligenti possa comportare dei rischi per i diritti fondamentali che devono essere prevenuti e gestiti e che, qualora non sia possibile mantenere (o riportare) l'attività di tali sistemi entro livelli tollerabili di rischio, questa debba essere vietata *tout court*[444].

---

[442] Regolamento (Ue) 2024/1689 del Parlamento Europeo e del Consiglio. La logica di prevenzione e gestione del rischio emerge diffusamente nel testo, a partire dai Considerando 26 e 27 che espressamente citano l'approccio basato sul rischio come base per "un insieme proporzionato ed efficace di regole vincolanti". L'art. 3, par. 1, n. 2) del Regolamento fornisce poi una definizione di 'rischio': "la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso". Sulla centralità del concetto di rischio all'interno dell'AI Act e il significato di tale scelta, *ex multis*, L. FLORIDI, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in Philosophy and Technology, 2021, n. 34, 2021, pp. 215-222; F.C. LA VATTIATA, *Brevi note "a caldo" sulla recente Proposta di Regolamento UE in tema di intelligenza artificiale*, in Dir. Pen. Uomo, 2021, fasc. 6, pp. 140-158.

Si tratta d'altra parte di un atteggiarsi del principio di precauzione che non è nuovo al legislatore europeo che, come notano G. FORTI, *"Accesso" alle informazioni sul rischio e responsabilità: una lettura del principio di precauzione*, in Criminalia, 2006, p. 192, ispira ad esempio la materia ambientale, oltre che i campi della sanità pubblica, della sicurezza alimentare e della sicurezza dei prodotti. Sulle applicazioni del principio in questione da parte della CGUE, si veda C. RUGA RIVA, *Principio di precauzione e diritto penale. Genesi e contenuto della colpa in contesti di incertezza scientifica*, in Dolcini E.–Paliero C.E. (a cura di), Studi in onore di Giorgio Marinucci, vol. II, Milano, Giuffrè, 2006, pp. 1746-1747.

[443] Gli artt. 1-2 del Regolamento classificano infatti i sistemi di intelligenza artificiale in base al livello di rischio e impone requisiti di sviluppo, implementazione e utilizzo in base alla classificazione del rischio. Sul concetto di affidabilità dei sistemi di intelligenza artificiale come sinonimo di accettabilità dei suoi rischi J. LAUX–S. WACHTER–B. MITTELSTADT, *Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk*, in Regulation & Governance, vol. 18, vssue 1, 2024, pp. 3-32.

[444] Come anticipato, l'AI Act definisce una 'piramide' dei rischi che possono derivare dall'utilizzo di sistemi di intelligenza artificiale, che ha alla base i sistemi 'a rischio minimo', salendo rischio 'limitato' e rischio 'alto' fino ad arrivare al vertice in cui si colloca il rischio 'inaccettabile'.

Sono sistemi a rischio inaccettabile, e perciò vietati, quelli che svolgono attività – elencate all''art. 5 (lett. a-h) – di manipolazione cognitivo-comportamentale di persone o di specifici gruppi vulnerabili (come i giocattoli che utilizzano l'assistenza vocale per incoraggiare comportamenti pericolosi dei minori), attività di classificazione sociale in base al comportamento, allo *status* socio-economico o alle caratteristiche personali dei singoli, attività di identificazione biometrica e

Si tratta di un'impostazione che, guardando al diritto penale, indubbiamente riecheggia la logica del rischio consentito[445], tipica delle attività della società del progresso[446], "espressamente autorizzate e disciplinate dal diritto nonostante sia

---

categorizzazione delle persone, o ancora sistemi che analizzano l'inferenza delle emozioni nell'ambito dei rapporti lavorativi o delle istituzioni scolastiche e alcune applicazioni di polizia predittiva.

[445] Sul punto, limitandosi alla sola dottrina italiana, *ex multis*, F. BRICOLA, *Aspetti problematici del cd. rischio consentito nei reati colposi*, in Bollettino dell'Università di Pavia, a.a. 1960-1961, p. 89 ss., poi in Scritti di diritto penale, vol. I, tomo I, Milano, Giuffrè, 1997, pp. 67-108; M. GALLO, *Colpa penale (diritto vigente),* in Enc. Dir., 1960, vol. VI, Milano, Giuffrè, pp. 624-643; G. MARINUCCI, *La colpa per inosservanza di leggi*, Milano, Giuffrè, 1965 rist. in La colpa. Studi, Milano, Giuffrè, 2013, pp.164-170; C. FIORE, *L'azione socialmente adeguata nel diritto penale*, Napoli, Morano, 1966; PADOVANI, *Colpa per inosservanza di legge ed "impossibilità" di adottare le cautele prescritte*, in *Riv. It. Dir. Proc. Pen.*, 1977, fasc. 2, pp. 767-772; V. MILITELLO, *Rischio e responsabilità penale*, Milano, Giuffrè, 1988; G. FORTI, *Colpa ed evento nel diritto penale*, Milano, Giuffrè, 1990; F. GIUNTA, *Illiceità e colpevolezza nella responsabilità colposa*, Cedam, Padova, 1993; M. DONINI, *Illecito e colpevolezza nell'imputazione del reato*, Milano, Giuffrè, 1991; ID, *Imputazione oggettiva dell'evento. "Nesso di rischio" e responsabilità per fatto proprio*, Torino, Giappichelli, 2006; ID, *Imputazione oggettiva dell'evento (diritto penale)*, in Enc. Dir., Annali III, Milano, Giuffrè, 2010, pp. 646-653; M. ROMANO, *Art.* 43, in Commentario sistematico del codice penale, vol. I, III ed., Milano, Giuffrè, 2004, p. 429; L. CORNACCHIA, *Concorso di colpe e principio di responsabilità penale per fatto proprio*, Torino, Giappichelli, 2004; D. CASTRONUOVO, *Responsabilità da prodotto e struttura del fatto colposo*, in Riv. It. Dir. Proc. Pen., 2005, fasc. 1, pp. 301-340; ID, *Principio di precauzione e beni legati alla sicurezza*, in Dir. Pen. Cont., 2011. ID, *Principio di precauzione e diritto penale. Paradigmi dell'incertezza nella struttura del reato*, Roma, Aracne, 2012; C. PERINI, *Il concetto di rischio nel diritto penale moderno*, Milano, Giuffrè, 2010; C. PIERGALLINI, *Danno da prodotto e responsabilità penale. Profili dommatici e politico-criminali*, Milano, Giuffrè, 2004; ID, Colpa (dir. pen.), in Enc. Dir., Annali X, 2017, Milano, Giuffrè, p. 222-265.; ID, *Il fatto tipico colposo*, in C.E. Paliero (a cura di), Il sistema penale, Torino, Giappichelli, 2024, pp. 300-301; S. ZIRULIA, *Esposizione a sostanze tossiche e responsabilità penale*, Milano, Giuffrè, 2018, pp. 335-467.
Nella manualistica: G. FIANDACA–E. MUSCO, *Diritto penale*, *op. cit.,* pp. 585-587; F. MANTOVANI, *Diritto penale. Parte generale.*, X ed., Padova, Cedam, 2017, pp. 343-347; D. PULITANÒ, *Diritto penale*, VII ed., Torino, Giappichelli, 2017, pp. 307-309.

[446] Come nota V. MILITELLO, *Rischio e responsabilità penale*, *op. cit.*, pp. 55 ss, il concetto di rischio consentito, o *erlaubutes Risiko* come elaborato dalla dottrina tedesca, trova impulso decisivo in due fattori concorrenti: la rapida emersione di una nuova fenomenologia criminologica (dettata dalle grandi trasformazioni economiche e tecniche) e l'inadeguatezza della concezione della colpa allora prevalente. Il progresso tecnico e le condizioni lavorative connesse all'industrializzazione (lo sfruttamento di miniere, l'automatizzazione delle fabbriche, i mezzi meccanici di trasporto pubblico e privato) determinarono infatti l'emergere di attività produttive potenzialmente pericolose ma socialmente utili, determinando l'aumento di statistiche di reati colposi e al contempo l'indisponibilità a "bollare come antigiuridiche quelle attività divenute in breve tempo componenti indispensabili della vita associata". Tradizionalmente, il concetto si accosta alla circolazione stradale e ferroviaria, alla produzione delle industrie chimiche e siderurgiche, ma anche all'attività sportiva. Per una ulteriore ricostruzione storica del rischio consentito come criterio di esclusione della responsabilità penale di condotte al contempo

facilmente prevedibile che, in ogni caso, la loro realizzazione comporti un certo margine di rischio"[447], sia cioè in sé e per sé pericolosa.

Di fronte ad attività che possono essere fonte di un rischio per beni giuridici rilevanti, si pongono due alternative.

Una prima soluzione sarebbe adottare un approccio precauzionale 'forte'[448], imponendo un divieto *tout court* all'esercizio dell'attività stessa. Nel caso degli algoritmici di *trading* ciò si tradurrebbe in un obbligo di totale astensione dalla creazione e dall'uso di sistemi che creino rischi considerati intollerabili.

Si tratta di un'alternativa evidentemente non praticabile per le inaccettabili conseguenze in termini di progresso tecnologico, che porta con sé – oltre a rischi inediti – anche innumerevoli benefici sociali[449].

La seconda soluzione è dunque l'unica vera alternativa praticabile, ossia quella di autorizzare l'attività, pur nella consapevolezza del suo potenziale lesivo.

Anche in questo caso, tuttavia, non verrebbe scongiurata la possibilità che tali attività – autorizzate dall'ordinamento – possano determinare eventi lesivi pienamente prevedibili, per cui la regola di condotta che consentirebbe di scongiurare il verificarsi dell'evento lesivo dovrebbe essere quella l'astensione[450].

---

socialmente utili e riconoscibilmente lesive di beni giuridici, si veda S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.*, pp. 342-354. Sulla concettualizzazione di 'società del rischio', di distribuzione del rischio e sul legame, nella società moderna, fra produzione sociale di ricchezza e produzione sociale dei rischi, si veda l'opera di U. BECK, *Risikogesellschaft. Auf Dem Weg in Eine Andere Moderne*, Suhrkamp, 1986 (ed italiana, La società del rischio. Verso una seconda modernità, Roma, Carocci, 2000, a cura di Walter Privitera), pp. 25-65.

[447] Così M. GALLO, *Colpa penale (diritto vigente)*, *op. cit.*, p. 640 nonché ID, *Diritto penale italiano. Appunti di parte generale*, Vol. I, III ed., Torino, Giappichelli, 2021, p. 491.

[448] Si tratterebbe di una soluzione evidentemente inaccettabile, non solo in riferimento alla negoziazione algoritmica, ma più in generale per tutte le attività produttive della cui attività nessuno dubita ma che non sono 'a rischio zero'.

[449] V. MILITELLO, *Rischio e responsabilità penale*, *op. cit.*, p. 14 secondo cui l'ordinamento non può vietare in generale ogni attività che sia fonte di offese per gli oggetti meritevoli di tutela. D'altra parte, se così fosse, si incorrerebbe nel rischio che la maggior parte delle attività della società moderna dovrebbero essere inibite, perché foriere di pericolo.

Secondo C. PIERGALLINI, *Danno da prodotto e responsabilità penale*, *op. cit.*, pp. 545-546, anche di fronte a un farmaco la soglia oltrepassata la quale si imporrà il ritiro del medesimo è definita dalla "valutazione costi/benefici: se il pregiudizio arrecato alla vita e all'integrità fisica è inferiore alla tutela che il farmaco assicura allo stesso bene, non si può profilare un obbligo di rimuovere la condizione di rischio, a patto, ovviamente, che il farmaco non risulti surrogabile da un altro provvisto di minori livelli di dannosità". Sul punto, Cfr. anche S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.*, p. 351.

[450] M. GALLO, *Colpa penale (diritto vigente)*, *op. cit.*, p. 640 nonché ID, *Diritto penale italiano, op. cit.*, p. 491 che prendendo ad esempio la circolazione stradale afferma che, essendo possibile che anche chi guida un'automobile a velocità moderata abbia "la possibilità di prevedere

Ciò comporterebbe però un'inaccettabile contraddizione: da un lato autorizzare condotte di cui si conosce la potenziale pericolosità e dall'altro lato rimproverare le conseguenze dannose di tali condotte[451].

Tale contraddizione viene dunque sciolta solo concependo un'area di rischio consentito, capace di bilanciare istanze di progresso e tutela di beni giuridici rilevanti.

Nei limiti di tale area, determinate "aggressioni ai beni giuridici [sono] oggettivamente permesse"[452], in virtù dei benefici che l'esercizio dell'attività apporta alla collettività.

Sicché, l'illecito che eventualmente si verifichi può essere rimproverato all'agente "solo se la sua condotta abbia creato o innalzato ad un livello patologico, e dunque illecito, la quantità di rischio insista nella situazione in cui si colloca l'azione"[453]. Viceversa, chi abbia con la sua attività pericolosa determinato

---

l'investimento di un passante che gli si cacci sotto le ruote" e che quindi la regola di condotta tendente ad evitare l'evento sarebbe in questo caso quella di non guidare l'automobile.

[451] M. GALLO, *Colpa penale (diritto vigente)*, *op. cit.*, p. 640; S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.*, p. 352.

Sulla qualificazione del rischio consentito in dottrina si contrappongono diverse tesi: elemento negativo della tipicità, causa di esclusione dell'antigiuridicità del fatto, causa di esclusione della colpevolezza. Cfr. C. PERINI, *Il concetto di rischio*, *op. cit.*, p. 10 ss e M. DONINI, *Imputazione oggettiva dell'evento*, *op. cit.* pp. 52 ss.; nonché S. CANESTRARI, *L'illecito penale preterintenzionale*, Padova, Cedam, 1989, pp. 94 ss.. Nonché, L. CORNACCHIA, *Concorso di colpe*, *op. cit.*, p. 420 che evidenzia la funzione di allocazione in capo alla collettività anziché in capo al singolo soggetto che esercita l'attività.

[452] S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.*, p. 339, il quale individua in tale elemento il "significato minimo ed unitamente condiviso" della categoria del rischio consentito.

La definizione di tale area di rischio ammesso dall'ordinamento è l'esito di un bilanciamento fra i pericoli che lo svolgimento di una determinata attività può comportare per la collettività e i benefici che essa è in grado di apportare.

Come evidenziato da V. MILITELLO, *Rischio e responsabilità penale*, *op. cit.,* pp. 164-167, il grado di pericolosità dell'attività è determinato da tre fattori: il tipo di bene giuridico minacciato, la quantità di offese che esso rischia di subire e la probabilità della lesione stessa. L'interesse e l'utilità sociale che 'controbilanciano' la potenziale minaccia vengono definiti considerando, anche in questo caso, il bene giuridico che trae beneficio dall'attività stessa e l'intensità di tale vantaggio. Sicché, "tendenzialmente rientreranno nei limiti del rischio consentito possibilità di verificazione del danno tanto più elevato quanto maggiore sia il valore sociale dell'attività e quanto minore sia l'entità del possibile danno, con l'avvertenza che in ogni caso non potranno legittimarsi attività idonee a ledere beni giuridici con una probabilità vicina alla certezza o, viceversa, non si potranno tendenzialmente precludere condotte in conseguenza delle quali sia del tutto improbabile la verificazione del danno" così G. FORTI, *Colpa ed evento nel diritto penale*, *op. cit.*, p. 266.

[453] Così F. CONSULICH, *Rischio consentito*, in M. Donini (diretto da), Il reato colposo. Enciclopedia del diritto, Milano, Giuffrè, 2021, p. 1104.

l'evento penalmente rilevante, mantenendosi entro l'area di rischio consentito, non può essere rimproverato[454].

In questo contesto si muove dunque l'esercizio di alcune attività, che sempre di più sono caratterizzate dalla coesistenza di 'macchina' e uomo e, in particolare il *trading* algoritmico. Come avviene per la circolazione stradale, prototipo dell'attività rischiosa consentita[455], *mutatis mutandis* nel caso della negoziazione algoritmica, l'area dello svolgimento lecito dell'attività è definita dal bilanciamento fra i benefici che essa è in grado di apportare alla società e la sua pericolosità strutturale verso beni tutelati dall'ordinamento[456].

5.2.2. Il trading algoritmico come attività a rischio consentito

---

[454] Posto che la necessità del rischio consentito si può manifesta con riferimento ad attività che non riducono 'a zero' la pericolosità dell'azione, ma che considerano lecite azioni che conservano un coefficiente di pericolosità anche dopo l'applicazione delle cautele necessarie. Cfr. V. MILITELLO, *Rischio e responsabilità penale*, *op. cit.*, p. 140.

[455] Fra le varie attività, che nella società moderna comportano allo stesso tempo potenziali rischi e altrettanti benefici, un esempio di scuola è quello della circolazione stradale. Sul punto, *ex multis*, M. GALLO, *Colpa penale (diritto vigente)*, *op. cit.*, p. 640. Infatti, la guida di un autoveicolo è di per sé un'attività che può comportare pericoli per la vita e l'integrità della persona. Di fronte a un simile coefficiente di pericolosità, l'ordinamento potrebbe da un lato imporre un divieto assoluto di esercitare l'attività di guida ovvero dall'altro lato regolare tale attività in modo tale da ridurre il rischio del verificarsi di eventi lesivi. Essendo la prima opzione evidentemente inaccettabile, visti benefici economico-sociali che tale attività apporta alla collettività, l'unica alternativa in effetti accettabile è quella di imporre al guidatore cautele volte a prevenire (o almeno contenere entro livelli accettabili) il rischio, come il rispetto dei limiti di velocità, l'obbligo di fermarsi ai semafori e le norme di precedenza. Sicché il guidatore accorto, che si sia conformato ai doveri imposti dall'ordinamento, può contare sul fatto che non verrà chiamato a rispondere del fatto di reato che abbia cagionato nonostante il rispetto di tutte le cautele previste. Ciò non, si badi, non significa che il guidatore sarà esente da responsabilità con riferimento a qualsiasi evento lesivo causato per imprudenza o volontariamente. Come nota F. CONSULICH, *Rischio consentito*, *op. cit.*, p. 1115 "[c]hi travolge con un autoarticolato il pedone che attraversa un'intersezione semaforica con luce verde può ben essere condannato senza che risulti contraddetta la constatazione che la guida è un'attività rischiosa legalmente consentita".

[456] È quella che G. FORTI, *Colpa ed evento*, *op. cit.*, p. 253 definisce "dialettica fra libertà di azione e aspettative di sicurezza della società". I limiti dell'area di rischio consentiti vengono definiti utilizzando criteri normativi e, in particolare, sulla base delle regole cautelari codificate che disciplinano le diverse attività, proprie o improprie (capaci di azzerare il rischio, le prime e solo di contenerlo entro margini tollerabili, le seconde), rigide o elastiche (a seconda che predeterminino o meno in modo assoluto la regola di condotta da adottare) Sul punto ampiamente S. ZIRULIA, Esposizione a sostanze tossiche, op. cit., 360-367; nonché G. FORTI, *Colpa ed evento*, *op. cit.*, p. 258. In particolare per quanto attiene alla distinzione fra regole cautelari proprie e improprie ai fini della definizione dell'area di rischio consentito: P. VENEZIANI, ***Regole cautelari "proprie" ed "improprie" nella prospettiva delle fattispecie colpose causalmente orientate***, Padova, Cedam, 2003, pp. 15-18.

L'esito di tale bilanciamento, nello specifico ambito di cui si tratta, è contenuto nelle norme che regolano l'attività di negoziazione algoritmica, che esprimono un consenso implicito per l'esercizio di tale attività, benché pericolosa, attraverso la sua regolazione.

I vantaggi che il *trading* algoritmico apporta ai mercati vengono fatti risalire principalmente all'aumento di liquidità che esso determina, che favorisce a propria volta l'attenuarsi delle oscillazioni dei prezzi e la riduzione dei costi di transazione. Ciò comporta, tra l'altro, anche maggiore disponibilità a effettuare transazioni da parte degli intermediari che comprano e vendono titoli per conto proprio (*market maker*)[457].

D'altra parte, tale tecnologia è all'origine anche di una serie di potenziali rischi, come l'aumento del sovraccarico dei sistemi nelle sedi di negoziazione a causa del gran numero di ordini o l'eventuale reazione eccessiva ad altri eventi di mercato[458]. O ancora, "la negoziazione algoritmica o la tecnica di negoziazione

---

[457] Oltre al fatto che il *trading* algoritmico può essere estremamente redditizio per il *trader* e per la società di *trading*.

Cfr. Considerando 62 della Direttiva MiFID II, "la tecnologia di negoziazione ha apportato vantaggi al mercato e ai partecipanti al mercato, come una più ampia partecipazione ai mercati, un aumento di liquidità, differenziali più ridotti, minore volatilità a breve termine e i mezzi per ottenere una migliore esecuzione degli ordini per i clienti".

Quanto all'impatto che la negoziazione algoritmica ha sul funzionamento dei mercati, in dottrina si vedano: D. LEIS, *High Frequency Trading*, *op. cit*. pp. 25-26; G. STRAMPELLI–G. BALP, *Preserving Capital Markets*, *op. cit*., pp. 5-15; O. COSME JR., *Regulating High-Frequency Trading*, 2019, *op. cit.*, p. 370: V. CAIVANO, *L'impatto del* trading *ad alta frequenza*, *op. cit.* pp. 1-34; ANGEL J.J.–HARRIS L.E.–SPATT C.S., Equity Trading in the 21st Century, 23 febbraio 2010, in Quarterly Journal of Finance, 2011, vol. 1, issue 1, pp. 1-53; V. MANAHOV–R. HUDSON–B. GEBKA, *Does High Frequency Trading Affect Technical Analysis and Market Efficency? And if So, How?*, in Journal of International Financial Markets Institutions and Money, 2014, vol. 28, pp. 131-157.

Sul punto anche F. CONSULICH, *Il nastro di Möbius*, *op. cit.*, p. 203, pur premettendo che la conoscenza del fenomeno sconta la comparsa relativamente recente degli algoritmi sui mercati, rileva come il giudizio rispetto agli operatori algoritmici non sia univoco e come per alcuni Autori, gli algoritmi di negoziazione ad alta frequenza inciderebbero negativamente "sulla valenza informativa e segnaletica dei prezzi di mercato", secondo altri "forse la maggioranza, sono di opposta opinione e ritengono che la diffusione dell'*hft* non soltanto non pregiudichi l'efficienza degli scambi, ma, al contrario, contribuisca a velocizzare il processo di incorporazione delle informazioni nei prezzi e ridurne il grado di volatilità". Nello stesso senso, F. ANNUNZIATA, *Intelligenza artificiale e disciplina degli abusi di mercato*, Atti del XV Convegno Nazionale Orizzonti del Diritto Commerciale. 23-24 febbraio 2024, in https://www.orizzontideldirittocommerciale.it/atti-dellanno-2024/, p. 15.

[458] Si pensi agli episodi di *flash crash,* fra cui quello del 6 maggio 2010. Sulle cause che hanno determinato l'episodio e sul ruolo specifico dei sistemi di negoziazione algoritmica ad alta frequenza, si veda KIRILENKO A.–KYLE A.S.–SAMADI M.–TUZUN T., *The Flash Crash: High Frequency Trading in an Electronic Market*, in The Journal of Finance, 2017, vol. 72, issue 3, pp.

algoritmica ad alta frequenza possono, come ogni altra forma di negoziazione, prestarsi a talune forme di comportamento, se non utilizzate correttamente, vietate a norma del Regolamento (UE) n. 596/2014"[459].

Questa tensione fra benefici e potenziali rischi, tipica di un ambiente "di rischio istituzionalizzato"[460], ha portato il legislatore a disciplinare l'utilizzo di algoritmi di *trading* in modo dettagliato, tramite una combinazione di misure e controlli specifici del rischio diretti, da un lato, alle imprese che effettuano negoziazioni algoritmiche o adottano tecniche di negoziazione algoritmica ad alta frequenza e di altre misure dirette, d'altro lato, ai gestori delle sedi di negoziazione a cui tale imprese hanno accesso[461].

Si possono dunque considerare, nell'ottica sopra indicata, un insieme di regole di condotta che implicitamente riconoscono la pericolosità dell'attività e che altrettanto implicitamente la facoltizzano, disegnando i limiti entro i quali è possibile esercitare l'attività pericolosa senza vedersi rimproverati gli eventi dannosi che possano occorrere nonostante il rispetto delle regole che disciplinano l'attività stessa.

L'obiettivo sotteso è quello di scongiurare l'eventualità che i sistemi di negoziazione algoritmica creino un mercato disordinato o che vengano utilizzati per scopi vietati, fra cui la commissione di abusi di mercato. Tali norme dunque rispondono a una logica preventiva, a fronte di un'attività che presenta indubbi profili di pericolosità.

Perciò, di fronte ai possibili pericoli derivanti dall'utilizzo dei sistemi di negoziazione algoritmica, il legislatore tratteggia i limiti entro i quali tale utilizzo è

967-998. Altri episodi si sono registrati nel 2012 (1 agosto 2012, Knight Capital) e nel 2016 (7 ottobre 2016, episodio di c.d. *fat finger*).

[459] Considerando 62 della Direttiva MiFID II.

[460] Cfr. C. PIERGALLINI, *Danno da prodotto e responsabilità penale*, *op. cit.*, p. 11 definisce i mercati finanziari quali "ambienti di rischio istituzionalizzati che condizionano le aspettative di numerose persone".

[461] L'obiettivo specifico – ed espressamente indicato nel Considerando 63 della Direttiva MiFID II – è proprio "mitigare tali rischi potenziali derivanti da un maggior ricorso alla tecnologia". L'ottica prudenziale e di controllo e gestione dei potenziali rischi derivanti dalla negoziazione algoritmica è propria, oltre che della Direttiva MiFID II e tra le numerose disposizioni, dei regolamenti che ingrano tale Direttiva, ossia: Regolamento Delegato UE 2017/589 (requisiti organizzativi delle imprese di investimento che effettuano negoziazione algoritmica, già RTS 6); del Regolamento Delegato UE 2017/584 (requisiti organizzativi delle sedi di negoziazione, già RTS 7); Regolamento Delegato UE 2017/578 (obblighi in materia di accordi e sistemi di *market making*, già RTS 8); Regolamento Delegato UE 2017/565; t.u.f. (D.lgs. 24 febbraio 1998, n. 58 specificamente artt. 65 *sexies* e 67 *ter*); nonché il Regolamento Mercati Consob (Delibera Consob n. 20249 del 28 dicembre 2017 e successive modifiche). Cfr. sul punto F. CONSULICH, Flash offenders, *op. cit.*, pp. 1044-1046.

ritenuto lecito per scongiurare scelte alternative inaccettabili, quale ad esempio porre un divieto assoluto a tale attività[462].

L'impianto fornisce una cornice normativa entro cui il *trader* può – per dirla con Marinucci – realizzare impunemente la sua attività pericolosa, regole cautelari scritte attraverso cui l'ordinamento disciplina una determinata attività e che sono il risultato del bilanciamento di interessi tra pericolosità dell'attività e i suoi risvolti socialmente utili[463], nella consapevolezza che "tutti i diritti fondamentali tutelati dalla Costituzione si trovano in rapporto di integrazione reciproca e non è possibile individuare uno di essi che abbia la prevalenza assoluta sugli altri"[464].

Sicché, così come – pur con le dovute, non trascurabili, differenze[465] – il produttore è tenuto a rispettare degli obblighi prima e dopo l'introduzione del

---

[462] Ovviamente, partendo dal presupposto che la probabilità del verificarsi di lesioni al bene giuridico tutelato – il corretto funzionamento del mercato – sia effettivamente reale, ma non superi una soglia di 'tollerabilità' che imporrebbe un divieto assoluto di svolgimento dell'attività stessa. Sul punto, G. FORTI, *Colpa ed evento*, *op. cit.*, p. 256; nonché S. ZIRULIA, *Esposizione a sostanze tossiche e responsabilità penale*, op. cit., p. 371 "è la stessa vita di relazione che, mettendo tra loro in contatto i beni giuridici, costringe entro una certa misura a comprimerne alcuni a beneficio di altri" altrimenti "il legislatore si troverebbe costretto a compiere scelte assurdamente drastiche quali vietare la circolazione stradale, vietare la produzione e la vendita di bevande alcoliche, spostare sulla sanità la spesa pubblica attualmente indirizzata alle attività culturali e via dicendo".

[463] G. MARINUCCI, *La colpa per inosservanza*, *op. cit.*, p. 170, secondo cui le regole prudenzialiscritte "se non valgono […] a fissare una immutabile falsariga per il comportamento dell'agente, servono però a tracciare gli schemi fondamentali entro i quali può realizzare, impunemente, la sua attività pericolosa".

[464] Corte Cost., 9 maggio 2013, n. 85, Rel. Silvestri.

[465] Posto che: i) la responsabilità del produttore ha natura colposa e ii) l'algoritmo di *trading* non può essere considerato un 'prodotto' vero e proprio, dal momento che, una volta immesso sul mercato, non viene usato da consumatori 'inesperti' (come avviene invece, ad esempio, per le automobili a guida autonoma), bensì è uno strumento che rimane sostanzialmente nelle mani di chi l'ha progettato – i programmatori delle società che effettuano il *trading* – e che quindi proprio per questo sono utilizzatori particolarmente qualificati, in grado di utilizzarlo al meglio e di riconoscerne i profili di pericolosità. L'algoritmo di *trading* infatti non esce dalla sfera del produttore, non circola fra un numero indefinito di destinatari, come invece avviene per la maggior parte dei prodotti in commercio, compresi quelli che integrano sistemi di intelligenza artificiale, come ad esempio le automobili a guida autonoma. Queste ultime, una volta uscite dalla sfera di controllo del programmatore, possono produrre rischi che chi ha programmato la macchina non può direttamente governare.

Per il parallelismo fra 'prodotto' e il sistema di intelligenza artificiale, si vedano, seppur con visioni parzialmente divergenti, F. CONSULICH, Flash offenders, *op. cit.*, pp. 1038-1040; A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.,* p. 506; ID., *Profili penalistici delle* self-driving cars, Dir. Pen. Cont. Riv. Trim., 2019, fasc. 2, pp. 19-20; C. PIERGALLINI, *Intelligenza artificiale*, *op. cit.*, pp. 1753 ss.; S. GLESS–E. SILVERMAN–T. WEIGEND, *If robots cause harm, who is to blame?*, *op. cit.*, pp. 412-436 nonché B. FRAGASSO, *La responsabilità penale del produttore*, *op. cit.*, p. 33 secondo

prodotto sul mercato, anche l'attività di *trading* può essere esercitata solo in conformità a una serie di "doveri di controllo e organizzazione prudenziale"[466], preventivi e successivi all'immissione.

5.2.3. I confini del trading algoritmico consentito: i doveri di organizzazione e controllo delle sedi di negoziazione e di chi svolge l'attività

Da un lato, le sedi di negoziazione sono tenute a predisporre sistemi, procedure e meccanismi efficaci per assicurare la resilienza dei mercati e l'ordine nelle negoziazioni e, in particolare, per identificare gli atti che possono costituire comportamenti vietati dal Regolamento MAR[467].
Dall'altro lato, chi svolge *trading* algoritmico è tenuto a rispettare a una serie di obblighi relativi alla fase precedente all'immissione dei sistemi sul mercato e

---

cui il dibattito intorno all'intelligenza artificiale fa riemergere questioni mai sopite in tema di responsabilità penale per danno da prodotto, quali "l'indebita sovrapposizione tra struttura commissiva e omissiva del reato; l'ostica identificazione dei soggetti personalmente responsabili all'interno delle organizzazioni complesse; l'individuazione del nesso di causalità in relazione a prodotti caratterizzati da opacità; l'accertamento della colpa in situazioni di incertezza scientifica". Il concetto di responsabilità del produttore per danno da prodotto è tradizionalmente ricondotto alle offese provocate ai consumatori per la messa in commercio di prodotti difettosi (c.d. responsabilità per il tipo di produzione) e a quelle provocate dall'attività produttiva ai beni vita e salute dei soggetti interessati dall'attività di impresa (c.d. responsabilità per il modo di produzione). Definizione che risale a F. BRICOLA, *Responsabilità penale per il tipo e modo di produzione*, in AA.VV., La responsabilità per i danni all'ambiente e ai consumatori, Milano, 1978, pp. 75 ss, poi in Scritti di diritto penale, vol. I, tomo II, Milano, Giuffrè, 1997, pp. 1231-1254, per una rilettura si vedano D. CASTRONUOVO, *Responsabilità da prodotto op. cit.*, pp. 301-340 e C. PERINI, *Il concetto di rischio*, *op. cit.*, pp. 239-240. Sugli obblighi del produttore prima dell'introduzione del prodotto sul mercato, in particolare il dovere di immettere sul mercato prodotti sicuri e fornire informazioni utili alla valutazione e alla prevenzione dei rischi connessi all'uso del prodotto, di cui all'art. 104, primo e secondo comma, cod. cons. in relazione al settore della sicurezza generale dei prodotti si veda l'approfondita analisi di R. BERTOLESI, *Intelligenza artificiale e responsabilità penale*, *op. cit.*, pp. 143 ss.

[466] Così F. CONSULICH, *Manipolazione del mercato e declino*, *op. cit*., p. 18.

[467] Per gli obblighi imposti ai mercati regolamentati e ai gestori di sistemi multilaterali di negoziazione o sistemi organizzati di negoziazione, si vedano: Regolamento Delegato UE 2017/584 (già RTS 7), nonché art. 9 Regolamento Mercati (Delibera Consob n. 20249 del 28 dicembre 2017 e successive modifiche), l'art. 65 *ter* t.u.f. e in particolare, il secondo comma, lett. f) a norma della quale essi dispongono di "sistemi, procedure e meccanismi efficaci: […] per controllare gli ordini inseriti, incluse le cancellazioni e le operazioni eseguite dai loro membri o partecipanti o clienti, per identificare le violazioni delle regole del sistema, le condizioni di negoziazione anormali o gli atti che possono indicare comportamenti vietati dal regolamento (UE) n. 596/2014 o le disfunzioni del sistema in relazione a uno strumento finanziario". Gli atti che possono indicare un comportamento vietato ai sensi del regolamento (UE) n. 596/2014 devono essere segnalati senza indugio alla Consob, *ex* art. 65 *septies*, quarto comma, t.u.f.

alcune cautele che invece riguardano la fase successiva[468]. Tali regole sono plasmate sulla possibilità che il sistema – pur immesso sul mercato in modo rispettoso delle norme pre-immissione – mostrino successivamente segnali di pericolosità ulteriore.

L'elemento centrale attorno a cui ruotano le regole di prevenzione del rischio che vincolano chi svolge la negoziazione algoritmica è la conoscenza specifica dei meccanismi di funzionamento dei sistemi, per consentire l'autovalutazione dei rischi che il loro impiego comporta, secondo la logica per cui tipi di rischi diversi dovrebbero essere oggetto di tipi diversi di controlli[469].

Sicché, chi effettua *trading* algoritmico deve essere necessariamente autorizzato come impresa di investimento ed è tenuto a predisporre presidi organizzativi generali e di governo dei sistemi[470], il personale preposto al controllo deve avere almeno "una conoscenza generale delle modalità di funzionamento dei sistemi di negoziazione algoritmica"[471] e comunque deve essere in continuo contatto con le persone dell'impresa che abbiano una conoscenza tecnica approfondita dei sistemi stessi[472].

---

[468] Ci si riferisce in particolare Proseguendo nel parallelismo con la responsabilità da prodotto, come sottolinea R. BERTOLESI, *Intelligenza artificiale e responsabilità penale*, *op. cit.*, "esistono dei casi in cui il prodotto sia introdotto sul mercato nel pieno rispetto dei doveri di diligenza cristallizzati in norme tecniche, codici di condotta, etc e, soltanto successivamente, mostri segnali di una pericolosità 'ulteriore' a quella linea di principio consentito".

[469] Considerando 11 Regolamento Delegato UE 2017/589 (già RTS 6).

[470] Art. 1 Regolamento Delegato UE 2017/589 (già RTS 6) impone di adottare un "dispositivo di *governance* chiaro e formalizzato, che tiene conto della natura, delle dimensioni e della complessità dell'attività svolta", nonché di prevedere chiare linee di responsabilità, procedure efficaci per la comunicazione di informazioni all'interno dell'impresa di investimento, nonché la separazione tra i compiti e le responsabilità delle sale operative e le funzioni di supporto e controllo del rischio, per impedire che vengano occultate attività di negoziazione non autorizzate.

[471] Art. 2 Regolamento Delegato UE 2017/589 (già RTS 6).

[472] In base all'art. 3 del Regolamento Delegato UE 2017/589 (già RTS 6), le persone in possesso delle competenze necessarie per gestire i sistemi di negoziazione devono essere in "numero sufficiente" e devono possedere conoscenze tecniche in relazione ai sistemi e gli algoritmi utilizzati, al monitoraggio e alle prove degli stessi, nonché conoscere le strategie di negoziazione messe in atto e gli obblighi giuridici dell'impresa di investimento. Tali doveri devono essere rispettati anche nel caso in cui l'*hardware* e il *software* utilizzati per la negoziazione algoritmica siano acquisiti mediante esternalizzazione o appalto (art. 4 del Regolamento Delegato UE 2017/589).

Su chi effettua negoziazione algoritmica incombono poi obblighi di sviluppo e verifica dei sistemi precedenti all'installazione e al rilascio[473], volte ad assicurare che l'algoritmo non si comporti in modo imprevisto, sia conforme agli obblighi imposti alle imprese di investimento e alle regole delle sedi di negoziazione e che non contribuisca a creare condizioni di negoziazione anormali, continui a funzionare in caso di condizioni di stress del mercato e, se necessario, consenta la disattivazione del sistema[474].

Sono dunque obblighi finalizzati a far emergere rischi o pericoli non riconoscibili al momento dell'immissione sul mercato dell'algoritmo.

Inoltre, nella fase successiva all'installazione, le imprese di investimento sono tenute a effettuare autovalutazioni e convalide annuali[475] e soprattutto devono monitorare "tutte le attività di negoziazione che avvengono sui propri sistemi di negoziazione, comprese quelle dei clienti, per individuare segnali di potenziali manipolazioni del mercato ai sensi dell'art. 12 del Regolamento (Ue) n. 596/2014"[476].

I contenuti specifici delle cautele che l'impresa di investimento deve adottare per l'individuazione delle manipolazioni del mercato sono descritti in modo puntuale dal Regolamento Delegato UE 2017/589, che impone l'utilizzo di un sistema automatizzato di sorveglianza, in grado di monitorare gli ordini e le operazioni, di generare allarmi e produrre rapporti; nonché di raccogliere e analizzare *ex post* i dati sugli ordini e le operazioni[477]. Tale sistema di sorveglianza automatico deve

---

[473] I test precedenti all'installazione o all'aggiornamento del sistema – effettuati in base a metodologie chiaramente definite – devono essere effettuati un in ambiente di prova distinti dall'ambiente di produzione, "dedicato specificatamente allo sviluppo e alle prove dei sistemi di negoziazione algoritmica e degli algoritmi di negoziazione" (art. 7 Regolamento Delegato UE 2017/589).

[474] Art. 5 Regolamento Delegato UE 2017/589 e art. 67 *ter*, primo comma lett. a) t.u.f.

[475] Così come impone l'art. 9 del Regolamento Delegato UE 2017/589. Il procedimento di autovalutazione deve riguardare in particolare la capacità di sopportare un aumento del flusso degli ordini o le condizioni di stress del mercato (art. 10 del Regolamento stesso).

[476] Art. 67 ter t.u.f., primo comma, lett. b) e c) e art. 13 Regolamento Delegato UE 2017/589. Tale controllo, insieme alla c.d. *kill functionality*, al monitoraggio in tempo reale sulle attività di negoziazione algoritmica e ai controlli pre e post-negoziazione fa parte degli strumenti di cui l'impresa di investimento deve munirsi per garantire la resilienza dei sistemi di cui al Capo II Resilienza dei sistemi di negoziazione, Sezione III Mezzi per assicurare la resilienza del Regolamento Delegato.

[477] Il sistema automatizzato – concepito in funzione delle specifiche caratteristiche dell'attività svolta dall'impresa di investimento – deve sorvegliare l'intera gamma delle attività di negoziazione e tutti gli ordini immessi. Le segnalazioni inviate dal sistema devono essere

assicurare il rispetto delle condizioni imposte dai regolamenti e deve essere adeguato rispetto alla specifica attività di negoziazione svolta[478].

Inoltre, il personale preposto deve avere un potere di intervento effettivo sui sistemi di negoziazione algoritmica che passa per una conoscenza generale dei meccanismi di funzionamento degli stessi e delle relative strategie, nonché una competenza sufficiente per dare seguito alle informazioni trasmesse con allarmi automatici. Ma soprattutto devono godere della "sufficiente autorità per opporsi alla persona responsabile nei casi in cui questa attività crei condizioni negoziazione anormali o faccia sorgere sospetti di abusi di mercato"[479].

In capo a chi svolge negoziazione algoritmica incombono poi alcuni poi gli obblighi specifici di interlocuzione e comunicazione alla Consob delle misure organizzative e di gestione del rischio adottate per prevenire comportamenti anomali o contrari alle disposizioni del Regolamento MAR[480].

---

analizzate e confrontate con altre attività di negoziazione pertinenti svolte dall'impresa (art. 13 par. 3 Regolamento Delegato UE 2017/589).

Inoltre, il sistema deve essere in grado di "generare allarmi operabili all'inizio del successivo giorno di negoziazione o, in caso di elaborazione manuale, alla fine del successivo giorno di negoziazione. Il sistema di sorveglianza […] è dotato di documentazione e procedure adeguate che consentano di dare un seguito effettivo agli allarmi da esso generati" (art. 13 par. 7 Regolamento Delegato UE 2017/589).

[478] Adeguatezza che deve essere riesaminata almeno una volta l'anno (art. 13, par. 6 Regolamento Delegato UE 2017/589).

[479] Art. 3 Regolamento delegato (UE) 2017/589. In particolare, per quanto riguarda il dovere di monitoraggio in tempo reale, è fatto obbligo, durante le ore di invio di ordini ai mercati regolamentati, di monitorare in tempo reale tutte le attività di *trading* algoritmico che avvengono sotto il codice di *trading* dell'impresa, comprese quelle dei suoi clienti, per segni di *trading* disordinato, inclusa l'attività di *trading* tra mercati, classi di *asset* o prodotti, nei casi in cui l'impresa o i suoi clienti si impegnano in tali attività. Il monitoraggio in tempo reale del *trading* algoritmico deve essere effettuato dal responsabile dell'algoritmo di *trading* o della strategia di *trading* algoritmico e dalla funzione di gestione del rischio o da una funzione di controllo del rischio indipendente stabilita per questo scopo. Tale funzione di controllo non deve essere gerarchicamente dipendente dal responsabile dell'algoritmo.

[480] Ai sensi dell'art. 67 ter, secondo comma, t.u.f. (che recepisce l'art. 17 par. 2 MiFID II) lo svolgimento di negoziazione algoritmica deve essere notificato alla Consob (o alla diversa autorità dello Stato membro della sede di negoziazione in cui effettuano l'attività).

La Consob, secondo quanto previsto dal terzo comma del medesimo articolo, oltre a vigilare sul rispetto dei requisiti organizzativi e di gestione, può chiedere, su base regolare o ad hoc: a) una descrizione della natura delle strategie di negoziazione algoritmica; b) i dettagli sui parametri o sui limiti di negoziazione a cui il sistema è soggetto; c) i controlli di conformità e di rischio attuati per assicurare i propri sistemi di negoziazione algoritmica siano resilienti e dispongano di sufficiente capacità d) i dettagli sulla verifica dei sistemi; e) ulteriori informazioni sulla negoziazione algoritmica effettuata e sui sistemi utilizzati.

La previsione di tali obblighi è un'ulteriore conferma della riconducibilità dell'attività a un "ambito normalmente lecito nel suo complesso"[481]. Si ricadrebbe infatti in un'inaccettabile contraddizione se si considerasse illegittima un'attività rispetto alla quale un'autorità amministrativa, pur non conferendo alcuna autorizzazione, potesse in ogni caso ricevere informazioni e imporre l'adozione di misure per lo svolgimento dell'attività stessa[482].

Le previsioni sin qui illustrate confermato dunque la possibilità di ricondurre la negoziazione algoritmica nello spettro delle attività che, pur potendo agevolare il verificarsi di eventi lesivi per beni giuridici rilevanti – nello specifico, abusi di mercato –, sono ammesse dall'ordinamento.

L'attività di *trading* algoritmico pur potenzialmente foriera di rischi per l'integrità dei mercati, è lecita se esercitata nel rispetto dei requisiti sopra illustrati.

Ciò comporta – in via generale – che qualora chi è responsabile della programmazione e della gestione dell'algoritmo si sia conformato a tali regole cautelari, non può essere chiamato a rispondere degli eventi che si verifichino malgrado il rispetto di tali norme[483].

Se dunque i rischi che persistono nonostante l'adeguamento a tali regole costituiscono rischi consentiti o tollerati dall'ordinamento, tendenzialmente[484] il programmatore che abbia concepito l'algoritmo in conformità alle norme che regolano la negoziazione algoritmica potrà dunque riporre un ragionevole

---

Inoltre, l'articolo 48, secondo comma, del Regolamento Consob n. 20249/2017 ("RM") dispone che le s.i.m. e le banche italiane comunichino alla Consob, in sede di avvio dell'operatività e in occasione di ogni successivo cambiamento, lo svolgimento di attività di negoziazione algoritmica o l'implementazione di tecniche di negoziazione algoritmica ad alta frequenza, fornendo gli elementi informativi di seguito indicati: a) la data di avvio operatività; b) le sedi di negoziazione su cui si svolge l'attività, identificate da apposito codice MIC; c) la classe degli strumenti finanziari su cui si svolge l'attività; d) l'eventuale svolgimento di attività di negoziazione algoritmica o *hft* tramite DEA al mercato.

[481] V. MILITELLO, *Rischio e responsabilità penale*, *op. cit.*, p. 120.

[482] Sulle autorizzazioni amministrative come fonti del rischio consentito si veda V. MILITELLO, *Rischio e responsabilità penale*, *op. cit.*, pp. 91 ss.

[483] Cfr. Sulla funzione di garanzia dell'iniziativa del singolo della categoria del rischio consentito, G. MARINUCCI, *La colpa per inosservanza di leggi*, *op. cit.*., p. 198; nonché C. RUGA RIVA, *Il principio di precauzione*, *op. cit.*, pp. 1756-1757 "l'*osservanza* dei limiti dettati dal legislatore in via precauzionale, allo scopo di fronteggiare pericoli ipotetici, dovrebbe escludere la punibilità dell'agente che, pur rispettandoli, abbia causato eventi offensivi". Almeno, come si approfondirà *infra*, "nella misura in cui le soglie di attenzione non siano invalidate da successive diverse conoscenze scientifiche, che ne dimostrino l'inadeguatezza a contrastare pericoli".

[484] Salvo le ipotesi legate allo sviluppo tecnologico e all'eventuale fallimento della regola cautelare, di cui si tratterà *infra*.

affidamento sul fatto che non potrà essere chiamato a rispondere degli eventuali illeciti cagionati dall'operare degli algoritmi stessi[485].
Viceversa, i rischi derivanti dalla condotta di chi usa l'algoritmo di *trading* discostandosi deliberatamente dall'area del rischio consentito o tollerato dall'ordinamento, sono idonei a costituire il fondamento di un rimprovero penale. Posto che "laddove l'agente si sia comportato in maniera contraria al dovere di diligenza, potrà profilarsi a suo carico una responsabilità per la causazione lesiva a titolo di dolo o colpa"[486].
Ed è in effetti in questo ambito che, come si vedrà, pare muoversi l'attuale sistema che regola l'operatività dei sistemi di negoziazione algoritmica.
Chiarito quindi il contesto entro il quale si inquadra il fenomeno degli 'abusi di mercato algoritmici', si illustreranno alcune ipotesi in cui la commissione del reato è l'esito di una decisione umana, di una programmazione incompleta o scorretta o di una decisione 'autonoma' dell'algoritmo al fine di valutare l'effettività del sistema sanzionatorio attualmente vigente con riferimento a tali fatti[487].

6. Gli 'abusi di mercato algoritmici': i principali profili di problematicità

All'interno del quadro sin qui delineato, partendo dalla considerazione secondo cui il *trading* algoritmico può essere qualificato come attività rischiosa ma consentita entro determinati limiti, occorre vagliare in quali casi e in che termini tale l'attività possa assumere rilevanza penale.
A tal fine, si distinguerà fra diverse ipotesi – che, lo si anticipa sin d'ora, presentano diversi gradi di problematicità – a seconda del tipo di sistema di

---

[485] Sulla funzione di tutela dell'affidamento della definizione dell'area di rischio consentito si veda ampiamente G. FORTI, *Colpa ed evento*, *op. cit.*, pp. 281-289.

[486] S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.*, p. 396.

[487] Nell'analisi che verrà condotta, si parte dal presupposto che, nell'attuale sistema dei mercati finanziari, le società di *trading*, che svolgono direttamente attività di negoziazione sui mercati, dispongono di *team* interni dedicati alla programmazione degli algoritmi di *trading*. In questo contesto, non vi è una netta separazione tra chi sviluppa il *software* e chi lo utilizza, poiché la programmazione degli algoritmi è strettamente integrata all'interno della stessa struttura operativa della società. Di conseguenza, si assumerà l'esistenza di una sorta di identità funzionale tra il programmatore e l'utilizzatore dell'algoritmo, presupponendo che la volontà della società, e dunque del *trader*, si rifletta interamente nelle scelte programmate dell'algoritmo. Questo approccio consente di affrontare le questioni legate alla responsabilità per abusi di mercato non solo dal punto di vista di chi opera materialmente le transazioni, ma anche da quello di chi ha contribuito a modellare il comportamento dell'algoritmo, ritenuto elemento essenziale dell'attività di *trading*.

negoziazione impiegato: algoritmi 'tradizionali', da un lato e algoritmi basati su sistemi di intelligenza artificiale 'forte', dall'altro.
Nel primo caso – quello che presuppone l'uso di sistemi tradizionali – l'abuso di mercato può essere determinato da: i) l'utilizzo deliberato e malevolo dell'algoritmo di *trading*; ii) la mancata o inadeguata programmazione dell'algoritmo rispetto alle norme che governano l'attività.
Tali scenari sono ipotizzabili anche nella seconda ipotesi di 'abuso di mercato algoritmico', quello che vede coinvolti algoritmi basati su sistemi di intelligenza artificiale 'forte', a cui se ne aggiunge un terzo. In questo caso infatti l'abuso di mercato può essere dovuto a: i) l'utilizzo deliberato e malevolo dell'algoritmo di *trading*; ii) la mancata o inadeguata programmazione dell'algoritmo rispetto alle norme che governano l'attività e iii) la mancata adozione di misure ulteriori rispetto a quelle previste dalle regole che governano l'attività, di cui era prevedibile l'inadeguatezza.

7. Gli 'abusi di mercato algoritmici': l'utilizzo di sistemi di negoziazione algoritmica 'tradizionali'

Come anticipato, la realizzazione di condotte abusive tramite sistemi di negoziazione algoritmica 'tradizionali' può dipendere dall'utilizzo deliberato e malevolo degli algoritmi ovvero dalla mancata o inadeguata programmazione degli stessi.
Si tratta di casi che, seppur differenti, possiedono una caratteristica comune: la natura meramente strumentale dell'algoritmo di *trading*.
Ciò comporta che il destinatario della sanzione per il comportamento abusivo sia necessariamente l'essere umano che lo programma o lo utilizza e che il tipo di sanzione inflitta – penale o amministrativa – dipenda essenzialmente dall'elemento soggettivo che sorregge il suo agire.

7.1. Gli 'abusi di mercato algoritmici' tradizionali: il primo scenario

Il primo scenario che si analizzerà è dunque quello che riguarda l'utilizzo deliberato di un sistema di negoziazione algoritmica per la commissione di un abuso di informazioni privilegiate o di una manipolazione del mercato[488]. Sono

[488] Sebbene quest'ultima sia più frequente, al punto che il legislatore europeo, all'art. 12, par. 2, lett. c.) del regolamento MAR, nel tipizzare l'illecito di manipolazione del mercato, fa espresso riferimento alla negoziazione algoritmica; mentre lo stesso non avviene per la fattispecie di *insider trading*.

cioè i casi in cui l'alterazione del corretto funzionamento del mercato sia l'esito di un impiego malevolo volontario delle potenzialità dei sistemi di negoziazione algoritmica.

La capacità di inserimento di ordini di acquisto per elevate quantità e l'estrema velocità di azione fanno della negoziazione algoritmica lo strumento ideale di distorsione abusiva dei prezzi degli strumenti finanziari.

Come anticipato, fra gli schemi di *trading* algoritmico più noti si possono citare le pratiche sopra illustrate di *pump and dump* e *trash and cash*, *marking the close*, *painting the tape*, *spoofing*, *layering*, nonché *quote stuffing e smoking, pinging*.

Ebbene, non vi sono particolari dubbi che qualora questi schemi vengano materialmente posti in essere dall'algoritmo su decisione dell'essere umano le diverse condotte incorrerebbero nel divieto di manipolazione del mercato come attualmente formulato.

Ciò, si badi, non comporta che l'algoritmo possa o debba essere considerato responsabile dell'illecito. Al contrario, la lesione del bene giuridico rimane nel pieno dominio di chi utilizza l'algoritmo stesso. Vale a dire che in questo caso non si pone in discussione che la 'macchina' sia una mera esecutrice della volontà umana, un suo strumento.

Il fatto, dunque, in questa ipotesi non è dell'algoritmo.

Per questa ragione, è fondamentale volgere l'attenzione allo stato psicologico soggetto che opera sui mercati tramite algoritmi di *trading*.

L'utilizzo di un sistema di negoziazione algoritmica per commettere il reato può avvenire perché – come nei casi americani e inglesi sopracitati – chi fa *trading* ha deliberatamente scelto di utilizzare un sistema algoritmico 'classico' (ad esempio ad alta frequenza) o uno basato su sistemi di intelligenza artificiale 'debole' per compiere condotte abusive. Oppure perché si è servito di una 'macchina', che deliberatamente non era stata programmata in modo tale da evitare la commissione di operazioni illecite.

Oggetto del rimprovero è dunque, in definitiva, l'aver tenuto una condotta attiva di incorporazione nel codice di programmazione della strategia abusiva o di aver omesso una opportuna programmazione atta a evitare che la macchina ponesse in essere detta strategia, previa la rappresentazione e volizione dell'abuso di mercato per come si è effettivamente verificato[489]. In questi i casi il

[489] A. AZZUTTI–W.G. RINGE–H.S. STIEHL, *Machine Learning, Market Manipulation*, *op. cit.*, p. 117: "Le turbative del mercato possono derivare anche da algoritmi creati e utilizzati consapevolmente da esseri umani per scopi illeciti. In questi casi, l'abuso di mercato algoritmico

comportamento volontario è dunque penalmente rilevante, poiché sia la manipolazione di mercato sia l'abuso di informazioni privilegiate sono fattispecie dolose[490].

L'art. 185 t.u.f. richiede infatti un dolo generico avente ad oggetto, oltre la volontà di diffondere notizie false o il compimento di artifici, anche la loro idoneità a provocare una sensibile alterazione del prezzo di strumenti finanziari, senza che sia richiesta alcuna finalità ulteriore.

Così l'art. 184 t.u.f. che considera penalmente rilevanti solo le condotte supportate dalla rappresentazione della natura privilegiata dell'informazione e la volontà di utilizzarla, comunicarla a terzi o raccomandare operazioni sulla base di questa.

La dimostrazione della sussistenza del dolo dovrà quindi passare per l'accertamento del fatto che l'abuso di mercato algoritmico sia stato progettato, addestrato e voluto o comunque accettato come conseguenza dell'uso di un algoritmo non del tutto dominabile[491].

Ciò è avvenuto, ad esempio, nel processo Coscia nel quale si è dimostrato che il *trader* avesse chiesto a un programmatore di concepire un algoritmo di negoziazione ad alta frequenza che fosse in grado di posizionare piccoli ordini di vendita a un prezzo inferiore al prezzo di mercato di quel momento e contemporaneamente ordini acquisto di grande volume dall'altro lato del mercato, in modo tale da creare l'illusione di un movimento di mercato e negoziare poi il piccolo ordine di vendita a un prezzo più alto[492].

è 'by-design'" (traduzione nostra). In questo senso, occorre evidentemente accertare la rappresentazione e volizione da parte dell'agente delle concrete modalità di manipolazione per come effettivamente si è verificata e non una generica perturbazione del mercato in astratto. Altrimenti, come nota F. CONSULICH, *Il nastro di Möbius*, *op. cit.*, p. 219, il dolo del fatto si trasformerebbe in una sorta di dolo generale. Sull'inaccettabilità di richiedere ai fini del dolo la coscienza e volontà di offendere, genericamente, gli interessi dell'economia pubblica quale evento in senso giuridico, si veda C. PEDRAZZI, *Problemi del delitto di aggiotaggio*, *op. cit.*, p. 15.

[490] Si tratta, come nota A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.,* pp. 499-520, di reati "a matrice dolosa commessi dall'uomo a mezzo IA", in cui il sistema è disegnato appositamente perché in date condizioni commetta un certo delitto, cui abbia interesse.

[491] Sulla base della duplice componente psicologica del dolo: rappresentazione e volontà degli elementi che integrano la fattispecie oggettiva. Cfr., *ex multis*, limitandosi a parte della manualistica, G. FIANDACA–E. MUSCO, *Diritto penale. Parte Generale*, IX ed., Bologna, 2024, pp. 363-381; G. MARINUCCI–E. DOLCINI–G.L. GATTA, *Manuale di diritto penale*, *op. cit*., pp. 392-418.

[492] La norma americana anti-*spoofin*g 7 U.S.C. § 6c(a)(5)(C), impone la prova del fatto che il soggetto abbia immesso l'ordine sul mercato con l'intento di cancellarlo prima dell'esecuzione. Questa previsione impone dunque un particolare onere all'accusa, che limita la condanna ai soli casi in cui sia dimostrata tale volontà.

Evidentemente, l'intensità del dolo varia nel caso in cui si dimostri che il soggetto ha programmato l'algoritmo allo scopo di commettere l'illecito (come, ad esempio, nei procedimenti Coscia e Navinder Sarao)

Per quanto attiene a questo primo scenario dunque, essendo l'algoritmo un mero strumento dell'uomo non si pongono particolari ostacoli all'applicazione dei tradizionali modelli di attribuzione della responsabilità[493].

Sicché il soggetto penalmente responsabile può essere individuato nel programmatore, se incardinato nella società di *trading* ovvero il soggetto che se ne serve (*trader*), salva la dimostrazione della sussistenza del dolo[494].

Se dunque da un punto di vista teorico le attuali fattispecie si mostrino adeguate a contrastare il fenomeno dell'utilizzo deliberato dell'algoritmo come strumento di commissione del reato, occorre però segnalare la necessità di un accertamento rigoroso della responsabilità in concreto.

In questo senso, vengono in soccorso gli indicatori di manipolazione informativa e operativa contenuti nell'Allegato I al Regolamento MAR e nell'Allegato II al Regolamento Delegato 2016/522.

La circostanza che determinate operazioni o ordini costituiscano una quota significativa del volume degli scambi giornaliero di un titolo; l'avvio di operazioni di parte di persone con un'importante posizione di acquisto o di vendita, l'immutata titolarità economica di uno strumento finanziario all'esito di un'operazione; la concentrazione di ordini in un breve lasso di tempo che determina una variazione successivamente invertita; nonché l'esecuzione di operazioni contestualmente o in un momento ravvicinato alla diffusione di informazioni false o fuorvianti o alla diffusione o elaborazione di raccomandazioni

---

[493] Si rientra, dunque, nell'ambito di sistemi di intelligenza che non rinunciano al controllo umano e che si atteggiano "come meri strumenti di altri attori", dei quali sono "un prolungamento", così C. PIERGALLINI, *Intelligenza artificiale*, *op. cit*., p. 1750.

D'altra parte, come si è dimostrato, la maggior parte di questi comportamenti potrebbe effettivamente rientrare nelle forme tradizionali e ben note di manipolazione di mercato, già affrontate dalla Direttiva sull'Abuso di Mercato del 2003 e ora ribadite dal Regolamento sull'Abuso di Mercato: non si tratta quindi di nuove forme di manipolazione di per sé, ma si sviluppano attraverso l'uso di algoritmi, spesso con grande velocità. In questo senso, F. ANNUNZIATA, *Artificial* Intelligence, *op. cit.*, p. 145.

[494] F. D'ALESSANDRO, *La manipolazione del mercato*, *op. cit.*, p. 215 sottolinea la necessità di un accertamento particolarmente rigoroso dell'elemento soggettivo, che rifugga "da inversioni metodologiche che si configurino come impossibili scorciatoie nell'accertamento dell'illecito". Nello stesso senso L. FOFFANI, *Art. 185 t.u.f.*, in F. Palazzo–Paliero C.E. (a cura di), Commentario breve alle leggi penali complementari, Padova, II ed., 2007, il quale ammonisce di fronte al rischio di un "pericoloso slabbramento del dolo eventuale" ove non venga debitamente valorizzata la natura dissimulatoria o ingannatrice della condotta complessivamente considerata.

di investimento sono errate o tendenziose o manifestamente influenzate da interessi determinanti sono tutti elementi che – per quanto non tassativamente rivelatori di una manipolazione – costituiscono un utile strumento interpretativo per il giudice[495].

Gli indicatori potrebbero essere peraltro rilevati anche dai più sofisticati sistemi di *machine learning* progettati per individuare gli abusi di mercato. Questi strumenti sono infatti in grado di rilevare gli scostamenti nell'operatività di un investitore dal comportamento medio e in caso di superamento di certa soglia di sensitività, di segnalarlo come anomalo e potenzialmente meritevole di approfondimenti ulteriori[496].

Inoltre, nella valutazione dell'elemento soggettivo, il giudice potrebbe considerare l'effettivo dell'adeguamento agli obblighi imposti a chi effettua negoziazione algoritmica dai regolamenti sopra citati e dal t.u.f. volti a prevenire che i sistemi di negoziazione algoritmica vengano utilizzati per scopi vietati, fra cui la

---

[495] Strumento interpretativo e non integrativo della fattispecie penale, come sottolineato da F. CONSULICH, *Manipolazione dei mercati e diritto eurounitario*, in Le Società, 2016, fasc. 2, p. 211.

[496] Un esempio di applicazioni di intelligenza artificiale in grado di segnalare potenziali abusi è descritto in A. RAVAGNANI–F. LILLO–P. DERIU–P. MAZZARISI–F. MEDDA–A. RUSSO, *Dimensionality reduction techniques to support insider trading detection*, in Consob. Quaderni FinTech, 12 febbraio 2024.

Si tratta di una metodologia basata su tecniche di apprendimento automatico non supervisionato (algoritmo di *clustering k-means* e reti di co-occorenza validate statisticamente), capace di fornire un'indicazione sulla presenza o meno di anomalie nel comportamento di *trading* e che supporta i processi di monitoraggio e sorveglianza da parte dell'Autorità competente e la valutazione della condotta. In particolare, il sistema è in grado di individuare – tramite *clustering* dinamico – comportamenti sospetti legati a un evento *price sensitive*. I comportamenti sono considerati sospetti qualora si rilevi una discontinuità nell'attività di *trading* sia rispetto all'attività normale del medesimo investitore sia rispetto all'attività degli altri investitori che svolgono attività simili.

Azioni analoghe sono state intraprese anche in altri Paesi.

Ad ottobre 2024, l'Autorità di vigilanza sui mercati olandese (Dutch Authority for the Financial Markets, AFM) ha annunciato una collaborazione con l'Università di Oxford per lo sviluppo di modelli *data-driven* per identificare gli abusi di mercato posti in essere tramite algoritmi (in particolare i casi di collusione da parte dei *market-maker*) https://www.bloomberg.com/news/articles/2024-10-29/dutch-regulator-seeks-better-algo-testing-to-avert-market-abuse?srnd=homepage-canada&embedded-checkout=true.

Analogamente, l'autorità di vigilanza sui mercati finanziari francese (Autorité des Marchés Financiers, AMF), ha sviluppato la piattaforma ICY per il monitoraggio dell'attività di *trading* e l'individuazione degli abusi di mercato, basata sui *Big Data*; così come hanno fatto l'Autorità Federale di Vigilanza Finanziaria tedesca (BaFin) con il sistema automatizzato di allerta e monitoraggio del mercato "ALMA" e la SEC negli Stati Uniti con il *Market Information Data Analytics System* (MIDAS), che analizza dati di *trading* da tutti i mercati azionari statunitensi e identifica anomalie.

commissione di abusi di mercato[497]. Ci si riferisce in particolare ai doveri di verifica dei sistemi precedenti alla loro installazione e al rilascio[498], agli obblighi successivi all'installazione (fra cui l'adozione di un sistema di controllo e sorveglianza che monitori ordini e operazioni[499]), oltre che agli obblighi di notifica e comunicazione alla Consob[500].

Lo stesso vale per la capacità della persona che compie operazioni o inoltra ordini di compravendita potenzialmente abusivi di dimostrare che le motivazioni alla base di tali operazioni o tali ordini fossero legittime e conformi alle prassi ammesse sul mercato.

Si tratta di elementi che possono essere utilizzati dal giudice nell'accertamento dell'atteggiamento psicologico dell'agente, ma nei quali non può evidentemente esaurirsi la dimostrazione della sussistenza del dolo, onde evitare di trasformarlo in un criterio di imputazione normativa[501].

7.2. Gli 'abusi di mercato algoritmici' tradizionali: il secondo scenario

Si possono poi ricondurre alle ipotesi di 'abuso di mercato algoritmico' commesso tramite sistemi di *trading* algoritmico 'tradizionale' anche altre ipotesi. Primo caso:

> *Viene sviluppato un algoritmo di* market making*, il cui scopo è fornire liquidità al mercato comprando e vendendo titoli con margini molto stretti, guadagnando sulla differenza tra il prezzo di acquisto e quello di vendita. L'algoritmo è progettato per adattare i propri ordini di acquisto e vendita in base alle variazioni di prezzo del mercato, ma non è stato programmato per evitare*

---

[497] In particolare, le previsioni di cui all'art. 67 *ter* t.u.f., del Regolamento Delegato UE 2017/589 e del Regolamento Mercati Consob.

[498] Artt. 5 e 7 Regolamento Delegato UE 2017/589, nonché art. 67 *ter*, primo comma, t.u.f..

[499] Sistemi che, oltre a garantire la resilienza dei propri sistemi e a impedire l'invio di ordini che rechino pregiudizio ai mercati, devono evitare che gli algoritmi siano utilizzati per finalità contrarie al Regolamento MAR (artt. 67 *ter*, primo comma, t.u.f. e art. 13 Regolamento Delegato UE 2017/589).

[500] Articolo 67 *ter*, secondo e terzo comma, t.u.f. (che recepisce l'articolo 17, par. 2, MiFID II)

[501] Sulle critiche alla tendenza (giurisprudenziale) al "depauperamento dell'ossatura costitutiva del dolo" da criterio che affonda le radici nella dimensione naturalistica a dimensione tipologica, in virtù di un improprio processo di oggettivizzazione si veda C. PIERGALLINI, *Danno da prodotto*, *op. cit.*, pp. 401-402.

di immettere ordini in modo eccessivo quando rileva fluttuazioni temporanee.

Per massimizzare la sua efficienza, l'algoritmo è impostato per reagire rapidamente a piccole variazioni di prezzo con una quantità elevata di ordini, senza che i programmatori abbiano considerato il rischio di influenzare il mercato.

Tuttavia, quando l'algoritmo rileva che le condizioni di mercato stanno cambiando e che l'operazione potrebbe non risultare redditizia, cancella gli ordini prima che vengano eseguiti. Questa pratica di immettere ordini rapidamente e cancellarli prima dell'esecuzione crea un'apparenza artificiale di domanda o offerta, inducendo altri operatori a reagire a queste fluttuazioni apparenti.

Di conseguenza, anche una piccola oscillazione nei prezzi viene amplificata dall'algoritmo, che genera un grande volume di ordini di acquisto o vendita e, cancellandoli immediatamente, crea una pressione artificiale sui prezzi. Gli altri operatori, vedendo un forte movimento di ordini, vengono indotti a modificare i propri comportamenti di trading*, aggravando ulteriormente l'oscillazione del mercato*[502]*.*

Secondo caso:

Un algoritmo di trading *viene programmato per evitare comportamenti esplicitamente proibiti, come il* pump and dump *(modificazione dei prezzi attraverso un rapido aumento della domanda e successiva vendita massiccia di un titolo), ma non prevede misure di prevenzione per altre pratiche altrettanto problematiche, come il* quote stuffing *(invio di grandi quantità di ordini non destinati all'esecuzione, per sovraccaricare il sistema di trading e ritardare la gestione degli ordini legittimi).*

---

[502] Ipotesi analoga è quella di un algoritmo di *high-frequency trading* che consente di eseguire un elevato numero di ordini al secondo. Durante la fase di sviluppo, non viene implementato alcun sistema per impedire comportamenti che potrebbero provocare una manipolazione dei prezzi o 'gonfiare' artificialmente i volumi di scambio**.** L'algoritmo inizia a piazzare ordini di acquisto e vendita che vengono immediatamente cancellati (c.d. *order spoofing*). Questo comportamento, anche se non intenzionalmente programmato per manipolare il mercato, provoca una falsa percezione di domanda e offerta, distorcendo i prezzi dei titoli.

> *L'algoritmo, per massimizzare i profitti, inizia a generare enormi volumi di ordini che non intende realmente eseguire e che infatti che vengono immediatamente cancellati, provocando un rallentamento nel sistema di gestione degli ordini e ostacolando la capacità degli altri trader di negoziare in modo efficiente. Anche se il gestore aveva previsto misure per prevenire certe forme di manipolazione, il* quote stuffing *non era stato contemplato. Di conseguenza, il mercato subisce una distorsione che favorisce chi utilizza questo algoritmo, causando una manipolazione indiretta.*

In queste ipotesi, a differenza della prima illustrata, il sistema di negoziazione algoritmica non è stato programmato appositamente per porre in essere una strategia illecita.

Diversamente, l'abuso di mercato è il risultato di una programmazione che, pur essendo non volta ad agevolare condotte illecite, consente comunque di porre in essere strategie riconducibili alla fattispecie astratta dal punto di vista oggettivo.

Gli algoritmi di *trading* non vengono, cioè, utilizzati al solo scopo di commettere il reato.

Nel primo esempio la quantità elevata di ordini inseriti e poi cancellati crea una falsa impressione di liquidità e movimento di mercato, distorcendo il prezzo dei titoli.

L'algoritmo ha agito senza che gli fosse stata fornita alcuna istruzione volta a evitare il realizzarsi di comportamenti che potessero ricadere nel divieto di manipolazione del mercato.

Nel secondo esempio, invece, in sede di programmazione sono state proibite alcune condotte manipolative, ma tale divieto non è stato esteso ad alte pratiche potenzialmente abusive. La programmazione è solo parzialmente adeguata rispetto alla possibile condotta illecita.

In entrambi i casi, il comportamento posto in essere pare riconducibile, per quanto riguarda l'elemento oggettivo, alla fattispecie di manipolazione del mercato.

Si tratta di comportamenti che, come quelli descritti nel primo scenario, ricadono nell'ambito di applicazione delle disposizioni del t.u.f. e del Regolamento MAR. Si richiamano dunque tutte le considerazioni sin qui svolte in merito.

Ciò posto, anche in questo scenario, l'indagine sulla rilevanza penale dei comportamenti illustrati e sull'adeguatezza dell'attuale sistema di contrasto agli

abusi di mercato impone di concentrarsi sull'analisi dell'elemento soggettivo di chi fa uso del sistema di negoziazione algoritmica.

Diversamente dall'ipotesi in cui l'algoritmo viene usato deliberatamente allo scopo di commettere il reato, sfruttandone le potenzialità, in questo caso chi utilizza l'algoritmo di *trading* non agisce allo scopo precipuo di realizzare il fatto di reato. Si tratta dunque di indagare quale sia l'atteggiamento psicologico che supporta la condotta: volontario o negligente.

Verosimilmente, gli ultimi esempi non si conciliano con l'intensità massima della volontà, ma non escludono né la previsione dell'illecito, né la sua volizione.

Anzi, la previsione è un presupposto necessario perché i comportamenti possano essere qualificati come illeciti penali[503].

È dunque innanzitutto necessario accertare che, in sede di programmazione, fosse prevedibile che l'algoritmo potesse porre in essere una condotta rientrante nel divieto di manipolazione del mercato ed escludere che *l'output* prodotto dall'algoritmo non rientri nella sfera dell'imprevedibilità.

Perciò, l'oggetto dell'accertamento deve essere l'effettiva rappresentazione e volizione non solo delle modalità con cui opera dell'algoritmo[504], ma anche di quali fra le strategie che l'algoritmo è in grado di realizzare siano potenzialmente manipolatorie.

Anche in questo caso la valutazione può essere fatta sulla base del Regolamento MAR e degli indicatori di manipolazione[505]. Ma soprattutto, è in questo caso necessario valutare se chi ha utilizzato l'algoritmo lo abbia fatto adeguandosi o meno alle norme regolamentari che regolano l'utilizzo dei sistemi di negoziazione algoritmica, fra cui gli obblighi pre-immissione dei sistemi, gli obblighi di controllo successivi all'immissione stessa e ai doveri di comunicazione alla Consob[506].

---

[503] Qualora non si dimostrasse la sussistenza del dolo, ma piuttosto della colpa, l'illecito avrebbe natura amministrativa.

[504] Poiché, come si è detto, gli algoritmi di *trading* possono operare in vari modi, tra cui l'esecuzione automatica di ordini, l'arbitraggio, il *market making* e le altre strategie di *trading* citate. Ogni algoritmo ha una logica di programmazione unica, che determina come reagisce a specifiche condizioni di mercato. Pertanto, è necessario che siano comprensibili non solo le potenzialità dell'algoritmo, ma anche come le sue azioni possano influenzare il mercato e gli altri operatori.

[505] L'approccio casistico del legislatore europeo può quindi essere sfruttato in sede di programmazione dell'algoritmo, per 'addestrarlo' a non incorrere nelle ipotesi ivi contenute e consente anche di condurre il giudizio di prevedibilità.

[506] Ci si riferisce alle sopra citate norme del Regolamento Delegato UE 2017/584 e del Regolamento Mercati, nonché alle disposizioni dell'art. 67 *ter* t.u.f. Il tutto, evidentemente, previa la verifica del fatto che, ove si fossero rispettati i canoni imposi da tali regole fossero capaci di evitare che l'algoritmo ponesse in essere strategie abusive.

Evidentemente, l'esito positivo di questa verifica non sarebbe sufficiente a muovere un rimprovero doloso a chi ha utilizzato l'algoritmo, pena un'indebita 'normativizzazione' del dolo. Viceversa, come già anticipato, tali elementi devono contribuire all'accertamento della componente naturalistico-psicologico propria del dolo e quindi devono essere valutate insieme all'effettiva adesione soggettiva dell'agente all'abuso di mercato[507].

Solo in questo caso, il giudice potrà muovere un rimprovero doloso – anche nella forma eventuale[508] – a chi, servendosi dell'algoritmo, ha posto in essere il fatto riconducibile alla fattispecie incriminatrice.

Tornando dunque agli esempi, nel primo caso l'algoritmo di *market making* è stato progettato per reagire rapidamente alle fluttuazioni di prezzo, senza considerare il potenziale impatto di ordini eccessivi sul mercato e delle immediate cancellazioni.

Qualora si dimostrasse che in sede di programmazione fosse stata prevista la possibilità che il sistema potesse distorcere i prezzi e avessero comunque deciso di procedere senza prendere alcuna contromisura volta ad evitare detta distorsione – e dunque l'abuso di mercato sia stato voluto –, si configurerebbe un atteggiamento doloso.

Nel secondo esempio, l'algoritmo è stato programmato per evitare pratiche come il *pump and dump*, ma non il *quote stuffing*. Se i programmatori, pur rappresentandosi il rischio che quest'ultima strategia abusiva venisse posta in essere, avessero scelto di non inserire nel codice di programmazione misure volte a prevenirlo, anche in questo caso si potrebbe ritenere integrato l'elemento soggettivo del dolo.

Ciò non implica, si badi, che ove non vi fosse la prova della rappresentazione e volizione da parte di chi ha utilizzato l'algoritmo di *trading*, il comportamento – pur oggettivamente riconducibile alle fattispecie che sanzionano gli abusi di mercato – andrebbe impunito.

Come noto, mentre la rilevanza penale delle condotte è limitata a quelle supportate da rappresentazione e volizione, stante l'assenza di una espressa punibilità per colpa, al contrario gli illeciti amministrativi sono punibili anche se

---

[507] La verifica deve, come è evidente, avere ad oggetto il fatto per come si è in effetti verificato e non la generica capacità dell'algoritmo di porre in essere una qualsiasi strategia abusiva.

[508] Sulle specifiche problematiche connesse all'accertamento del dolo eventuale si rinvia al par 8. I sistemi di *negoziazione* algoritmica basati su sistemi di intelligenza artificiale 'forte', *infra*.

commessi in forma colposa. È dunque in questo ambito che si può collocare il rimprovero, ai sensi degli artt. 187 *bis* e 187 *ter* t.u.f.[509].
Si tratta, peraltro, di un'ipotesi tutt'altro che teorica, dal momento che "rispecchia quanto accaduto nella maggior parte dei *flash crash*"[510] compreso il caso del 2012 che ha coinvolto Knight Capital e che ha dato innesco ai primi interventi del legislatore europeo in materia di *trading* algoritmico.
Nella valutazione della responsabilità colposa, occorrerà in particolare accertare se l'agente si sia adeguato o meno alle regole governano l'esercizio dell'attività di negoziazione algoritmica[511].

In definitiva, anche alla luce di questi ultimi esempi, si può affermare che, qualora l'abuso di mercato sia commesso attraverso algoritmi di *trading* tradizionali che agiscono materialmente sui mercati come strumento dell'agire umano, non si prospetta un vuoto di tutela da parte dell'ordinamento[512].
Quando cioè l'algoritmo è un mero strumento nelle mani dell'uomo, l'intervento della 'macchina' non influisce sulla possibilità di muovere un rimprovero penale a chi programma o utilizza tale strumento[513], purché venga provato che vi sia stata una rappresentazione e accettazione della realizzazione dell'illecito per come concretamente verificatosi nel caso concreto.

---

[509] Rimprovero che secondo la giurisprudenza non sarebbe sottoposto al medesimo onore probatorio applicabile all'illecito penale. Cfr. Cass. Pen, Sez. V, 9 gennaio 2020, n. 397, "il giudizio di colpevolezza è ancorato a parametri normativi estranei al dato puramente psicologico, limitando l'indagine all'accertamento della 'suità' della condotta inosservante, con la conseguenza che, una volta integrata e provata all'autorità amministrativa la fattispecie tipica dell'illecito, grava sul trasgressore, in virtù della presunzione di colpa posta dall'art. 3 della l. 24 novembre 1981, n. 689, l'onere di provare di aver agito in assenza di colpevolezza". Nello stesso senso, Cass. Pen., Sez. V. 31 ottobre 2018, n. 49869. L'argomento della giurisprudenza è respinto da S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., p. 94.

[510] F. ANNUNZIATA, *Intelligenza artificiale*, *op. cit.*, p. 18.

[511] Con riferimento ai casi in cui l'algoritmo è un mero strumento nelle mani dell'essere umano, F. CONSULICH, Flash offenders, *op. cit.*, pp. 1034-1035 rileva come qualora l'uomo "determinasse solo il *genus* del reato, senza definire il *tempus* e il *modus* dell'illecito, non vi sarebbe modo di configurare una responsabilità dolosa a suo carico" mentre l'imputazione colposa, "che non si focalizza mai su una rappresentazione anticipata dell'evento *singulatim*, ma sulla riconduzione dell'evento *hic et nunc* ad una classe di *avvenimenti avversi*" prometterebbe risultati migliori.

[512] Come rileva F. CONSULICH, Flash Offenders, *op. cit.*, p. 1034, "per quanto peculiare e sofisticato, l'AI rimane uno mero 'utensile'". Di fronte a questa condizione, l'Autore ipotizza il conio del concetto – che definisce "critico" – "di *imputazione mediata* per indicare tutti i casi in cui lo strumento abbia una propria parte di autonomia nel concretizzare il progetto illecito dell'unico soggetto perseguibile, la persona finisca che se ne avvalga".

[513] Cfr. F. CONSULICH–M. MAUGERI–C. MILIA–T.N. POLI–G. TROVATORE, *AI e abusi di mercato*, *op. cit.*, p. 28.

La prova della sussistenza del dolo richiede, cioè, particolare rigore, soprattutto riguardo alla consapevolezza e la volontà da parte dei programmatori e degli operatori sul potenziale impatto dell'algoritmo[514].

8. I sistemi di negoziazione algoritmica basati su sistemi di intelligenza artificiale 'forte'

Chiarito che l'utilizzo gli algoritmi di *trading* tradizionali o basati su sistemi di intelligenza artificiale 'debole' non pone particolari problemi in termini di efficacia di tutela perché le condotte poste in essere tramite quelli che devono essere considerati meri strumenti sono pacificamente riconducibili alle fattispecie penali – qualora i comportamenti siano dolosi – o amministrative – in caso di atteggiamento colposo –, si tratta ora di comprendere se valga altrettanto quando il sistema di negoziazione algoritmica si basi su intelligenza artificiale 'forte'.
Per quanto l'azione degli algoritmi basati su *reinforcement learning* (e ancor più *deep reinforcement learning*) sia, allo stato attuale, ampiamente ancorata all'essere umano per cui agiscono e ai suoi interessi[515], una disamina completa delle applicazioni di intelligenza artificiale al *trading* e conseguenti rischi penali da questa derivante non può prescindere dall'analisi dell'ipotesi in cui la 'macchina' commetta 'da sola' un abuso di mercato.

---

[514] Sul punto occorre rilevare che la dottrina americana, rispetto alla normativa anti *spoofing* – del Dodd-Frank Act 7 U.S.C. § 6c(a)(5)(c)) – che impone di verificare che il soggetto abbia inviato l'ordine con l'intenzione di cancellarlo prima di eseguirlo ("*the intent to cancel the bid or offer before execution*"), sostiene l'estrema difficoltà di dimostrare in questi casi l'"*intent*". G. SCOPINO, D*o Automated Trading Systems Dream of Manipulating the Price of Futures Contracts? Policing Markets for Improper Trading Practices by Algorithmic Robots*, in Florida Law Review, 2015, vol. 67, issue 1, p. 233., nonché T.C.W. LIN, *The New Market Manipulation*, *op. cit.*, p. 1301 e A. AZZUTTI–W.G.RINGE–H.S. STIEHL, *Machine Learning, Market Manipulation*, *op. cit*., pp. 116-122.

[515] A. AZZUTTI– W.G.RINGE–H.S. STIEHL, *Machine Learning, Market Manipulation*, *op. cit.*, p. 101 secondo cui persiste una mancanza di evidenze univoche riguardo alla capacità dei *trader* AI autonomi di compiere una manipolazione di mercato senza che vengano esplicitamente programmati o istruiti a farlo da esseri umani (Traduzione nostra); Più in generale, C. PIERGALLINI, *Intelligenza artificiale*, *op. cit.*, p. 1748 "i sistemi di IA prevalentemente in uso paiono non rinunciare al controllo umano, sì da atteggiarsi come meri strumenti di altri attori, dei quali costituirebbero, pertanto, un prolungamento"; nonché B. FRAGASSO, *Intelligenza artificiale e crisi*, *op. cit.*, p. 289, secondo cui i sistemi di *deep learning* non sono propriamente 'agenti' nel senso kantiano del termine "poiché le 'finalità' delle loro azioni parrebbero pur sempre etero-definite", sebbene non siano nemmeno strumenti pienamente dominabili dall'uomo perché non reagiscono in modo deterministico agli *input* di quest'ultimo. Nello stesso senso, di recente, F. CONSULICH*, Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit*., par. 1.

La questione, in termini sintetici, è se sia possibile – e in quale modo – sanzionare, con gli strumenti attualmente disponibili, l'abuso di mercato commesso 'da' o 'tramite' sistemi di negoziazione algoritmici basati su intelligenza artificiale 'forte', non del tutto governabili dall'uomo.

8.1. I sistemi di intelligenza artificiale forte e la crisi delle categorie tradizionali del diritto penale

Il problema della tenuta delle categorie tradizionali con riferimento all'operare di sistemi di intelligenza artificiale dotati di un certo grado di autonomia si pone, oltre che con riferimento agli investimenti finanziari, anche in altri importanti settori dell'agire umano[516].

Come anticipato, di fronte alla prospettiva di un progresso tecnologico tanto dirompente da far ipotizzare che le macchine delinquano 'da sole', si farebbe sempre più pressante il rischio di un vuoto di tutela rispetto ad offese non attribuibili né al programmatore o utilizzatore umano, né alla macchina stessa[517]. Si suppone cioè che l'utilizzo di tali sistemi crei rischi ignoti, di cui non si può del tutto dimostrare la portata.

In dottrina, si è infatti affermato a più riprese che alcune delle caratteristiche tipiche dei sistemi di intelligenza artificiale 'forte' – quali l'autonomia, la scarsa comprensibilità del loro agire, oltre che la loro capacità di interagire con altri sistemi dotati degli stessi attributi[518] – comporterebbero una crisi dei tradizionali criteri ascrittivi del fatto illecito[519].

---

[516] Sul punto, si vedano, per tutti, L. PICOTTI, *Categorie tradizionali del diritto penale*, *op. cit.*, p. 8; nonché L. PICOTTI, *Resolution on traditional criminal law categories and AI*, in L. Picotti-B. Panattoni (a cura di), Traditional Criminal Law Categories and AI: Crisis or Palingenesis?, in Revue Internationale de Droit Penal, Vol. 94, Issue 1/2023 e B. FRAGASSO, *Intelligenza artificiale e crisi*, *op. cit.*, *passim*.

[517] Essendo stata già esclusa la praticabilità di una responsabilità diretta della macchina. Cfr. A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, p. 516, nonché S. BECK, *Intelligent agents and criminal law*, *op. cit.*, pp. 138-143.

[518] Cfr. B. FRAGASSO, *Intelligenza artificiale e crisi*, *op. cit.*, p. 288 secondo cui l'intelligenza artificiale aprirebbe un "nuovo capitolo del rapporto tormentato tra tecnologia e *agency* umana", specie alla luce dell'imprevedibilità dei sistemi che, in questa nuova prospettiva, non costituirebbe più un difetto, ma un risultato voluto per raggiungere risultati più performanti.

[519] Il tema è oggetto di approfondito studio da parte della dottrina italiana a cui si rinvia, senza pretesa di esaustività: F. BASILE, *Intelligenza artificiale e diritto penale*, *op. cit.*, pp. 1-33; F. CONSULICH, Flash offenders, *op. cit.,* pp. 1051-1055 e *passim*; P. SEVERINO, *Intelligenza artificiale e diritto penale*, in U. Ruffolo (a cura di), Intelligenza artificiale. Il diritto, i diritti, l'etica, Milano, Giuffrè, 2020, pp. 531-545; R. BORSARI, *Intelligenza artificiale e responsabilità penale*, *op. cit.*, pp. 262-268; SALVADORI, *Agenti artificiali, opacità tecnologica*, *op. cit.*, pp. 262-268; A. FIORELLA,

La questione è stata affrontata, come si è già anticipato, in particolare per le automobili a guida autonoma, i *robot* chirurgici, i droni ad uso militare e i *social bot*[520].

Rispetto a tali applicazioni di intelligenza artificiale, si è frequentemente sottolineato che il sistema agirebbe in modo imponderabile, interponendosi tra la condotta del produttore e l'evento lesivo e potendo così mettere in discussione l'integrazione degli elementi del reato[521].

Tale fenomeno deriverebbe dall'impossibilità di ricostruire il meccanismo tramite cui dato un *input* si produca un determinato *output*, a causa dell'intrinseca opacità e imprevedibilità (c.d. *black box*) dei sistemi di intelligenza artificiale 'forte'. L'intelligenza artificiale 'forte' sarebbe cioè in grado di tenere "comportamenti attivi assolutamente imprevedibili, derivanti dal lavorio autoevolutivo del *machine learning*, tali che qualunque danno da essi derivante sfugga inesorabilmente alle capacità previsionali dei programmatori"[522].

Così, si prospetterebbe una vera e propria crisi del diritto penale d'evento, direttamente dipendente dall'opacità e dall'autonomia di tali sistemi.

Tale crisi si rivelerebbe in particolare con riferimento ai rimproveri colposi e, più nel dettaglio, rispetto alla verifica della sussistenza del nesso eziologico tra

---

Responsabilità penale dei Tutor *e dominabilità dell'Intelligenza Artificiale. Rischio permesso e limiti di autonomia dell'Intelligenza Artificiale*, in R. Giordano–A. Panzarola–A. Police–S. Preziosi–M. (a cura di), Il diritto nell'era digitale. *Persona, mercato, amministrazione, giustizia*, Milano, Giuffrè, 2022, p. 657; A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit*., pp. 516-520; B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, in Dir. inf., 2021, fasc. 1, pp. 317-368; 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., 2022, fasc. 9, pp. 3287-3304; M.B. MAGRO, Decisione umana, *op. cit.*, pp. 1-22; L. PICOTTI, *Categorie tradizionali del diritto penale*, *op. cit.*, pp. 1-20.

[520] Più recentemente R. COMPOSTELLA, *Auto a guida autonoma e diritto penale*, *op. cit.*; M. E. FLORIO, *Il dibattito sulla responsabilità penale, op. cit.* p. 1 e B. FRAGASSO, *Intelligenza artificiale e crisi*, *op. cit.*, p. 291, N. AMORE, *L'effetto della robotica, op. cit.*, pp. 101-246; M. LANZI, Self driving cars *e responsabilità penale. La gestione del "rischio stradale" nell'era dell'intelligenza artificiale*, Torino, Giappichelli, 2023, pp. 91-181; nonché gli Autori già citati nella nota precedente e, in particolare, BASILE, *Intelligenza artificiale e diritto penale*, *op. cit.*, 1-33.; F. CONSULICH, Flash offenders*, op. cit.*, 1015-1055; M.B. MAGRO, *Decisione umana*, *op. cit.,* pp.1-22; C. PIERGALLINI, *Intelligenza artificiale*, *op. cit.*, p. 1746-1747; A. FIORELLA, *Responsabilità penale dei* Tutor, *op. cit.*, *passim*; B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale*, *op. cit.*, pp. 317-368; M. CALDWELL– J.T.A. ANDREWS–T. TANAY–L.D. GRIFFIN, *AI enabled future crime*, *op. cit.*, pp. 1-13.

[521] Cfr. B. FRAGASSO, *Intelligenza artificiale e crisi*, *op. cit.*, pp. 291-292 e i riportati esempi riferiti ai c.d. *Clinical Decision Support Systems* (CDSS) e ai sistemi di i.a. generativa. Si veda sul punto anche F. CONSULICH, Flash offenders, *op. cit.*, pp. 1036 ss.

[522] A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, p. 507.

condotta umana ed evento lesivo, posta l'indisponibilità di un "corredo nomologico che consenta di *spiegare* il comportamento dei sistemi di i.a."[523]. Mancherebbero, cioè, le leggi scientifiche di copertura sulla base delle quali svolgere l'accertamento causale.
A ciò si aggiungerebbe la difficoltà di accertare le due componenti del nesso fra colpa ed evento: la concretizzazione del rischio fra regola cautelare violata ed evento lesivo e l'efficacia impeditiva della condotta alternativa doverosa.
L'imprevedibilità e l'opacità dei sistemi in questione impedirebbero di stabilire con la dovuta certezza se in effetti l'evento lesivo verificatosi sia la concretizzazione del rischio che la norma cautelare violata mirava ad evitare; ma soprattutto non sarebbe possibile stabilire in modo rigoroso se l'evento lesivo si sarebbe verificato o meno in caso di comportamento fedele a quanto imponeva la regola cautelare.

8.2. La crisi del diritto penale d'evento e le specificità degli 'abusi di mercato algoritmici'

Orbene, se i rilievi sopra illustrati sono certamente suggestivi per le tipologie di reato rispetto alle quali in dottrina ci si è maggiormente soffermati (ad esempio l'omicidio e le lesioni nell'ambito della circolazione di automobili a guida autonoma), occorre tuttavia rilevare come essi abbiano delle significative differenze con le fattispecie *market abuse*, oggetto del presente lavoro.
Tali differenze valgono ad escludere che per gli illeciti in questione si pongano i medesimi problemi prospettati dalla dottrina per un duplice ordine di ragioni.
In primo luogo, lo scoglio insuperabile di fronte al quale si manifesterebbe la principale ragione di crisi del diritto penale di fronte ai sistemi di intelligenza artificiale è l'impossibilità di accertare il nesso colpa ed evento.
Ebbene, gli abusi di mercato sono concepiti dal legislatore come illeciti in cui il fatto si esaurisce nel compimento dell'azione stessa[524]. Come tali, non è richiesto che dall'azione derivi un accadimento temporalmente o spazialmente

[523] Così B. FRAGASSO, *Intelligenza artificiale e crisi*, *op. cit.*, p. 299.

[524] Limitandosi alla manualistica, si vedano G. MARINUCCI – E. DOLCINI – G. L. GATTA, *Manuale di diritto penale*, *op. cit.*, p. 306 nonché G. FIANDACA–E. MUSCO, *Diritto penale*, *op. cit.*, pp. 215, i quali (p. 241) sottolineano come "nell'ambito dei reati di mera condotta, definiti tali perché privi di un evento c.d. naturalistico, a rigore non è necessario ipotizzare un evento giuridico come risultato che consegue o si aggiunge alla condotta medesima".

separato[525]. Tanto potrebbe bastare ad affermare che in questo ambito non si ripropongono i problemi di accertamento poc'anzi illustrati.

A questa conclusione, con specifico riferimento alla fattispecie di manipolazione del mercato, si potrebbe obiettare che in realtà vi sarebbe un evento che il giudice deve accertare: l'evento di pericolo concreto che tradizionalmente si rinviene nel riferimento all'idoneità alterativa della condotta operato dall'art. 185 t.u.f.[526]. Tanto che, in sede processuale, la sensibile alterazione dei prezzi costituisce base probatoria dell'indagine e financo "banco di prova della effettiva natura manipolatoria della transazione posta in essere, quale parametro attraverso cui accertare la concreta pericolosità della condotta" [527] e dunque, in definitiva, la sua rilevanza penale.

---

[525] Come nota F. MUCCIARELLI, *Materialità e offensività dell'alterazione*, *op. cit.*, p. 27 "vertendosi in tema di reati di pericolo, l'assenza di un evento implica che l'apprezzamento della causalità dovrà essere compiuto ed espresso in termini di potenzialità/probabilità causale". Sulla "disputa sul concetto di evento" in senso giuridico e in senso naturalistico e sulla necessità che il giudice, anche per i reati di mera condotta, dovrebbe ulteriormente verificare l'effettivo impatto della condotta sul bene giuridico protetto dalla norma, limitandosi anche in questo caso alla manualistica, si rinvia, senza pretesa di esclusività alcuna a G. FIANDACA–E. MUSCO, *Diritto penale*, *op. cit.*, pp. 239-242.

[526] Ossia l'attitudine della situazione di fatto verificatasi a produrre un evento dannoso. Cfr. G. FIANDACA–E. MUSCO, *Diritto penale*, *op. cit.*, p. 240 "l'evento di pericolo è configurabile soltanto nell'ambito delle figure di reato [..] a pericolo concreto, nelle quali spetta al giudice accertare se una effettiva situazione di pericolo si è verificata come conseguenza dell'azione".

[527] Così MAGRO, *Manipolazioni dei mercati*, *op. cit*., p. 260, che sottolinea come l'evento di danno patrimoniale costituito dall'effettiva alterazione dei prezzi non è elemento necessario ai fini della sussistenza della fattispecie.

Si evidenzia, inoltre, che stante la natura di reato di pericolo concreto e di mera condotta, il giudizio sull'effettiva pericolosità della manipolazione dovrebbe consistere in una prognosi *ex ante* e basarsi esclusivamente la congiuntura del mercato nel momento in cui si è svolta l'azione, senza tener conto delle reazioni del mercato conseguenti. Tuttavia, la dottrina sottolinea come l'assenza di certezze da parte delle scienze economiche nella spiegazione dei comportamenti del mercato finisco, di fatto, di attribuire rilevanza anche ad elementi successivi alla condotta (quale la reazione sortita sul mercato). Perciò il giudizio corre il rischio di trasformarsi in giudizio *ex post* su ciò che è in effetti accaduto (se effettivamente si siano rilevati effetti distorsivi o meno). Si tratta di una trasformazione che F. CONSULICH, *Manipolazione del mercato e disorientamenti dogmatici tra eventi di pericolo e pericolo di eventi*, in Le società, 2011, fasc. 7, p. 828 efficacemente sintetizza con la formula: "ciò che per la norma è pericolo, nella realtà empirica è evento". In definitiva, benché la norma tipizzi "un illecito di condotta pericolosa privo di un evento di danno o di pericolo, il processo penale rilegge sempre la disposizione, come nel caso che ha occasionato queste riflessioni, a partire dall'impatto della condotta sulla mercato, cioè dalla presenza o assenza […] di un evento di alterazione del mercato". Sull'effetto "confondente della cd distorsione del giudizio retrospettivo (*hindsight bias*)" e sul fatto "che la valutazione, svolta in una prospettiva *ex ante* ma compiuta *ex post*, sconta comunque la conoscenza di quanto successivamente accaduto", di recente, F. MUCCIARELLI, *Materialità e offensività dell'alterazione*, *op. cit.*, pp. 22-23.

Ma anche aderendo a questa impostazione, non pare superabile il secondo ostacolo, che peraltro riguarda sia la fattispecie di manipolazione del mercato, che quella di abuso di informazioni privilegiate.

L'accertamento del duplice nesso fra colpa ed evento – e le problematiche connesse – riguarda, come è evidente, esclusivamente i reati colposi.

Tuttavia, sia la manipolazione del mercato, sia l'abuso di informazioni privilegiate sono punite penalmente solo se commesse con dolo. La forma colposa è presidiata, invece, secondo l'interpretazione più convincente, solo dalla sanzione amministrativa[528]. Le formulazioni delle fattispecie amministrative, però, difettano del presupposto a cui ancorare la possibilità di operare la verifica del nesso in questione, ossia l'evento, ancorché inteso come evento di pericolo. Infatti, anche se l'evento "può consistere anche in un risultato esteriore che concretizza non già la effettiva lesione, ma la messa in pericolo di un bene protetto"[529], tale evento (di pericolo) è configurabile soltanto per le fattispecie di pericolo concreto. Ma per gli illeciti amministrativi, secondo l'interpretazione più convincente, è il legislatore ad aver stabilito *ex ante* la pericolosità del compimento di determinate condotte[530] e dunque il giudizio può arrestarsi alla prova della potenzialità alterativa delle medesime.

Non sarebbe dunque necessario, per le fattispecie amministrative, l'accertamento del nesso colpa-evento.

Ciò significa che i problemi sollevati dalla dottrina con riferimento alle altre ipotesi di applicazioni di intelligenza artificiale 'forte' non si possono riprodurre negli stessi termini per le fattispecie oggetto del presente lavoro, rispetto alle quali è necessario svolgere considerazioni – quantomeno su alcuni aspetti – differenti[531].

---

[528] Sulle diverse interpretazioni, vedi 3.3. L'illecito amministrativo, nonché 3.5. L'illecito amministrativo

[529] G. FIANDACA–E. MUSCO, *Diritto penale*, *op. cit.*, p. 240.

[530] Come nota F. D'ALESSANDRO, *L'aggiotaggio e la manipolazione del mercato*, in *L'aggiotaggio e la manipolazione del mercato*, in G. Canzio–L. Cerqua–L. Luparia, Diritto penale delle società. Accertamento delle responsabilità individuali e processo alla persona giuridica, Padova, Cedam, 2016, p. 763, in questo si sostanzia la "linea di demarcazione in grado di distinguere le condotte aventi rilevanza penale da quelle punibili a livello amministrativa".
Sulla compatibilità con il principio di offensività dei reati di pericolo astratto, per tutti, F. D'ALESSANDRO, Pericolo astratto, *op. cit.*, pp.163-180 e *passim*; nella manualistica, G. MARINUCCI–E. DOLCINI, *Corso di diritto penale*, III ed., Milano, Giuffrè, 2001, p. 563, secondo cui che dietro a uno schema apparentemente imperniato sull'offesa a un bene giuridico, tradiscono in realtà la repressione a mere disobbedienze a un divieto o a un comando legislativo.

[531] Oltre che, per così dire, meno complessi, specie per quanto riguarda la problematica connessa all'accertamento del duplice nesso colpa evento.

Proprio per queste differenze non pare che rispetto al *market abuse* algoritmico si possa affermare il rischio un vuoto di tutela rispetto a condotte offensive che secondo una parte della dottrina porrebbe di fronte all'inaccettabile alternativa fra la rassegnazione all'ineffettività del diritto penale e un suo adattamento che permetta di conservarne la funzione general-preventiva[532].
Al contrario, l'analisi che segue si svilupperà facendo specifico riferimento ai profili di pericolosità legati all'utilizzo degli algoritmi di *trading* basati su sistemi di intelligenza artificiale 'forte', al fine di valutare l'efficacia della risposta apportata dall'attuale sistema.

8.3. Sistemi di intelligenza artificiale 'forte' e gli 'abusi di mercato algoritmici': primo scenario

In primo luogo, è possibile che l'algoritmo di *trading* forte venga utilizzato deliberatamente per commettere un abuso di mercato.
In questo caso, è possibile a riconoscere in capo al soggetto che fa uso dell'algoritmo stesso una piena rappresentazione e volizione dell'illecito, in modo del tutto analogo a quanto accade per i sistemi di negoziazione algoritmica 'tradizionale'.
La centralità della rappresentazione e volizione dell'abuso fa sì che non rilevi tanto l'avanzamento tecnologico del sistema sfruttato o le sue caratteristiche specifiche, ma piuttosto la volontà di usare uno strumento che si sa essere in grado di porre in essere la strategia abusiva.

8.4. Sistemi di intelligenza artificiale 'forte' e gli 'abusi di mercato algoritmici': secondo scenario

È poi possibile immaginare un secondo scenario in cui il soggetto, pur non avendo di mira proprio la realizzazione dell'illecito, sia ad ogni modo consapevole e voglia che l'algoritmo di *trading* 'forte', operando sul mercato, ponga in essere la strategia abusiva.
Questa situazione si verifica qualora il soggetto si renda conto dell'inadeguata programmazione del sistema stesso rispetto alle regole cautelari stabilite dall'ordinamento per l'esercizio dell'attività e lo utilizzi comunque[533].

---

[532] Prospettive illustrate diffusamente da B. FRAGASSO, *Intelligenza artificiale e crisi*, *op. cit*, pp. 300-301 e L. PICOTTI, *Categorie tradizionali del diritto penale*, *op. cit.*, pp. 1-20.

[533] Di fronte a illeciti commessi da sistemi di intelligenza artificiale 'forte' si suole rilevare come sarebbe di ostacolo a un rimprovero penale la non 'spiegabilità' del meccanismo tramite

In questo caso, “la presenza di quella tensione verso il risultato che è la volontà, tipica del dolo, fa prescindere in larga misura dal concreto svolgimento del percorso causale attivato”[534] e quindi anche qualora il sistema utilizzato sia caratterizzato dalla c.d. *black box*, non rileva tanto l’effettiva comprensione del percorso logico seguito dall’algoritmo, ma quanto più il fatto che i tratti assunti in concreto dall’illecito rientrino nella descrizione presente nella mente dell’attore umano[535].

Oggetto del rimprovero è dunque l’aver utilizzato un sistema che si sapeva di non poter controllare, avendo accettato che uno dei risultati di tale mancato controllo fosse la realizzazione di una strategia vietata.

L’ipotesi di un rimprovero doloso non è esclusa dal fatto che si versi in un ambito di un’attività pericolosa consentita dall’ordinamento, nei termini sopra descritti. Si delinea infatti una ipotesi di responsabilità dolosa per il fatto dell’agente che intenzionalmente esercita un’attività – pericolosa ma accettata dall’ordinamento – per ottenere il risultato voluto e che deliberatamente violi le regole fissate dall’ordinamento per l’esercizio lecito dell’attività medesima[536].

---

cui, dato un *input* noto, il sistema abbia determinato un determinato *output*. Questa prospettiva non pare decisiva di fronte ai reati in questione che anticipano la sanzione al compimento della mera condotta e soprattutto considerato che l’oggetto del rimprovero, in questo, è aver utilizzato un sistema foriero di esiti potenzialmente abusivi, accettando che l’algoritmo – non governabile – ponesse in essere l’abuso. Si verserà quindi nell’ipotesi del dolo eventuale, compatibile con entrambe le fattispecie incriminatrici in questione. Cfr. S. SEMINARA, *Diritto penale commerciale*, 2022, *op. cit*., p. 110 e F. D’ALESSANDRO, *La manipolazione del mercato*, *op. cit.*, p. 195 ss.

[534] Così A. CAPPELLINI, Machina delinquere non potest*?, op. cit.*, p. 505 che – seppur con riferimento ai reati di evento – specifica che in questa ipotesi “qualunque deviazione imprevedibile del comportamento della macchina si risolve in una mera *aberratio causae*: la quale, come insegna la migliore dottrina, di norma non fa certo venire meno il doloro rispetto a quel fatto”. Cfr. F. PALAZZO, C*orso di diritto penale*, VII ed., Torino, 2018, pp. 290-291

[535] Ciò significa non arrestare l’analisi alla dimostrazione della mera e generale intenzione di manipolare il mercato in termini astratti, ma valutare la rappresentazione e volizione del fatto in concreto.

[536] Il tema dei rapporti fra rischio consentito e reati dolosi è oggetto di ampio dibattito in dottrina, che vede contrapposte due tesi che possono così sintetizzarsi, senza pretesa di esaustività alcuna e rinviando sul punto ai contribuiti più recenti: S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.*, pp. 386-390; nonché C. PERINI, *Il concetto di rischio*, *op. cit.*, pp. 141-165.

Una, minoritaria, che esclude la compatibilità della categoria in questione con il rimprovero doloso, stante la differenza strutturale fra imputazione dolosa e imputazione colposa (oltre che per scongiurare il rischio di abuso dell’impunità garantita dall’area di rischio consentito): F. GIUNTA, *Illiceità e colpevolezza nella responsabilità colposa*, *op. cit.*, pp. 357 ss; nonché S. CANESTRARI, *Dolo eventuale e colpa cosciente. Ai confini tra dolo e colpa nella struttura delle tipologie delittuose*, Milano, Giuffrè, 1999, pp. 12-16, 90 ss, 184 ss.; ID, *La distinzione tra dolo*

L'esistenza cioè di un'area di rischio tollerata dall'ordinamento lascia impregiudicata la verifica della rappresentazione e volizione del fatto illecito[537]. Proprio l'effettiva sussistenza dell'elemento soggettivo deve essere oggetto di un accertamento rigoroso, onde evitare il rischio – censurato dalla dottrina – di un 'appiattimento' del dolo su valutazioni meramente normative[538]. La prova che chi si è servito di uno strumento non governabile si sia in effetti rappresentato e abbia voluto l'abuso può quindi passare dalla dimostrazione del fatto che il soggetto sapeva che l'algoritmo non era programmato per evitare condotte potenzialmente abusive e che, cosciente di ciò, se ne sia comunque servito[539].

---

eventuale e colpa cosciente nei contesti a rischio di base «consentito», in Dir. Pen. Cont., 6 febbraio 2013, pp. 4-11 e *passim.*

La tesi maggioritaria invece, muovendo dalla considerazione per cui "tra dolo e colpa esiste un rapporto di 'più a meno'" così G. FORTI, *Colpa ed evento*, *op. cit.*, p. 388; che si traduce, nelle parole di Marinucci, nella formula "non c'è dolo senza colpa" Cfr. G. MARINUCCI, *Non c'è dolo senza colpa. Morte dell'"imputazione oggettiva dell'evento" e trasfigurazione nella colpevolezza?*, in Riv. it. dir. proc. pen., 1991, fasc. 1, pp. 3-39 esclude un'incompatibilità strutturale fra il rimprovero doloso e il rischio consentito. "Il superamento del rischio consentito denota una mancata considerazione degli interessi altrui che ben può essere comune sia al dolo che alla colpa", posto che cioè che occorre accertare, indipendentemente dai motivi e delle intenzioni, è se l'ordinamento imponeva di comportarsi diversamente (così G. FORTI, *Colpa ed evento*, *op. cit.*, p. 390 e 388, nt. 80). Non pare infatti decisivo alcun riferimento alla diligenza, che – seppur caratteristico dell'illecito colposo – non è invero assente nel delitto doloso: anzi, "anche l'imputazione dolosa richiede la violazione della diligenza richiesta" (G. FORTI, *Colpa ed evento*, *op. cit.*, pp. 387–388) con la sola differenza che mentre nei delitti colposi il dovere di diligenza è "espressione di quella riconoscibilità del pericolo su cui si basa il rimprovero dell'agente, in quelli dolosi il paramento della riconoscibilità risulta in qualche modo superato e 'mascherato' dall'effettivo coefficiente psicologico ravvisabile in capo all'agente" così G. FORTI, *Colpa ed evento*, *op. cit.*, pp. 386–387. Dolo e colpa hanno dunque in comune la componente oggettiva di violazione della diligenza, "i.e. di superamento del rischio consentito dall'ordinamento. Ove sul piano oggettivo la condotta rimanga nell'ambito del dovere di diligenza e, dunque, del rischio consentito, non si avrà colpa, ma non si avrà nemmeno dolo, dal momento che al soggetto che pure abbia voluto l'evento, non potrà muoversi alcun rimprovero fondato sul dovere di riconoscere la verificazione dell'evento", G. FORTI, *Colpa ed evento*, *op. cit.*, pp. 389–390. In senso favorevole all'applicabilità del limite del rischio consentito ai reati dolosi anche M. DONINI, *Illecito e colpevolezza*, *op. cit.*, pp. 311-312.

[537] Sulla necessità di un puntuale accertamento volitivo in capo all'agente cfr. S. ZIRULIA, Esposizione a sostanze tossiche, *op cit.*. p. 335; nonché S. CANESTRARI, *Dolo eventuale e colpa cosciente*, *op. cit.*, p. 116 che richiama la necessità di evitare il ricorso a "schemi presuntivi di accertamento del dolo" e valorizzare invece "la verifica circa la rappresentazione attuale nella sfera cognitiva dell'agente degli elementi costitutivi del fatto".

[538] Che, come anticipato, nel caso di manipolazione del mercato non richiede la prova dell'idoneità alterativa della condotta, trattandosi di fattispecie di pericolo astratto.

[539] La consapevolezza può essere dedotta anche dal fatto che questi abbia ricevuto dei 'segnali di allarme' in tal senso – quale, ad esempio, il precedente coinvolgimento dell'algoritmo di *trading* nella commissione.

La sussistenza del dolo deve quindi passare per l'accertamento di una presa di posizione volontaristica da parte del soggetto agente all'abuso di mercato, che non può esaurirsi nella mera volizione del turbamento del mercato, ma che deve avere ad oggetto la strategia abusiva che la 'macchina' pone in essere. Come anticipato, essendo questo l'oggetto del dolo, la rappresentazione e volizione possono dirsi integrate anche in assenza di conoscenze specialistiche circa la *modalità tecnica* con cui agisce l'algoritmo (che sarebbe preclusa dalla c.d. *black box*).

Il soggetto, dunque, potrà essere chiamato a rispondere qualora sia accertato che, pur non avendo agito allo scopo di realizzare la strategia abusiva, la abbia prevista come conseguenza dell'immissione dell'algoritmo di *trading* sul mercato in termini di certezza ovvero di seria possibilità e che, ciononostante, che abbia agito comunque, pur di non rinunciare all'azione e ai vantaggi che avrebbe tratto dall'operare del sistema di negoziazione algoritmica[540].

Anche la dimostrazione del fatto che l'abuso di mercato sia stato considerato e voluto dal soggetto agente come mero 'prezzo da pagare' per l'obiettivo

[540] In questo senso, limitandosi alla sola manualistica, si veda G. MARINUCCI–E.DOLCINI–G.L. GATTA, *Manuale di diritto penale*, *op. cit.*, pp. 399-403 ; nonché, in giurisprudenza, Cass. Pen., Sezioni Unite, 18 settembre 2014 (ud. 24 aprile 2014), n. 38343: ""l'agente […], dopo aver tutto soppesato, dopo aver considerato il fine perseguito e l'eventuale prezzo da pagare, si sia consapevolmente determinato ad agire comunque, ad accettare l'eventualità della causazione dell'offesa", avendo compiuto "una scelta razionale […] assimilabile alla volontà". Più di recente in giurisprudenza, Cass. Pen., Sez. VI, 18 ottobre 2022, n. 47152: "il dolo eventuale ricorre quando l'agente si sia chiaramente rappresentata la significativa possibilità di verificazione dell'evento concreto e ciononostante, dopo aver considerato il fine perseguito e l'eventuale prezzo da pagare, si sia determinato comunque, anche a costo di causare l'evento lesivo, aderendo ad esso per il caso in cui non si verifichi".
Sui criteri che guidano distintivi di dolo eventuale e colpa cosciente, si rinvia, senza pretesa di esaustività a F. VIGANÒ, *Il dolo eventuale nella giurisprudenza recente*, in Il libro dell'anno del diritto 2013 Treccani, 2013, pp. 118-127; G. FIANDACA, *Sul dolo eventuale nella giurisprudenza più recente, tra approccio oggettivizzante-probatorio e messaggio generalpreventivo*, in Dir. Pen. Cont. Riv. Trim., 2012, fasc. 1, pp. 152-162; S. CANESTRARI, *La distinzione tra dolo eventuale e colpa* cosciente, *op. cit.* pp. 1-22.

perseguito[541] – il profitto[542] – deve dunque passare per l'accertamento di elementi fattuali che possano guidare nella lettura del moto interiore che ha sorretto la condotta[543].

In questo senso, il giudice può ricorrere agli indicatori elaborati dalla giurisprudenza, dovendo tenere in particolare considerazione la prospettiva di profitto che guida l'agire di chi utilizza l'algoritmo di *trading*, al fine di stabilire se questi, avendo previsto in termini di certezza la verificazione dell'abuso di mercato, avrebbe agito egualmente[544]. In altri termini, occorrerebbe operare una

---

[541] Il riferimento è alla tesi del bilanciamento di interessi fra il fine che guida l'agente e il prezzo da pagare per arrivarci di S. PROSDOCIMI, Dolus eventualis. *Il dolo eventuale nella struttura delle fattispecie penali*, 1993, Milano, Giuffrè, p. 31.

In particolare, il richiamo all'argomento del 'costi quel che costi' rievoca la c.d. prima formula di Frank, che esclude il dolo eventuale qualora si dimostri che se il soggetto avesse avuto la certezza della verificazione dell'evento, si sarebbe trattenuto dalla condotta. Tale valutazione pone dunque l'accento sulla verificazione dell'evento come 'costo' che il soggetto è – o meno – disposto a tollerare e l'impatto che questo avrebbe avuto sul proprio piano di azione. Si tratta di un criterio non esente da critiche e che, in particolare, non sembra valere nel caso in cui il verificarsi dell'evento comporti il fallimento del piano perseguito Cfr. Sul punto, di recente, Cass. Pen., Sez. I, 7 febbraio 2020 (dep. 6 marzo 2020), n. 9049 "anche nell'ipotesi in cui la verificazione dell'evento collaterale rappresenti il fallimento del piano non può escludersi che l'agente abbia operato una consapevole opzione accettando la verificazione dell'evento. Può infatti accadere che nell'agente prevalga la speranza, il desiderio di realizzare un certo risultato anche di fronte all'eventualità che proprio quella condotta renda definitivamente non realizzabile il risultato perseguito", nello stesso senso, in dottrina, M. ROMANO, *Art. 43*, *op. cit*, p. 412. A favore di una valorizzazione della prima formula di Frank, F. VIGANÒ, *Il dolo eventuale*, *op. cit*. pp. 12–17. Secondo l'Autore, la distinzione fra accettazione del rischio e accettazione dell'evento lesivo previsto in termini di certezza, consente di evitare di rimproverare per dolo la morte del figlio al padre che lo abbia portato in gita nei pressi di un ghiacciaio, pur consapevole dei rischi di tale attività comporta. Rimprovero che apparirebbe evidentemente contrario al senso comune.

La contrarietà al senso comune, nell'esempio citato, è figlia di una incomparabilità fra il bene vita del figlio e l'interesse per la montagna del padre, che porta a concludere che il padre non avrebbe intrapreso o proseguito l'azione, laddove avesse previsto in termini di certezza la verificazione della morte del figlio.

Lo stesso potrebbe non valere se i beni in gioco fossero invece comparabili, come si potrebbe ipotizzare con riferimento alle condotte in esame.

[542] Cfr. sul punto C. PEDRAZZI, *Problemi del delitto di aggiotaggio*, *op. cit.*, pp. 94-95, che distinguendo fra il 'fine' e il 'fine ultimo' afferma "fine ultimo dell'aggiotaggio sarà quasi sempre il lucro".

[543] In questo senso Cass. Pen., S.U., 18 settembre 2014 (ud. 24 aprile 2014), n. 38343.

[544] Ci si riferisce agli "indizi o indicatori" non tassativi individuati dalla Cass. Pen., S.U., 18 settembre 2014 (ud. 24 aprile 2014), n. 38343, che guidano il giudice nell'accertamento della sussistenza del dolo eventuale o della colpa cosciente: la condotta che caratterizza l'illecito, la lontananza dalla condotta standard, la storia e le precedenti esperienze dell'agente, la personalità e le conoscenze dell'agente, la durata e la ripetizione della condotta, la condotta successiva al fatto, la probabilità di verificazione dell'evento, il contesto lecito o illecito entro cui si colloca il

"valutazione *ex ante* e dal punto di vista dell'agente circa l'impatto che la verificazione dell'evento avrebbe avuto sul suo piano d'azione, onde stabilire se essa rappresentasse o meno un costo che egli era disposto a tollerare"[545].
Qualora invece non si giunga alla prova di una simile adesione volontaristica all'illecito, anche nella forma del dolo eventuale, si dovrà valutare la sussistenza di un atteggiamento riconducibile alla colpa, da considerare in relazione all'illecito amministrativo.

8.5. Sistemi di intelligenza artificiale 'forte' e gli 'abusi di mercato algoritmici': terzo scenario

È poi possibile immaginare un terzo scenario, in cui l'abuso sia il risultato di una programmazione che, pur coerente con le regole che disciplinano l'attività, risulti però inadeguata o obsoleta.

Ebbene, proprio rispetto a questa ipotesi emerge il principale punto di contatto fra potenziale diffusione di sistemi di negoziazione algoritmica capaci di agire sui mercati in modo, per così dire, 'autonomo' e la categoria del rischio consentito.
Come anticipato, il diffondersi nei mercati di simili sistemi potrebbe determinare infatti l'insorgere di rischi difficilmente governabili e financo comprensibili

---

fatto, il fine della condotta (la congruenza del prezzo connesso all'evento non direttamente voluto rispetto al progetto d'azione), le conseguenze negative o lesive per l'agente in caso di verificazione dell'evento, e la prima formula di Frank. Sulle critiche ad alcuni di questi indici si veda A. AIMI, *Il dolo eventuale alla luce del caso Thyssenkrupp*, in Il libro dell'anno del diritto Treccani 2015, 2015, pp. 127-136 e, in particolare, rispetto al criterio del discostamento dalla regola cautelare, F. VIGANÒ, *Il dolo eventuale*, *op. cit*. p. 9.
Alcuni di questi, in particolare, potrebbero essere valorizzati con riferimento ai fatti in questione, fra cui in particolare si potrebbe valutare la misura del discostamento dai doveri pre e post immissione previsti dai sopra illustrati Regolamenti Delegati UE e dal Regolamento Mercati (nel senso che tanto più il soggetto si sia discostato dal comportamento imposto da tali disposizioni, quanto più si potrebbe valutare che il soggetto abbia accettato l'eventualità della causazione dell'offesa e si sia consapevolmente determinato ad agire comunque), il fine del suo agire e la congruenza del prezzo da pagare in caso di verificazione dell'offesa (si potrebbe cioè ritenere sussistente il dolo eventuale nel caso in cui il profitto garantito dall'abuso di mercato sia superiore al 'prezzo della sanzione').
L'utilità di tali indicatori non rimuove il rischio – evidenziato dalla più attenta dottrina – che, in assenza di una fattispecie penale colposa, onde evitare l'impunità per comportamenti che vengono percepiti come particolarmente offensivi, si finisca per "punire fatti ontologicamente o sostanzialmente colposi a titolo di dolo", così M. CATENACCI, *I poteri dello Stato e diritto penale*, in M. Almerighi–A. Manna (a cura di), I poteri dello Stato e la Costituzione, Roma, Aracne, 2011, p. 84. Sul punto si tornerà *infra*.

[545] F. VIGANÒ, *Il dolo eventuale*, *op. cit*. p. 14.

dall'uomo[546] e dunque influire sulla valutazione di accettabilità del pericolo che l'attività di *trading* comporta operata dal legislatore. Ad oggi, il legislatore ritiene che, pur se dotata di una componente di pericolosità, l'attività di negoziazione algoritmica possa legittimamente essere esercitata. Lo scenario attuale potrebbe però mutare di fronte all'affacciarsi sui mercati di algoritmi di *trading* basati su tecnologie più sofisticate, dotati delle già citate caratteristiche di autonomia e imprevedibilità, che li rendono significativamente differenti – e in questo senso più pericolosi – rispetto ai sistemi tradizionali[547].

Tali caratteristiche possono cioè creare una quota di rischio diverso e ulteriore rispetto a quello valutato al momento della definizione delle regole che disciplinano l'attività"[548], dovuto all'evoluzione della tecnologia dei sistemi.

Di fronte a tale cambiamento di prospettiva, occorre chiedersi se sia comunque possibile muovere un rimprovero colposo – poste le premesse svolte con riferimento alle ipotesi dolose – a chi ha utilizzato l'algoritmo che ha posto in essere la strategia abusiva. Ossia se il fatto rientra comunque nell'ambito del rischio consentito e, dunque, non sia sanzionabile.

Come noto, la definizione di un'area del rischio consentito non esclude, secondo la tesi maggioritaria in dottrina, la possibilità che si verifichino eventi lesivi nonostante l'adeguatezza della condotta alle regole cautelari[549]. Tali eventi lesivi non vengono sanzionati perché l'ordinamento accetta l'eventualità che le regole cautelari non azzerino totalmente i rischi potenzialmente derivanti dall'attività

---

[546] Si potrebbe definire come un ennesimo tassello nel tortuoso percorso di definizione dei rapporti fra diritto penale e progresso della tecnica, nonché dei rapporti fra diritto penale e moderna 'società del rischio'. Cfr. C.E. PALIERO, *L'autunno del patriarca. Rinnovamento o trasmutazione del diritto penale dei codici?*, in Riv. It. Dir. Proc. Pen., 1994, fasc. 4, pp. 1220-1250; F. STELLA, *Giustizia e modernità. La protezione dell'innocente e la tutela delle vittime*, Milano, Giuffrè, III ed., 2003; M. DONINI, *Il volto attuale dell'illecito penale*, Milano, Giuffrè, 2004, p. 97 ss.; C. PIERGALLINI, *Danno da prodotto e responsabilità penale*, *op. cit.*; A. GARGANI, *La "flessibilizzazione" giurisprudenziale delle categorie classiche del reato di fronte alle esigenze di controllo penale delle nuove fenomenologie di rischio*, in Leg. pen., 2011, fasc. 2, pp. 397-425.

[547] Cfr. DUTCH AUTHORITY FOR THE FINANCIAL MARKETS*, Machine Learning*, *op. cit*., pp. 13-14 circa l'effettivo utilizzo – allo stato attuale – dei sistemi di negoziazione algoritmica basati su *reinforcement learning* e sulle preoccupazioni dimostrate dalle società di *trading*, che paiono in parte contraddire il fatto che la non-governabilità della macchina sia un risultato "voluto e ricercato dagli stessi programmatori poiché consente di raggiungere i risultati più performanti" B. FRAGASSO, *Intelligenza artificiale*, *op. cit.*, p. 288.

[548] Così R. BERTOLESI, *Intelligenza artificiale e responsabilità penale*, *op. cit*. p. 191.

[549] Considerando la nozione di rischio consentito c.d. residuale (o *Restrisiko*), ossia del rischio che 'resiste' all'adozione della diligenza necessaria e "impermeabile alla colpa generica". Così S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.*, p. 409. Cfr. anche G. FORTI, *Colpa ed evento*, *op. cit.*, p. 457.

pericolosa ed esclude la responsabilità per tali eventi in capo a chi si sia adeguato alle regole cautelari. Si parla in questo caso di una *inidoneità "programmata"*[550].
Esiste però la – diversa – possibilità che la regola cautelare divenga inadeguata rispetto a rischi di cui si viene a conoscenza a seguito della sua formulazione. In questo caso il fallimento della regola cautelare sopravviene, rendendola obsoleta rispetto alla mutata realtà. In questo caso, l'*inidoneità* è dunque *sopravvenuta*.
Posto che non è rimproverabile il soggetto che abbia osservato i limiti dettati dal legislatore in via precauzionale, allo scopo di fronteggiare anche pericoli ipotetici e che, pur rispettandoli, abbia causato eventi offensivi[551], cosa accade nel caso in cui la regola cautelare si riveli inidonea alla prevenzione del rischio e che tale inidoneità non rientri nell'area di quanto programmato e accettato dall'ordinamento?
Se l'abuso di mercato è, cioè, la conseguenza dell'agire di un sistema di negoziazione algoritmica che può 'agire da solo', ma chi ha utilizzato l'algoritmo si è attenuto alle norme sopracitate che disciplinano l'attività e che impongono specifici doveri di controllo *pre* e *post* immissione e posto che tali regole risultano inidonee a prevenire la realizzazione di strategie abusive, è possibile addebitare a questi una responsabilità per l'illecito?
Si tratta di uno scenario che apre la strada a tematiche ampiamente affrontate dalla dottrina che si è occupata del tema del rischio consentito: i limiti dell'affidamento che l'agente può riporre nella regola cautelare, il suo fallimento[552] e il suo intrecciarsi con l'assenza di conoscenze scientifiche circa la pericolosità di una determinata attività.

---

[550] Così F. CONSULICH, Rischio consentito, *op. cit.*, p. 1116 che definisce "ordinario" il rischio consentito identificato *ex ante*, ossia il caso in cui sin dal momento della formulazione della regola di prudenza se ne conosce una o più aree di inefficienza, che viene accettata dall'ordinamento.

[551] In questi termini, C. RUGA RIVA, *Principio di precauzione e diritto penale. Genesi e contenuto della colpa in contesti di incertezza scientifica*, in E. Dolcini – C.E. Paliero (a cura di) *Studi in onore di Giorgio Marinucci*, vol. II, Milano, Giuffrè, 2006, p. 1743 ss, in particolare p. 1756.

[552] P. VENEZIANI, *Regole cautelari "proprie" ed "improprie"*, *op. cit.*, p. 16 nota che al fallimento sono soggette sia le regole cautelari 'proprie' che quelle 'improprie'.
Secondo l'Autore (pp. 61-88), poi, il fallimento della regola cautelare può verificarsi in astratto o in concreto, a seconda che dipenda da difetti generali e intrinseci alla regola cautelare ovvero dalla presenza di circostanze di fatto anomale che impediscono di garantire il livello di sicurezza desiderato. L'anomalia della circostanza di fatto non pone in discussione l'efficacia e la validità generale della regola cautelare in circostanze 'normali'.

8.5.1. I limiti del rischio consentito: il fallimento delle regole cautelari che disciplinano l'attività

Una prima necessaria premessa, sul punto, è che il rischio consentito, per quanto abbia una ineliminabile funzione di tutela dell'affidamento per il soggetto che eserciti l'attività pericolosa ammessa dall'ordinamento, non può tuttavia trasformarsi in un "singolare 'cappello protettivo' per attività pericolose per le quali potrebbero invece in concreto adottarsi più efficaci misure precauzionali"[553].
Proprio per questa ragione, come si è detto, non può essere escluso il rimprovero doloso laddove si accerti che chi ha utilizzato l'algoritmo avesse piena conoscenza dell'inadeguatezza delle norme che ne regolano l'attività – e che la mantengano entro limiti di pericolosità tollerati dall'ordinamento – e che, ciononostante, lo abbia utilizzato ugualmente.
La tutela dell'affidamento riposto dall'agente nella liceità del suo operato si sostanzia nella possibilità di "contare sul fatto che, conformando le proprie condotte a quelle dell'agente modello, non sarà chiamato a rispondere per gli eventuali effetti lesivi da essere scaturiti, nemmeno laddove fossero *ex ante* prevedibili"[554]. In questo senso, dunque, il rischio consentito costituisce un argine all'espansione della colpa generica. Ciò tuttavia non implica che quest'ultima perda in assoluto qualsiasi valore nell'accertamento della responsabilità[555].
Infatti, "laddove un evento lesivo si verifichi malgrado il rispetto della regola cautelare, ed emerga che le cause che hanno determinato il fallimento della regola […] erano *ex ante riconoscibili* da parte dell'agente […] o addirittura da lui *conosciute*"[556], è anzi doveroso pretendere l'adozione di ulteriori cautele fondate

[553] M. ROMANO, *Art. 43*, *op. cit.*, p. 429, il quale sottolinea la necessità di una verifica in concreto della conformità o meno alla regola di diligenza dell'attività.

[554] Cfr. S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.*, pp. 374-383 che sottolinea la validità di questa regola, sia a fronte di regole cautelari rigide, sia a fronte di regole cautelari elastiche.

[555] Sui rapporti fra colpa specifica e colpa generica si vedano le contrapposte tesi di G. MARINUCCI, *La colpa per inosservanza*, *op. cit.*, p. 236 e C. PIERGALLINI, *Attività produttive e imputazione per colpa: prove tecniche di diritto penale del rischio*, in Riv. It. Dir. proc. Pen., fasc. 4, 1997, p. 1942; Sul punto anche ampiamente C. RUGA RIVA, *Principio di precauzione*, *op. cit.*, p. 1757 e C. PERINI, *Il concetto di rischio*, *op. cit.*, p. 36.

[556] S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.,* p. 381, che propone l'esempio della legge cha autorizza l'uso di una sostanza tossica senza prendere in considerazione alcuni dei suoi effetti lesivi.

sul dovere di diligenza[557]. Tale dovere si sostanzia nell'obbligo di "curare la ricerca e l'applicazione di ulteriori misure precauzionali per mantenersi in 'regola' rispetto alle evoluzioni rispetto all'evoluzione tecnologica di settore"[558] e la sua violazione può quindi fondare la responsabilità dell'agente.

Sicché, tornando al nostro ambito e come già detto, qualora nella mancata adozione di cautele ulteriori – pur non imposte dall'ordinamento, ma rese necessarie dal fallimento di queste – si rinvenga un atteggiamento doloso, il soggetto sarà chiamato a rispondere penalmente dell'abuso[559].

Qualora invece il dolo non sussista, si verserà invece nell'ambito della colpa e in questo caso i canoni della diligenza, prudenza e perizia assumono un ruolo fondamentale di presidio contro forme di immunità assoluta.

La valutazione sulla responsabilità di chi utilizza l'algoritmo di *trading* passa in questo caso per l'accertamento della prevedibilità del fallimento delle regole di cui all'art. 67 ter t.u.f., del Regolamento Delegato UE 2017/589 e del Regolamento Mercati Consob che disciplinano l'esercizio dell'attività di negoziazione algoritmica[560].

Solo se la risposta è positiva, il superamento dell'area del rischio consentito determinerà un rimprovero. Se, cioè, non abbia adottato le misure necessarie – *i.e.* ulteriori precauzioni o financo la disattivazione del sistema – pur in presenza di inequivoci segnali d'allarme, potrà essere chiamato a rispondere.

Tale valutazione si deve riferire alle conoscenze disponibili all'agente modello appartenente alla stessa cerchia di riferimento dell'agente concreto.

A sua volta, la definizione di questa cerchia di riferimento dipende, secondo la dottrina, "dal confronto tra i livello di conoscenza di cui disponeva l'agente *al momento del fatto* e di quelli a (o messi a) disposizione delle istanze *latu sensu* pubbliche"[561].

---

[557] Cautele volte a ripristinare il livello di sicurezza al quale mirava la regola fallita, il cui contenuto varia a seconda che la regola cautelare violata fosse di natura propria o impropria, come evidenziato da S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.,* p. 383.

[558] In questi termini V. MILITELLO, *Rischio e responsabilità penale*, *op. cit.,* con riferimento al caso in cui l'area di rischio consentito sia definita da un atto autorizzatorio dell'autorità amministrativa.

[559] Quanto all'ammissibilità del rimprovero doloso in attività a rischio consentito si rinvia a quanto detto *supra*. Si rimproverebbe in questo caso l'assunzione di un rischio irragionevole omettendo di gestire un sistema di intelligenza artificiale che può determinare eventi dannosi.

[560] Sul tema, seppur con riferimento alle *self-driving* cars, si veda S. GLESS–E. SILVERMAN–T. WEIGEND, *If robots cause harm, who is to blame?*, *op. cit.*, pp. 430-431.

[561] G. FORTI, *"Accesso" alle informazioni*, *op. cit*., p. 195.

La premessa da cui è necessario partire nella definizione dell'agente modello è dunque il fatto che i soggetti che esercitano una determinata attività – specie se essa richiede conoscenze tecniche specifiche e avanzate – non solo si trovano in una posizione di maggiore vicinanza rispetto alle fonti di pericolo, ma "sono in genere quelli che dispongono delle maggiori conoscenze sul pericolo stesso (o almeno di alcune conoscenze indispensabili per la sua comprensione) e sono tendenzialmente (anche se non esclusivamente) le più idonee ad attivare in modo efficace e tempestivo le necessarie cautele preventive"[562].

Il *quantum* di diligenza richiesto all'agente, dunque, di fatto è aumentato dal *plus* di conoscenze di cui dispone e dalla conseguente possibilità di azione 'qualificata' connessa alla sua vicinanza alla fonte del pericolo, entrambi fattori capaci di modificare i connotati dell'agente modello cui fare riferimento[563].

Non vi è dubbio che queste condizioni si verifichino in un settore specializzato come quello del *trading* algoritmico.

Il '*trader* algoritmico modello' è certamente un soggetto dotato di conoscenze causali specifiche che gli consentono di cogliere i segnali rivelatori dell'inadeguatezza delle regole cautelari codificate vigenti. L'uso di sistemi di negoziazione algoritmica infatti implica e presuppone un livello avanzato di

---

[562] G. FORTI, *"Accesso" alle informazioni*, *op. cit*., p. 194, il quale traccia un parallelo con le affermazioni della dottrina in materia di reato omissivo improprio e definizione della posizione di garanzia. Sull'innalzamento del tasso di diligenza dovuto in virtù delle speciali conoscenze dell'agente anche F. CONSULICH, *Rischio consentito*, *op. cit.*, p. 1113, secondo cui "all'aumentare dello spettro del comportamento esigibile, si riduce proporzionalmente il rischio che è lecito correre". Con particolare riferimento al *trading* algoritmico preme evidenziare come lo stesso Regolamento delegato UE 589/2017, art. 3, preveda che, oltre ai programmatori, anche chi è preposto al controllo dei sistemi debba avere *almeno* una conoscenza generale delle modalità di funzionamento dei sistemi di negoziazione algoritmica e degli algoritmi di negoziazione dell'impresa e delle relative strategie, oltre alle competenze sufficienti per dare seguito alle informazioni trasmesse con allarmi automatici. Questa competenze deve permettere loro di avere la sufficiente autorità per opporsi alla persona responsabile nei casi in cui questa attività crei condizioni negoziazione anormali o faccia sorgere sospetti di abusi di mercato.

[563] Nella definizione dell'*homo eiusdem professionis et condicionis*, come noto, non vengono prese in considerazione le speciali capacità individuali del singolo agente, ma esclusivamente le conoscenze e abilità che portino a individuare un diverso modello di agente (quelle che M. ROMANO, *Art. 43*, *op. cit.*, p. 428 definisce "maggiori cognizioni causali"), posto che il diritto penale non potrebbe imporre al soggetto sempre e comunque lo sfruttamento integrale di una sua dote eccezionale sotto la minaccia della sanzione. Sul punto, in particolare, F. BASILE, *Fisionomia e ruolo dell'agente-modello ai fini dell'accertamento processuale della colpa generica*, in G. Bellantoni–D. Vigoni (a cura di), Scritti in onore di Mario Pisani, Piacenza, La Tribuna, 2011, vol. III, pp. 209-242; e, nella manualistica, G. MARINUCCI–E. DOLCINI–G.L. GATTA, *Manuale di diritto penale*, *op. cit.*, pp. 422-426; nonché G. FIANDACA–E. MUSCO, *Diritto penale*, *op. cit.*, pp. 583-585.

competenze tecniche che riguardano il funzionamento degli algoritmi e i rischi associati a tali strumenti. Ci si riferisce in particolare alle competenze nell'ambito della programmazione degli algoritmi[564], nella predisposizione di sistemi di analisi di grandi volumi di dati finanziari, storici e in tempo reale, nonché nelle tecniche di gestione del rischio connesse alle strategie algoritmiche[565]. Inoltre, una particolare fonte di conoscenza del rischio legato al *trading* algoritmico proviene dall'utilizzo di strumenti di simulazione per testare le *performance* degli algoritmi su dati storici (c.d. *backtesting*) e valutarne l'efficacia e la validità in diverse condizioni di mercato.

In questo caso la valutazione del comportamento richiesto al '*trader* algoritmico modello' passa per l'individualizzazione della misura della diligenza imposta, che viene innalzato in base alle specifiche conoscenze da questi detenute.

Infatti, chi detiene una posizione di particolare potere informativo è in grado di valutare i segnali di incipiente fallimento della regola cautelare e, di conseguenza, adottare ulteriori misure precauzionali. I 'segnali d'allarme' che devono sollecitare l'agente ad attivarsi in questo senso sono la frequenza e la diffusione degli eventi di danno (desumibili dal grado di reiterazione e di manifestazione del danno e dalla durata della commercializzazione del prodotto e della sua penetrazione sul mercato); l'intensità del rischio (intesa nel senso di gravità e omogeneità dei danni); il tasso predeterminato di un aumento del rischio e l'assenza di plausibili spiegazioni alternative all'uso del prodotto come causa degli episodi di danno e la surrogabilità del prodotto[566].

8.5.2. L'incertezza scientifica

---

[564] Che implicano la conoscenza di linguaggi di programmazione specifici della finanza.

[565] Ad esempio l'uso di *stop-loss order* automatici (ordine di chiudere una posizione acquistando o vendendo un titolo sul mercato quando questo raggiunge un determinato prezzo) e il *position sizing* (la dimensione di una posizione all'interno di un determinato portafoglio, ossia il numero di titoli che l'investitore può negoziare in modo da controllare il rischio e massimizzare i rendimenti).

[566] Sul punto C. PIERGALLINI, *Danno da prodotto e responsabilità penale*, *op. cit.*, p. 537 secondo cui "alla certezza o all'alta probabilità scientifica, deve subentrare una *certezza sociale*, caratterizzata dalla presenza di *segni* che, per poter assurgere al rilievo penale, devono tramandare l'immagine di un prodotto che *tende, propende al danno*" e che tradiscano una "*dannosità superiore*, sul piano dell'*analisi costi/benefici*, rispetto ai *possibili vantaggi che derivano dalla sua utilizzazione*". Sui 'segnali di allarme' anche D. CASTRONUOVO, *Principio di precauzione e diritto penale*, Aracne, 2013, p.168 e G. FORTI, *"Accesso" alle informazioni*, *op. cit.*, pp. 221 ss.

Le considerazioni sin qui svolte in tema di maggiori conoscenze del *trader* algoritmico e conseguente modifica della diligenza imposta, per quanto rilevanti nei termini sopra indicati, trovano tuttavia un limite nell'incertezza scientifica[567], con significative conseguenze in termini di responsabilità di chi utilizza l'algoritmo.

Si tratta di una questione che riguarda, ancora una volta, il giudizio di prevedibilità o *rectius* di riconoscibilità del pericolo di verificazione del fatto antigiuridico[568]. L'assenza di disponibilità *ex ante* di leggi scientifiche consolidate, sulla base delle quali si possa svolgere il giudizio di riconoscibilità, influisce infatti sulla possibilità di muovere un rimprovero all'agente, salvo non imputare una responsabilità per il sol fatto di aver posto in essere l'attività illecita[569].

Ci si domanda, in sostanza, quale sia il comportamento che l'agente dovrebbe tenere di fronte all'incipiente fallimento della regola cautelare nella capacità di contenere i rischi per cui erano state immaginate.

Una possibile risposta potrebbe rinvenirsi nel principio di precauzione[570], nella sua accezione 'pura'. Si potrebbe cioè ritenere che di fronte a un'attività che presenta un rischio potenziale – ma non supportato da certezze scientifiche – l'unica possibilità sia quella di imporre una totale astensione dalla stessa.

---

[567] C. RUGA RIVA, *Principio di precauzione*, *op. cit.*, p. 1743 definisce l'incertezza scientifica come quell'insieme di "contesti in cui si avanzano congetture di gravi pericoli per i beni fondamentali, pur in assenza di con solidate evidenze scientifiche circa l'effettiva pericolosità di date condotte, prodotti o sostanze o in presenza di dati scientifici discordanti o comunque non pienamente corroborati". Il tema è emerso con particolare rilievo in materia ambientale e rispetto all'utilizzo ed esposizione a sostanze tossiche. Cfr., inoltre, G. FORTI, *"Accesso" alle informazioni*, *op. cit.*, S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.*, 323 ss. Più in generale, C. PIERGALLINI, *Danno da prodotto e responsabilità penale*, *op. cit.*, pp. 552-554 e F. GIUNTA, *Il diritto penale e le suggestioni*, *op. cit.*, pp. 241-247.

[568] Sulla maggiore correttezza della locuzione indicata anziché del termine "prevedibilità" specie con riferimento agli illeciti colposi di mera condotta, in cui non vi è alcun evento da prevedere si veda F. BASILE, *Fisionomia e ruolo dell'agente-modello*, *op. cit*, pp. 214-215.

[569] Soluzione che tuttavia è del tutto in accettabile per l'evidente contrasto con il principio di colpevolezza. Al contrario, l'accertamento della responsabilità dell'agente deve passare necessariamente dall'individuazione di leggi scientifiche che potessero guidarlo nell'agire. Sul punto, in relazione ai contrapposti orientamenti di dottrina e giurisprudenza in relazione ai c.d. *toxic case*, si veda S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.*, pp. 316-333.

[570] Che, come nota C. PIERGALLINI, *Il paradigma della colpa nell'età del rischio: prove di resistenza del tipo*, in Riv. it. dir. proc. pen., 2005, fasc. 4, p. 1695, nt. 28 "presupposto comune e condizione tipica di applicazione del principio di precauzione è l'esistenza di un rischio connesso alla *incertezza sui potenziali effetti negativi* […] derivanti dallo svolgimento di una certa attività o dall'impiego di alcune tecnologie". Il principio di precauzione, secondo l'Autore (p. 1696), "sottende nessi causali non conosciuti, non accertati o comunque provvisti di tassi di frequenza estremamente ridotti", al contrario della regola cautelare che tende a "ricostruire i pericoli secondo la massima del sapere o del non-sapere".

In dottrina, tuttavia, non vi è consenso intorno alla possibilità di rinvenire nel principio di precauzione la soluzione alla gestione di siffatte situazioni[571].
Secondo alcuni Autori[572], proprio l'incertezza su quale sia la condotta doverosa capace di evitare l'evento dannoso è elemento ostativo alla valorizzazione del principio in esame[573], anche nell'accezione 'attenuata" che impone di individuare modalità di esercizio dell'attività che dovrebbero collocarsi su un certo livello di sicurezza[574].
A questa impostazione si contrappone una parte della dottrina secondo cui invece il principio di precauzione dovrebbe costituire uno dei parametri sulla base dei quali definire il contenuto di regole cautelari codificate ovvero, secondo altri, anche del rimprovero per colpa generica[575].
La posizione più convincente, tuttavia, con riferimento al settore dei rischi ambientali, proprio valorizzando la vicinanza rispetto alla fonte del rischio e al *plus* di conoscenze e al potere di azione che da tale vicinanza deriva, ammette la valorizzazione del principio di precauzione anche in ambito penalistico[576].

---

[571] Sulle diverse posizioni espresse dalla dottrina che si è occupata dell'imputazione per colpa nei *toxic cases*, ampiamente S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.*m pp. 317-335.

[572] C. PIERGALLINI, *Il paradigma della colpa*, *op. cit*., p. 1688; nonché F. GIUNTA, *Il diritto penale e le suggestioni del principio di precauzione*, in Criminalia, 2006, p. 241.

[573] Come efficacemente sottolinea F. GIUNTA, *Il diritto penale e le suggestioni, op. cit.*, p. 242, "in situazioni di incertezza scientifica, infatti, risulterebbe assai ardua la stessa riconoscibilità dei presupposti fattuali della condotta doverosa (qual è il grado di incertezza scientifica che l'operatore dovrebbe ritenere sufficiente per affermare la plausibilità del dubbio?) e non meno certo l'*ubi consistam* del dovere di diligenza".

[574] S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit*., p. 322, che sottolinea come gli Autori non individuino individuare né il livello accettabile, né la modalità tramite cui raggiungerlo, rendendo inaccettabile questa soluzione, specie sul piano piano della determinatezza e della irretroattività; nello stesso senso C. PIERGALLINI, *Il paradigma della colpa*, *op. cit*., p. 1697 e F. GIUNTA, *Il diritto penale e le suggestioni*, *op. cit.*, p. 230.

[575] Cfr. C. RUGA RIVA, *Principio di precauzione*, *op. cit.*, pp. 1758-1759 specie con riferimento a situazioni in cui il collegamento fra specifica patologia e esposizione a sostanze tossiche, non supportato da evidenze scientifiche al momento del fatto venga dimostrato in un momento successivo grazie ai progressi delle conoscenze scientifiche. Secondo l'Autore, il principio di precauzione – la cui fonte si può rinvenire in "numerose fonti internazionali e in particolare dal Trattato sull'Unione europea, che va ad arricchire lo spettro delle regole cautelari pronte a gemmare nel tronco dell'art. 43 c.p." – potrebbe incidere sul concetto normativo di colpa in contesti di incertezza scientifica. La precauzione sarebbe cioè "null'altro che la tradizionale prudenza di fronte a un contesto nuovo (l'incertezza scientifica)".

[576] G. FORTI, *"Accesso" alle informazioni*, *op. cit.*, p. 192 pur nella convinzione di una "esista una generale incompatibilità del principio di precauzione con i criteri retrospettivi propri della responsabilità penale e, soprattutto, con la correlativa necessità di appoggiare quest'ultima

Infatti, la logica sottesa alle norme che regolano il settore ambientale – di fonte europea e internazionale – è quella secondo cui, per anticipare la verificazione del danno e per facilitare e rendere meno oneroso il ristabilimento della situazione compromessa, è necessario un intervento da parte di chi si trova nella posizione più vicina alla fonte del pericolo. Sicché, proprio la prossimità alla fonte del pericolo, la posizione di controllo rispetto a questo e la conseguente possibilità di identificare la situazione potenzialmente lesiva non solo consentono di prefigurarsi le conseguenze più sfavorevoli dell'attività, ma impongono anche di arrestare o contenere i suoi sviluppi dannosi e, dunque, in ultima istanza ridurne i costi per la collettività. È in questo senso che la logica della precauzione può essere utilizzata per muovere un rimprovero a chi è dotato di conoscenze 'superiori' proprio per la sua vicinanza alla fonte del pericolo[577].

Inoltre, nei settori caratterizzati dai "moderni rischi tecnologici"[578], proprio le maggiori conoscenze di chi esercita l'attività determinano "un'elevazione dello standard della c.d. 'figura modello' utilizzato per la ricostruzione delle regole di diligenza" e devono essere prese in considerazione per stabilire se questi avesse un dovere di riconoscere il pericolo. Perciò, "il «dovere di riconoscere» il fatto rispetto al quale commisurare la condotta dell'agente sarà da ritenere sussistente nel momento in cui un soggetto dotato delle conoscenze proprie della figura modello di appartenenza, in rapporto alla situazione concreta (definita dall'insieme delle circostanze esteriori e, in più, delle conoscenze supplementari

---

su un sufficiente livello di certezza dei pericoli: requisito da cui, per definizione, l'idea di precauzione tende a prescindere", ritiene che in materia ambientale esso possa trovare un margine di applicabilità. La considerazione si basa su un'attenta lettura dei principali atti normativi comunitari e internazionali, che segnano un legame fra il principio di precauzione, il principio di correzione alla fonte dei danni causati all'ambiente e il principio 'chi inquina paga'.

[577] G. FORTI, *"Accesso" alle informazioni*, *op. cit.*, p. 195, "non sarà di per sé dunque la prospettabilità di rischi che potrà generare un dovere all'astensione dalla condotta pericolosa (e correlativamente un'imputazione di eventi non meglio descritti che se ne possano considerare, problematicamente, la «realizzazione»), almeno laddove la condotta possa iscriversi nell'alveo di rischi "autorizzati", bensì un insieme di elementi più complessi scaturenti dal confronto tra i livelli di conoscenza di cui disponeva l'agente al momento del fatto e di quelli a (o messi a) disposizione delle istanze *lato sensu* pubbliche". Inoltre, secondo l'Autore (p. 219), chi dispone di conoscenze superiori a quelle a disposizione è gravato dall'ulteriore "dovere di rendere edotta l'istanza di controllo di tutte le conoscenze che potrebbero modificare l'originaria valutazione" sull'estensione dell'area di rischio consentito, che è soggetta a un progressivo modularsi in base allo scambio di informazioni tra privato – particolarmente attrezzato di *know-how* tecnologico – e autorità.

[578] G. FORTI, *"Accesso" alle informazioni*, *op. cit.*, p. 217.

possedute dall'agente), avrebbe potuto rendersi conto della possibile verificazione del fatto"[579].

La disponibilità delle migliori conoscenze e di competenze specifiche sull'attività produttiva di rischio influisce inoltre sulla base fattuale e nomologica su cui fondare il giudizio di riconoscibilità del pericolo di verificazione del fatto antigiuridico[580]. In capo a "soggetti che abbiano le risorse economiche necessarie per predisporre o sviluppare programmi di ricerca, o comunque in capo ai soggetti che operino in settori ad elevata innovazione tecnica e tecnologica ove chi crea il rischio possiede le migliori conoscenze per dominarlo"[581] incombe un obbligo di approfondimento scientifico che muta la riconoscibilità del rischio stesso.

Ebbene, la ricostruzione svolta con specifico riferimento ai rischi ambientali derivanti dall'esercizio di attività produttive si basa su premesse che possono essere riprodotte con riferimento al contesto oggetto del presente lavoro.

Si è già evidenziato che l'utilizzo di applicazioni di intelligenza artificiale ha ricevuto una prima – fondamentale – fonte di disciplina nel recente Regolamento

---

[579] G. FORTI, *"Accesso" alle informazioni*, *op. cit.*, pp. 219-220 affronta il tema della rilevanza da attribuire alle qualità superiori che non abbiano che non abbiano subito ancora una tale standardizzazione entro la figura dell'agente modello e, di conseguenza, la misura della diligenza doverosa ed esclude che la lettura proposta segni l'abbandono della misura oggettiva della diligenza a favore della misura soggettiva. L'Autore sostiene infatti che "la misura oggettiva di diligenza si basa sul modello di un uomo avveduto «nella situazione dell'agente; situazione che comprende anche le conoscenze di questi in rapporto al concreto rischio di verificazione dell'evento»". Dunque, Il «dovere di riconoscere» il fatto rispetto al quale commisurare la condotta dell'agente sarà da ritenere sussistente nel momento in cui un soggetto dotato delle conoscenze proprie della figura modello di appartenenza, in rapporto alla situazione concreta (definita dall'insieme delle circostanze esteriori e, in più, delle conoscenze supplementari possedute dall'agente), avrebbe potuto rendersi conto della possibile verificazione del fatto". Si tratta di una soluzione coerente, secondo l'Autore, con il principio di affidamento che assicura ai singoli la libertà di azione, "solo fintanto che non siano ravvisabili nella situazione concreta circostanze particolari, che lo contraddicano".

[580] Come nota C. RUGA RIVA, *Principio di precauzione*, *op. cit.*, pp. 1761-1762, ci si chiede "a quali condizioni l'evento – astrattamente congetturabile al momento della condotta e poi «puntalmente» verificatosi – possa ritenersi prevedibile. […] Sono sufficienti *dati fattuali* oppure occorrono *congetture scientifiche*? E in quest'ultimo caso, quale è il grado di consenso all'interno della comunità scientifica reputato necessario? In line di massima, *dati fattuali* anomali fanno scorgere […] l'obbligo di conoscenza scientifica, a sua volta distinto in obbligo *di approfondimento scientifico* o *di aggiornamento scientifico* sulle possibili cause degli eventi riscontrati, l'*obbligo di monitoraggio* […] e *gli obblighi di informazione* (*di segnalazione di rischi, di suggerimento di cautele d'impiego, ecc.*).

[581] C. RUGA RIVA, *Principio di precauzione*, *op. cit.*, p. 1762.

sull'intelligenza artificiale. La logica sottesa a tale atto è quella di conoscenza, gestione e contenimento del rischio, a diversi livelli[582].

Proprio la logica della prevenzione del rischio rappresenta il primo elemento comune fra la disciplina della materia ambientale[583] e quella sull'intelligenza artificiale.

Così come nel settore ambientale[584], per le applicazioni di intelligenza artificiale il legislatore europeo ha costruito un impianto basato sul controllo e la limitazione crescente all'aumentare del rischio legato all'uso del sistema.

Il secondo punto di convergenza fra le regolamentazioni dei due settori sta poi nella logica della 'vicinanza' alla fonte di rischio.

Le norme in materia ambientale si fondano sui principi della precauzione e dell'azione preventiva in via prioritaria alla fonte dei danni causati all'ambiente[585], dunque i vari soggetti coinvolti nell'attività pericolosa hanno l'obbligo di adottare misure preventive per ridurne l'impatto ambientale e, in caso di danno, di coprire i costi associati al risanamento o alla compensazione dello stesso[586].

---

[582] In questo senso F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*, par. 4.

[583] I cui principi fondamentali sono ampiamente analizzati con riferimento agli aspetti di interesse penalistico nei lavori di G. FORTI, *"Accesso" alle informazioni*, *op. cit.* e C. RUGA RIVA, *Il principio di precauzione*, *op. cit.*, pp. 1743-1777.

[584] Invero, la logica dell'analisi e della gestione rischio è adottata dal legislatore europeo in numerosi settori, fra cui ad esempio quello alimentare. Cfr. Art. 6 del Regolamento (CE) n. 178/2002 del Parlamento e del Consiglio del 28 gennaio 2002 che stabilisce i principi e i requisiti generali della legislazione alimentare, istituisce l'Autorità europea per la sicurezza alimentare e fissa procedure nel campo della sicurezza alimentare: "1. Ai fini del conseguimento dell'obiettivo generale di un livello elevato di tutela della vita e della salute umana, la legislazione alimentare si basa sull'analisi del rischio, tranne quando ciò non sia confacente alle circostanze o alla natura del provvedimento. […] 3. La gestione del rischio tiene conto dei risultati della valutazione del rischio […]" e Art. 7: "1. Qualora, in circostanze specifiche a seguito di una valutazione delle informazioni disponibili, venga individuata la possibilità di effetti dannosi per la salute ma permanga una situazione d'incertezza sul piano scientifico, possono essere adottate le misure provvisorie di gestione del rischio necessarie per garantire il livello elevato di tutela della salute che la Comunità persegue, in attesa di ulteriori informazioni scientifiche per una valutazione più esauriente del rischio".

[585] Art. 191, par. 2, TFUE: "La politica dell'Unione in materia ambientale mira a un elevato livello di tutela, tenendo conto della diversità delle situazioni nelle varie regioni dell'Unione. Essa è fondata sui principi della precauzione e dell'azione preventiva, sul principio della correzione, in via prioritaria alla fonte, dei danni causati all'ambiente, nonché sul principio «chi inquina paga»".

[586] Oltre al produttore, anche altri soggetti lungo la catena di distribuzione possono essere responsabili della gestione dei rischi ambientali. Questo include chi gestisce rifiuti o chi distribuisce prodotti inquinanti. Tutti gli attori coinvolti devono garantire che le loro attività rispettino gli standard ambientali.

Nell'AI Act, il principio di gestione del rischio è applicato in modo del tutto sovrapponibile: i principali attori responsabili sono i fornitori, i distributori, e i *deployer*. La responsabilità è distribuita lungo la 'catena del valore tecnologico', in modo che ciascun attore abbia obblighi specifici per ridurre il rischio associato al sistema[587].

Se dunque la logica fondamentale è comune, si può tracciare un parallelo anche per quanto attiene ai ragionamenti sopracitati sull'atteggiarsi del principio di precauzione e del contenuto del rimprovero che si può muovere a chi esercita l'attività pericolosa. Ciò significa, in definitiva, che nel settore del *trading* algoritmico - anche di fronte a contesti di incertezza scientifica – si possono applicare i medesimi criteri di attribuzione della responsabilità.

Ferma la tendenziale e generale incompatibilità del principio di precauzione con "i criteri i criteri retrospettivi propri della responsabilità penale e, soprattutto, con la correlativa necessità di appoggiare quest'ultima su un sufficiente livello di certezza dei pericoli"[588], nel settore del *trading* algoritmico, esso può trovare un margine di applicabilità[589]. Anche di fronte all'incertezza scientifica, la posizione di privilegio informativo influisce sul giudizio di riconoscibilità del pericolo di verificazione del fatto antigiuridico e, dunque, sulla responsabilità. Tanto che il soggetto potrà essere ritenuto responsabile qualora il verificarsi del fatto antigiuridico sia riconducibile al mancato rispetto del canone di precauzione.

8.5.3. La ridefinizione legislativa dell'area di rischio consentito

Tutto ciò premesso, non si può trascurare il fatto che l'enorme velocità di sviluppo dei sistemi di intelligenza artificiale 'forte' apre all'eventualità che in futuro il fallimento della regola cautelare non sia colmabile attraverso il canone

---

[587] Gli obblighi sono stabiliti dalla Sezione III del regolamento (artt. 16-27) e consistono in buona sostanza nella valutazione preliminare del rischio del sistema prima della sua commercializzazione e nell'adozione di misure preventive per minimizzare il rischio; nella verifica che dei sistemi venga fatto un uso appropriato e conferme alle proprie finalità e caratteristiche; nel dovere di immissione sul mercato di prodotti rispettosi degli standard di sicurezza e dotati di adeguata documentazione.

[588] G. FORTI, *"Accesso" alle informazioni*, *op. cit.*, p. 192.

[589] Sulla – diversa – questione dell'utilizzabilità di una logica precauzionale nella deifnizione di nuove fattispecie incriminatrici, stante l'assenza di una dimostrazione oggettiva di qualche danno già sperimentato e sull'incompatibilità del principio in questione con la razionalità dell'intervento penale e i suoi principi di tipicità, materialità e provabilità processuale, si veda F. F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*, par. 1. L'Autore – peraltro riferendosi a tutte le applicazioni di i.a. e non solo al settore finanziario – ritiene che tale logica potrebbe supportare, semmai, soluzioni amministrative.

della colpa generica e della logica precauzionale e che, di conseguenza, proprio l'area del rischio consentito sia posta di fronte a una inadeguatezza intollerabile e incolmabile in via, per così dire, interpretativa.

Si tratta dei casi che la dottrina definisce di "inidoneità generale e assoluta"[590] della regola cautelare a contenere la pericolosità dell'attività entro margini tollerabili.

In effetti, fra i fattori che possono determinare tale condizione rientrano l'emergere di nuove conoscenze scientifiche riguardo l'attività pericolosa e l'evoluzione dell'attività stessa[591].

Quest'ultima eventualità è quella che con più probabilità potrebbe riguardare gli algoritmi di *trading*. Infatti, le regole del Regolamento MAR, del t.u.f., del Regolamento Delegato UE 2017/589 e del Regolamento Mercati Consob sono state elaborate guardando a sistemi che erano dotati di determinate caratteristiche – prima fra tutte la dipendenza dall'essere umano – che sembra potrebbero essere significativamente superate nei sistemi più evoluti[592].

L'obsolescenza dei confini dell'area di rischio consentito potrebbe dunque imporre un nuovo bilanciamento fra rischi e benefici, che grava necessariamente sull'ordinamento.

Il legislatore dovrà dunque riconsiderare se e entro quali limiti i rischi – prima sconosciuti – sono tollerabili, tenendo conto dell'utilità sociale dell'attività.

L'esito di tale valutazione è, anche in questo caso, frutto di una scelta fra due alternative nette: il divieto assoluto di esercizio dell'attività – perché dotata di un livello di pericolosità non accettabile e non contenibile – oppure la predisposizione di nuove regole cautelari che ri-definiscano l'area del rischio consentito[593].

---

[590] Così F. CONSULICH, *Rischio consentito*, *op. cit.*, p. 1116.

[591] Lo stato delle conoscenze scientifiche e tecniche al momento del danno rileva quale motivo di esclusione della responsabilità del produttore, ai sensi dell'art. 118, lett. e), d.lgs. 206/2005 qualora non permettesse di considerare ancora il prodotto come difettoso.

[592]Cfr. A. AZZUTTI–W.G. RINGE–H.S. STIEHL, *Machine Learning, Market Manipulation*, op. cit., pp. 83-92.

[593] Secondo la dottrina, è opportuno che tale processo di rivalutazione sia trasparente e coinvolga tutte le parti interessate, anche per consentire ai responsabili di adottare misure legittime in grado di realizzare il livello prescelto di protezione dei beni giuridici rilevanti, cfr. G. FORTI, *"Accesso" alle informazioni*, *op. cit.*, p. 164. In questo percorso di democratizzazione si collocano alcune forme di collaborazione dell'ESMA con Autorità di vigilanza sui mercati, come ad esempio quella olandese (AFM) per lo sviluppo di controlli pre negoziazione previsti da MiFID II (https://www.bloomberg.com/news/articles/2024-10-29/dutch-regulator-seeks-better-algo-testing-to-avert-market-abuse?embedded-checkout=true). Già prima, L'auspicio di

Lo scenario sin qui illustrato parte però dal presupposto che vi sia certezza sulla pericolosità – ancorché aumentata o comunque mutata – dell'attività.
Tale certezza potrebbe quantomeno essere messa in dubbio di fronte a un ambito, quello delle applicazioni di intelligenza artificiale, rispetto a cui vi è certamente un diffuso interesse ed entusiasmo, ma non altrettante conoscenze. Si pensi solo alla capacità dei sistemi di *machine learning* di emanciparsi dalle informazioni ricevute in sede di programmazione, giungendo a soluzioni *innovative* e addirittura, secondo alcuni, *creative*[594] che comporterebbe non solo una perdita di controllo degli *output*, ma anche una difficile comprensione da parte degli stessi soggetti che hanno programmato il sistema.

democratizzazione delle procedure di *risk assesment* era contenuto già nella Comunicazione della Commissione sul principio di precauzione (COM (2000) def.) del 2 febbraio 2000, punto 6.2, con riferimento al settore ambientale.

[594] B. FRAGASSO, *Intelligenza artificiale*, *op. cit.*, p. 289; A. CAPPELLINI, Machina delinquere non potest*?*, *op. cit.*, p. 506 fa riferimento a "prodotti soggettivizzati" che tengono "comportamenti attivi assolutamente imprevedibili, derivanti dal lavorio autoevolutivo del *machine learning*, tali che qualunque danno da essi derivante sfugga inesorabilmente alle capacità previsionali dei programmatori".

CAPITOLO IV

CONSIDERAZIONI CONCLUSIVE

SOMMARIO*: 1. The American Way:* il *Financial Artificial Intelligence Risk Reduction Act* – 1.1. La responsabilità del programmatore – 1.1.1. Le previsioni che regolano l'*an* della responsabilità dell'uomo – 1.1.2. Le previsioni che regolano il *quantum* della responsabilità dell'uomo – 1.2. I doveri del Financial Stability Oversight Council – 1.3. Un bilancio della soluzione americana – 2. Gli algoritmi di *trading* basati su sistemi di intelligenza artificiale c.d. 'forte' e il nuovo capitolo della 'società del rischio' – 3. Una possibile prospettiva *de iure condendo*

1. *The American Way*: il *Financial Artificial Intelligence Risk Reduction Act*

Negli Stati Uniti, il crescente impiego dell'intelligenza artificiale nel settore degli investimenti finanziari e la potenziale diffusione di sistemi dotati di una certa autonomia ha sollecitato l'opportunità di un intervento legislativo in materia.
Come già avvenuto in passato[595], il legislatore americano dimostra particolare attenzione per l'integrità dei mercati finanziari e le potenziali minacce provenienti dall'impiego di sistemi di intelligenza artificiale[596]. Si muove infatti in questa direzione il teso della proposta di Financial Artificial Intelligence Risk Reduction Act, presentata al Senato il 18 dicembre 2023[597].

---

[595] Ci si riferisce all'approvazione del già citato Dodd–Frank Act.

[596] Per una analisi dell'attuale utilizzo da parte degli *hedge fund* di tecnologie di intelligenza artificiale e di apprendimento automatico nelle decisioni di *trading*, dei potenziali rischi per la stabilità del mercato e dell'applicabilità delle normative esistenti a tali tecnologie si veda U.S. SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNAMETAL AFFAIRS, *AI in the real world. Hedge Funds' Use of Artificial Intelligence in Trading*, giugno 2024, in https://www.hsgac.senate.gov/wp-content/uploads/2024.06.11-Hedge-Fund-Use-of-AI-Report.pdf.

[597] Proposta di legge per la modifica del Financial Stability Act del 2010 ((12 U.S.C. 5321 et seq.). L'obiettivo dichiarato dell'atto è quello di "fornire al Financial Stability Oversight Council i compiti relativi all'intelligenza artificiale nel settore finanziario, e altri scopi" (traduzione nostra). In particolare, si propone l'inserimento, all'interno del sub. A del Financial Stability Act la sec. 126, intitolata "Disposizioni speciali relative all'intelligenza artificiale intelligenza artificiale nel settore finanziario" (traduzione nostra). Il testo della proposta è disponibile al seguente link: https://www.congress.gov/118/bills/s3554/BILLS-118s3554is.pdf. Sui limiti della scelta di presidiare verticalmente un solo settore, anziché prevedere una disciplina applicabile a diversi

Dal testo della proposta – attualmente in fase di esame presso il Committee on Banking, Housing, and Urban Affairs – emergono, in particolare, due elementi: la centralità della responsabilità dell''uomo dietro alla macchina' e la deterrenza all'uso improprio dell'i.a.
I principali interventi proposti riguardano infatti la disciplina della responsabilità per atti pregiudizievoli per l'integrità dei mercati e la sorveglianza sull'azione dei sistemi di intelligenza artificiale da parte del Financial Stability Oversight Council.

1.1. La responsabilità del programmatore

Le previsioni contenute nella proposta di FAIRR Act che attengono alla disciplina della responsabilità della persona che 'sta dietro alla macchina' possono essere ricondotte a due macro-categorie: quelle che *regolano l'an* della responsabilità dell'uomo e quelle che ne regolano il *quantum*.

1.1.1. Le previsioni che regolano l'an della responsabilità dell'uomo

La sec. 7 del FAIRR Act introduce due proposte di modifica del Securities Exchange Act.
La prima ha ad oggetto l'introduzione di una presunzione di sussistenza dell'elemento soggettivo[598] richiesto dalle leggi federali in materia finanziaria in capo a chiunque, direttamente o indirettamente, impieghi o faccia impiegare un modello di intelligenza artificiale in relazione a tutti gli atti, le pratiche o i comportamenti posti in essere da tale modello e a qualsiasi risultato derivante dall'uso di tale modello.
Per esplicita previsione dei proponenti, la persona 'dietro alla macchina' – chi impiega o fa impiegare il sistema di i.a. – risponde nella stessa misura in cui avrebbe risposto se avesse commesso direttamente tali atti, pratiche o comportamenti, a meno che non abbia preso misure preventive o altre cautele, quali, ad esempio, *policy* e procedure scritte verosimilmente capaci di prevenire le violazioni.

---

ambiti, anche alla luce del paragone con l'AI Act, si veda F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*, par. 3.
Guardando al contesto americano, è inoltre da segnalare il lavoro del Bipartisan Senate AI Working Group del maggio 2024: Bipartisan Senate AI Working Group, *Driving U.S. Innovation in Artificial Intelligence. A Roadmap for Artificial Intelligence Policy in the United State Senate*, Maggio 2024, in https://www.schumer.senate.gov/imo/media/doc/Roadmap_Electronic1.32pm.pdf.

[598] Sec. 42(a). Il testo della proposta fa riferimento a: "*scienter, other state of mind, or negligence requirements*".

Si tratta, in definitiva, di una disposizione che ha una duplice finalità: presumere la rimproverabilità soggettiva dell'illecito[599] e introdurre una sorta di *fictio* di commissione da parte dell'uomo del reato materialmente posto in essere dalla 'macchina'.
La seconda proposta di modifica stabilisce invece il divieto di previsione di cause di esonero contrattuale della responsabilità civile dello sviluppatore per difetti di progettazione o violazioni di obblighi impliciti da cui derivi una violazione delle leggi federali in materia finanziaria[600].

1.1.2. Le previsioni che regolano il quantum della responsabilità dell'uomo.

Infine, la sec. 6 del FAIRR Act prevede che, qualora la violazione delle regole della SEC per cui sono previste sanzioni civili siano commesse utilizzando sistemi di intelligenza artificiale, queste vengono triplicate[601].
Lo scopo di tale previsione viene identificato dalla dottrina nel rafforzamento dell'effetto deterrente verso l'uso improprio dei sistemi di intelligenza artificiale[602]

[599] Secondo F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*, par. 3 detta modifica ha l'obiettivo precipuo "modernizzare lo 'standard dell'*intent*"", che infatti si ritiene "integrato sulla base di una vera e propria presunzione di conoscenza e volontà che impedisce a qualunque *deployer* (fornitore) anche indiretto di AI in ambito finanziario di addurre l'ignoranza delle azioni del *software*".

[600] Sec. 42(b).

[601] La proposta fa riferimento all'art. 21(d)(3) del Securities Exchange Act, secondo cui l'ammontare delle sanzioni civili previste dal subpar. (A) non devono superare "il limite della sanzione altrimenti determinata ai sensi delle clausole (i), (ii), o (iii) della lettera (B)". S.C. 3024), non supererà il triplo della sanzione altrimenti determinata ai sensi della clausola (i), (ii) o (iii) della lettera (B)" (traduzione nostra).

[602] F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*, par. 3, secondo cui a tale previsione è sottesa l'idea che esistano strumenti afflittivi non penali che possono assolvere a una funzione di "intimidazione, ammonimento e orientamento sociale", scoraggiando l'uso dannoso dell'AI nei mercati finanziari.

1.2. I doveri del Financial Stability Oversight Council

Quanto al Financial Stability Oversight Council[603], si attribuisce a tale ente il compito di svolgere analisi[604] e proporre raccomandazioni[605] riguardo ai

---

[603] Agenzia governativa federale che ha il compito di i) identificare, valutare e monitorare eventuali rischi sistemici per la stabilità del sistema finanziario; ii) svolgere comunicazione con il pubblico riguardo a tali rischi; iii) favorire la cooperazione e la comunicazione tra le agenzie partecipanti al consiglio su questioni relative alla stabilità finanziaria.

[604] Il Financial Stability Oversight Council "coordina l'Ufficio di Ricerca Finanziaria, al fine di:

1) condurre una ricerca sull'uso dell'intelligenza artificiale da parte delle istituzioni finanziarie e degli enti che forniscono servizi o svolgono funzioni per conto delle istituzioni finanziarie;
2) identificare le minacce alla stabilità del sistema finanziario poste dall'uso di strumenti e tecnologie di intelligenza artificiale, quali:
    a) la generazione e l'uso di false rappresentazioni o simulazioni di eventi, discorsi o azioni di persone da parte di agenti malevoli volte a manipolare i mercati o gli strumenti finanziari o per causare perturbazioni nei mercati finanziari;
    b) qualsiasi altro atto o pratica associati all'uso o al supporto di strumenti o tecnologie di intelligenza artificiale che minacciano la stabilità del sistema finanziario;

   presentare – entro 180 giorni dalla data di entrata in vigore della presente sezione, in consultazione con le agenzie affiliate, le istituzioni finanziarie, i partecipanti al mercato dei valori mobiliari e le entità che forniscono servizi o svolgono funzioni per conto delle istituzioni finanziarie o dei partecipanti al mercato dei valori mobiliari – alla commissione per gli affari bancari, abitativi e urbani del Senato e alla commissione per i servizi finanziari della Camera dei Rappresentanti una relazione che:
    a) identifica le minacce descritte nel paragrafo 2.
    b) identifica le lacune specifiche nei regolamenti, nelle linee guida e negli standard di esame esistenti delle agenzie associate che impediscono risposte efficaci e complete da parte di ciascuna delle agenzie associate alle minacce descritte nel paragrafo (2);
    c) formula raccomandazioni specifiche per affrontare le lacune identificate nel sottoparagrafo (B), comprese, se del caso, raccomandazioni relative all'attuazione delle raccomandazioni contenute nel foglio informativo sulla sicurezza informatica pubblicato dalla National Security Agency, dal Federal Bureau of Investigation e dalla Cyber security and Infrastructure Security Agency il 12 settembre 2023;" (traduzione nostra).

[605] Il Financial Stability Oversight Council "coordina l'Ufficio di Ricerca Finanziaria, al fine di: […]

3) presentare – entro 180 giorni dalla data di entrata in vigore della presente sezione, in consultazione con le agenzie affiliate, le istituzioni finanziarie, i partecipanti al mercato dei valori mobiliari e le entità che forniscono servizi o svolgono funzioni per conto delle istituzioni finanziarie o dei partecipanti al mercato dei valori mobiliari – alla commissione per gli affari bancari, abitativi e urbani del Senato e alla commissione per i servizi finanziari della Camera dei Rappresentanti una relazione che:
    a) identifica le minacce descritte nel paragrafo 2.

potenziali rischi per la stabilità l'integrità del sistema finanziario posti dall'uso dell'intelligenza artificiale.
L'azione, basata sullo studio delle transazioni che avvengono sui mercati, del Financial Stability Oversight Council è, cioè, finalizzata a un governo informato delle effettive minacce alla stabilità del mercato poste dall'uso di sistemi di intelligenza artificiale.
L'idea di fondo sembra dunque essere quella che le analisi condotte in relazione agli usi che di tali sistemi fanno i principali attori del mercato sia possibile definire in modo compiuto quali siano le potenziali minacce e vulnerabilità emergenti.
Si tratta, in definitiva, della stessa necessità sottesa all'ipotesi di riconsiderazione dell'area del rischio consentito – sulla base di un nuovo bilanciamento fra rischi e benefici – che si auspicava con riferimento al sistema italiano.

1.3. Un bilancio sulla soluzione americana

La proposta di FAIRR Act – la cui *ratio* fondamentale è obbligare tutti i soggetti coinvolti nel processo di implementazione di un sistema di intelligenza artificiale a "soddisfare una serie di requisiti tecnici pensati per assicurare il contenimento del rischio finanziario illecito"[606] – sebbene tuttora in fase di approvazione, è stata oggetto di alcune osservazioni anche da parte della dottrina italiana, che ne ha fornito un giudizio parzialmente positivo.
Se da un lato, secondo le prime letture, il testo è stato accolto con favore nella parte in cui, prevedendo una riconsiderazione delle regole in responsabilità del

b) identifica le lacune specifiche nei regolamenti, nelle linee guida e negli standard di esame esistenti delle agenzie associate che impediscono risposte efficaci e complete da parte di ciascuna delle agenzie associate alle minacce descritte nel paragrafo (2);
c) formula raccomandazioni specifiche per affrontare le lacune identificate nel sottoparagrafo (B), comprese, se del caso, raccomandazioni relative all'attuazione delle raccomandazioni contenute nel foglio informativo sulla sicurezza informatica pubblicato dalla National Security Agency, dal Federal Bureau of Investigation e dalla Cyber security and Infrastructure Security Agency il 12 settembre 2023;

4) individuare, se del caso, le opportunità di uso delle tecnologie di intelligenza artificiale nella regolamentazione e nella vigilanza finanziaria, specificando che qualsiasi uso dell'intelligenza artificiale da parte delle agenzie nella regolamentazione e nella vigilanza dovrebbe essere trasparente e divulgato ai soggetti regolamentati, come opportuno." (traduzione nostra).

[606] Così F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*, par. 3.

programmatore, ha trovato una soluzione che potrebbe "colmare il ben noto *responsibility gap* in materia"[607]; dall'altro se ne sono rilevate alcune criticità.

In particolare, si è notato che "il meccanismo mira evidentemente a contrastare le frodi autonomamente generate dall'AI, attraverso i propri processi di apprendimento e decisionali: ritenendo responsabili gli sviluppatori e i distributori per le azioni della loro creatura informatica, si rimprovera loro, in sostanza, di non aver per tempo assunto azioni preventive adeguate".

La soluzione individuata dal FAIRR Act tuttavia è stata criticata perché eccessivamente severa e dunque foriera del rischio di una sorta di 'ricerca difensiva'[608], dal momento che gli sviluppatori, anche "dimostrando la massima cura nella progettazione e realizzazione del software, […] non potrebbero in alcun modo scampare alla sanzione"[609].

A questi rilievi, con riferimento alla questione affrontata nel presente lavoro, si potrebbe aggiungere una breve considerazione sulla replicabilità della 'soluzione americana' nell'ordinamento *penale* italiano, con particolare riferimento alle regole di attribuzione della responsabilità alla persona 'dietro alla macchina'.

Sebbene costituiscano un apprezzabile tentativo di risolvere l'ormai annosa questione del *liability gap*, la presunzione di sussistenza dell'elemento soggettivo e il meccanismo di *fictio* contenute nel FAIRR Act, così come attualmente formulate, non potrebbero essere utilizzate a modello della responsabilità *penale* nostrana.

Nella formulazione americana c'è infatti un 'grande assente': il principio di colpevolezza[610]. Sia la presunzione – apparentemente invincibile – di rimproverabilità, sia il meccanismo di trasposizione dell'agire artificiale in capo all'agente umano tradiscono infatti un rimprovero di natura oggettiva, inconciliabile con i principi fondamentali in materia penale.

Ciò tuttavia non toglie che la proposta americana possa essere un modello, anche al di qua dell'oceano, per sanzionare le condotte abusive tramite strumenti

---

[607] Così F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*, par. 3. Sul concetto di *responsibility gap*, A. MATTHIAS, *The responsibility gap: Ascribing responsibility for the actions of learning automata*, in Ethics and Information Technology, 2004, Vol. 6, Issue 3, par. 4.

[608] Volendo mutuare il termine dall'ambito medico.

[609] F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*, par. 3 ritiene la scelta "discutibile, se non controproducente, poiché disincentiva la ricerca e la messa in opera di tutele e meccanismi di sicurezza".

[610] La letteratura sul punto è, come noto, vastissima: per sintesi e senza pretesa di esaustività, si rinvia, F. BASILE, Principio di colpevolezza e responsabilità oggettiva, in R. Garofoli, T. Treu, Il libro dell'anno del diritto 2013, Roma, Treccani, 2013.

diversi da quello penale ma non meno efficaci in termini di preventivi, come condivisibilmente auspicato dalla dottrina[611].

A tal proposito, occorre notare che qualora si dovesse guardare alla sanzione amministrativa quale strumento per punire le condotte abusive, la Cassazione ha osservato che per gli illeciti amministrativi "il giudizio di colpevolezza è ancorato a parametri normativi estranei al dato puramente psicologico […] con la conseguenza che, una volta integrata e provata dall'autorità amministrativa la fattispecie tipica dell'illecito, grava sul trasgressore, in virtù della presunzione di colpa posta dall'art. 3 della l. 24 novembre 1981, n. 689, l'onere di provare di aver agito in assenza di colpevolezza"[612].

2. Gli algoritmi di *trading* basati su sistemi di intelligenza artificiale c.d. 'forte' *e* il nuovo capitolo della 'società del rischio'

Riportando la prospettiva al contesto domestico, le considerazioni svolte in ordine alla possibile rilevanza penale dell'agire abusivo degli algoritmi di *trading* portano dunque a ipotizzare l'affacciarsi di nuova fase della moderna 'società del rischio', in cui l'intelligenza artificiale costituisce il nuovo ambito di applicazione della categoria del rischio consentito[613] e dell'approccio alla

---

[611] F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*, par. 3.

[612] Cass. Pen., Sez. V, 9 gennaio 2020, n. 397; nello stesso senso Cass. Pen., Sez. V, 31 ottobre 2018, n. 49869. Tale argomento secondo S. Seminara, *Diritto penale commerciale*, *op. cit.*, p. 94 va fermamente respinto. L'Autore, nel sostenere la responsabilità esclusivamente dolosa – e non anche colposa –anche per l'art. 187 *bis* t.u.f., sostiene che "l'illecito in esame, anche sul versante amministrativo, non può prescindere dalla consapevolezza della natura privilegiata dell'informazione, necessaria perché possa parlarsi di un suo utilizzo, e tale requisito non ha nulla a che vedere con la 'suità' dell'azione, attendendo invece al dolo". Sulla natura colposa dell'illecito amministrativo si veda tuttavia *supra* cap. II, par. 3.3.

[613] Sull'utilità del riferimento a questa categoria, nella dottrina più recente si contrappongono due visioni. Una prima – F. CONSULICH, *Rischio consentito*, *op. cit.*, p. 1135 –, più scettica, ritiene che l'utilità del concetto sia "oggi ridotta, confinata, sul piano dell'interpretazione della fattispecie e, dal punto di vista politico-criminale, della legittimazione delle attività pericolose e della discrasia che esse presentano fra offesa sostanziale e liceità formale della conodtta dell'agente". A questa si contrappone l'idea secondo cui sarebbe invece opportuno valorizzare il rischio consentito "in chiave limitatrice della responsabilità penale […] per impedire che l'imputazione di eventi lesivi derivati da attività strutturalmente pericolose si riduca a mero automatismo, cioè ad una forma occulta di responsabilità oggettiva", così S. ZIRULIA, *Esposizione a sostanze tossiche*, *op. cit.*, p. 339.

gestione e prevenzione del rischio che caratterizza da tempo numerosi settori dell'agire umano[614].

Pur muovendoci in contesi nei quali i meccanismi di causazione dell'abuso di mercato potrebbero non essere del tutto ricostruibili[615], allo stato attuale non sussiste un espresso divieto di utilizzazione di algoritmi di *trading* basati su sistemi di intelligenza artificiale 'forte'[616].

Ciò comporta che anche con riferimento agli algoritmi di *trading* basati su sistemi di intelligenza artificiale c.d. 'forte' – così come si è fatto per gli algoritmi di *trading* 'tradizionali' – il ragionamento deve seguire le logiche illustrate.

La premessa necessaria della tesi qui proposta è che i sistemi di negoziazione algoritmica 'forti' sono sì dotati della capacità di "autoapprendere, sono ontologicamente *imprevedibili*. Solo che *questa connaturata imprevedibilità è a sua volta* prevedibile da parte del costruttore"[617].

Dunque, escluse le ipotesi in cui si può muovere un rimprovero doloso in riferimento all' 'abuso di mercato algoritmico', si possono immaginare scenari in cui l'abuso di mercato sia il risultato di un atteggiamento colposo dell'umano che

---

[614] Primo fra tutti il settore ambientale, terreno dell'elezione del principio di precauzione, che, come nota G. FORTI, *"Accesso" alle informazioni*, *op. cit.*, pp. 160 ss "ha trovato la sua più nota e citata formulazione al Principio 15 della Dichiarazione sull'Ambiente e lo Sviluppo (resa alla Conferenza delle Nazioni Unite, riunita a Rio de Janeiro dal 3 al 14 giugno 1992)"; nonché nel Trattato che istituisce la Comunità europea (art. 174, secondo comma) e, tra l'altro, nella Comunicazione della Commissione sul principio di precauzione, *cit*. Anche in questo caso, infatti, il bilanciamento fra libertà e diritti degli individui, industrie e organizzazioni ed esigenza di riduzione dei i rischi di effetti negativi per l'ambiente e per la salute degli esseri umani, degli animali e delle piante avviene sulla base di informazioni non sufficienti, conclusive o certe. Anche in quel contesto, cioè, si discute della possibile presa in considerazione dell'incertezza scientifica nell'analisi del rischio e, in particolare se tale presa di posizione deve essere effettuata nella valutazione e nella gestione del rischio (punto 5 della Comunicazione).

[615] Si tratta dello stesso problema che rileva C. RUGA RIVA, *Il principio di precauzione*, *op. cit.*, p. 1765 nel caso delle patologie di cui si suppone la correlazione all'esposizione a determinate sostanze.

[616] Opzione che rimane nel novero delle possibili scelte politico-criminali che il legislatore potrebbe prendere, pur con le dovute cautele in termini di progresso scientifico e tecnologico e considerati attentamente i potenziali benefici l'utilizzo di tali sistemi può apportare ai mercati e all'economia. Cfr. A. CAPPELLINI, Machina delinquere non potest?, *op. cit.*, p. 516. Questa sarebbe un'opzione obbligata se si ritenesse che si tratta di un tipo di produzione per cui non esistono meccanismi idonei a contenere il rischio entro un limite tollerabile. Tale valutazione, rispetto ad attività rispetto alle quali non vi è certezza scientifica, pare particolarmente problematica perché rischia di avere un effetto inaccettabile – seguendo la logica costi/benefici sopracitata – sulla libera iniziativa economica e sul progresso tecnologico che può comportare benefici alla società intera. Sulla necessità di bilanciare questi interessi, con riferimento all'operatività dei sistemi di intelligenza artificiale 'forte' F. CONSULICH, *Intelligenza artificiale e reati finanziari*, *op. cit.*, p. 261.

[617] C. PIERGALLINI, *Intelligenza artificiale*, *op. cit.*, p. 1759.

lo utilizza e debba quindi *rebus sic stantibus* essere sanzionato come illecito amministrativo.

L'abuso di mercato può essere la conseguenza della mancata adozione di regole precauzionali ulteriori rispetto a quelle codificate, che non risultino più adeguate rispetto all'evoluzione tecnologica di settore[618].

Ovvero si può rimproverare di non essersi astenuto dall'utilizzo di strumenti la cui capacità di causare l'illecito non potesse essere controllata adottando ulteriori misure precauzionali.

In contesti di particolare incertezza scientifica, il parametro sulla base del quale si può muovere un rimprovero per colpa è certamente quello della sufficiente univocità dei segnali di fallimento della regola cautelare. In questo, la particolare preparazione di cui dispone il '*trader* algoritmico modello' influisce, innalzandola, sulla diligenza imposta.

Il rimprovero per colpa deve tenere necessariamente conto della prevedibilità *ex ante* del fallimento delle regole che disciplinano l'attività di negoziazione algoritmica e delle ulteriori cautele fondate sul dovere di diligenza che incombe sul soggetto che utilizza l'algoritmo e che, in quanto tale, è dotato di un *know-how* e di un potere informativo particolarmente qualificato[619].

Il giudizio sulla prevedibilità o meno del fallimento della regola cautelare e il conseguente *standard* di diligenza imposto deve tenere conto del fatto che chi effettua *trading* algoritmico – in qualità di soggetto dotato delle risorse economiche necessarie per predisporre o sviluppare programmi di ricerca o comunque di soggetto che opera in settori ad elevata innovazione tecnica e

---

[618] Qualora il soggetto versi in situazione di dubbio, occorre considerare che, secondo C. RUGA RIVA, *Principio di precauzione*, *op. cit.*, p. 1761, mentre in contesti di *certezza* scientifica il dubbio su di un dato di realtà è di regola compatibile con il momento rappresentativo del dolo – essendo sufficiente ai fini del dolo eventuale che l'agente si rappresenti il verificarsi dell'evento come seriamente possibile, posto che "in contesti di certezza scientifica il dubbio riguarda solo la circostanza del concreto verificarsi dell'evento nel mondo reale" in contesti di *incertezza* scientifica, quando il dubbio attiene innanzitutto l'astratta attitudine causale della condotta a realizzare l'evento lesivo, ancor prima che il suo concreto realizzarsi, il serio dubbio sulle conseguenze offensive della propria condotta, secondo la dottrina, "sembra poter integrare la prevedibilità nell'ambito della colpa"[618]. Ciò dipenderebbe proprio dalla duplice incertezza: "non si sa con certezza se una data condotta causerà determinati eventi nel mondo reale, posto che si è in dubbio circa la plausibilità che una determinata congettura scientifica che correla gli eventi osservati alla condotta «sospetta»"

[619] Peraltro, mutuando il pensiero di G. FORTI, *"Accesso" alle informazioni*, *op. cit.*, p. 195, di fronte a un mutamento dei rischi derivanti dal diffondersi di sistemi basati su intelligenza artificiale 'forte', sul soggetto grava anche un dovere di rendere edotta la parte pubblica di tutte le conoscenze che potrebbero modificare l'originaria valutazione sull'area di rischio consentito.

tecnologica – è gravato da un obbligo di approfondimento scientifico rispetto al proprio campo di attività e ai rischi ad essa connessa. Se tale approfondimento "alimenta il dubbio sulla pericolosità della condotta consentendo di ipotizzare determinate correlazioni causali, o di affermare determinate frequenze statistiche"[620], su tale dubbio si baserà il giudizio di responsabilità.

La responsabilità del soggetto che utilizza il sistema di negoziazione algoritmica 'forte' potrà dunque essere affermata se si ritiene abbia tenuto un comportamento colposo.

Ciò non toglie che, di fronte a un'evoluzione così significativa dei sistemi si possa ritenere preferibile una rivalutazione da parte del legislatore delle regole che governano l'attività di negoziazione algoritmica. Le regole che, rispetto ai sistemi 'tradizionali' parevano adeguate a evitare che gli algoritmi realizzassero strategie abusive possono infatti, oggi, mostrare la loro obsolescenza, non colmabile tramite l'imposizione di *standard* di diligenza più elevati agli operatori.

Questi ultimi, tuttavia, potrebbero acquisire un ruolo fondamentale nella nuova valutazione dei rischi connessi all'utilizzo di sistemi sempre più intelligenti, dando vita a un processo di democratizzazione della valutazione del rischio, auspicato dalla dottrina[621] . L'estensione dell'area del rischio consentito sarebbe, in questo modo, il frutto di uno scambio fra settore pubblico e settore privato, che nell'ambito dei "moderni rischi tecnologici"[622] è indubbiamente dotato di conoscenze superiori.

La collocazione del dibattito sulla rilevanza penale del *trading* algoritmico entro i confini del rischio consentito pare quindi dimostrare la tenuta del sistema e l'applicabilità categorie tradizionali del reato anche all'ambito del '*market abuse* algoritmico'.

Alla luce dell'analisi dell'attuale contesto dei mercati finanziari, dell'evoluzione degli strumenti di *trading* e della diffusione di sistemi sempre più sofisticati dal punto di vista tecnologico appare chiaro l'affacciarsi di una nuova epoca della società del rischio, caratterizzata da un nuovo atteggiarsi dei rapporti fra produzione sociale della ricchezza e produzione sociale dei rischi[623].

---

[620] C. RUGA RIVA, *Principio di precauzione*, *op. cit.*, p. 1763.

[621] C. PIERGALLINI, *Intelligenza artificiale*, *op. cit*., pp. 1772-1773, nonché G. FORTI, *"Accesso" alle informazioni*, *op. cit.*, p. 155 ss e 164.

[622] G. FORTI, *"Accesso" alle informazioni*, *op. cit.*, p. 217.

[623] Sul punto si veda l'ampia ricostruzione di C. PIERGALLINI, *Danno da prodotto*, op. cit., pp. 480-521.

Pur trattandosi di sistemi dotati di indubbie componenti di innovatività, ad essi si possono applicare *mutatis mutandis* i canoni elaborati con riferimento alla produzione industriale, ai rischi ambientali, ai danni alla salute derivante dall'esposizione a sostanze tossiche, senza sottovalutare il fatto che, ancor più dei precedenti, i nuovi rischi associati all'utilizzo di sistemi di intelligenza artificiale 'forte' nel *trading* hanno una dimensione globale e degli effetti maggiori, che talvolta sfuggono alla percezione immediata dell'uomo[624].

Tale prospettiva consente peraltro di lasciare in sottofondo altre soluzioni – suggestive, ma non altrettanto convincenti e soprattutto elaborate con riferimento a settori differenti da quello finanziario[625] – per evitare che il coinvolgimento degli algoritmi nella commissione di abusi di mercato finisca per risultare impunita,

---

[624] Il riferimento è all'opera di U. BECK, *La società del rischio*, *op. cit*.,, analizzata, fra gli altri, da C. PIERGALLINI, *Danno da prodotto*, op. cit., pp. 4-11.

[625] Ci si riferisce, in particolare, alle seguenti tesi,:

a) la posizione di garanzia (elaborata specialmente con riferimento ai reati di omicidio o lesioni causate dall'automobile a guida autonoma). Cfr. C. PIERGALLINI, *Intelligenza artificiale*, *op. cit.*, p. 1753, "poiché si è dinnanzi a mezzi automatizzati che, comunque soggiacciono al controllo umano, è da intravedere nella figura del conducente il soggetto obbligato a controllare il veicolo e quindi impedire i danni ai terzi. Si prefigura una posizione di garanzia, funzionalmente inquadrabile nella categoria delle posizioni di controllo, imperniata sul governo della fonte di pericolo". Nello stesso senso A. CAPPELLINI, *Profili penalistici*, *op. cit.*, p. 334. La tesi non pare applicabile però agli abusi di mercato, come detto, sono fattispecie di mera condotta che non richiedono la realizzazione di un evento che il soggetto umano avrebbe l'obbligo giuridico di impedire;
b) l'autoria mediata, ipotizzando un concorso fra soggetti di natura diversa: l'umano, che pone in essere la condotta atipica, e la 'macchina', che realizzerebbe la condotta tipica. Si tratta tuttavia di una tesi che presuppone la possibilità di applicare le regole del concorso di persone nel reato a soggetti che non sono umani. Di fatto, è auna soluzione che, ancora una volta, finisce per colmare il vuoto dell'arretratezza del diritto contemporaneo ipotizzando un meccanismo di imputazione della responsabilità esclusivamente all'uomo che sfrutta a fini illeciti l'interazione con un'intelligenza artificiale, benché questi non sia non autore diretto del fatto, come rilevano F. Consulich, *Flash offenders, op. cit.*, pp. 1033-1034 e F. CONSULICH–M. MAUGERI–C. MILIA–T.N. POLI–G. TROVATORE, *AI e abusi di mercato*, *op. cit.*, p. 90.
c) Una responsabilità indipendente, ma che richiede il fatto dell'individuo, secondo il meccanismo di cui all'art. 8 d.lgs. 231/2001, che permette di sanzionare l'ente anche qualora sia ignoto l'autore del reato. Cfr. F. CONSULICH, Flash offenders, *op. cit.*, p. 1042. Tale opzione, pur astrattamente adeguata ad affrontare le problematiche connesse con l'uso dei sistemi algoritmici 'forti' dovrebbe passare per una modifica *de lege ferenda*.

prime fra tutte le inaccettabili ipotesi del superamento del dogma *machina delinquere non potest*[626] o della responsabilità oggettiva dell'uomo[627].

3. Una possibile prospettiva *de iure condendo*

L'analisi e le considerazioni sin qui svolte si collocano, evidentemente, in una prospettiva *de iure condito* che, tuttavia, non può esimere dallo sviluppare alcune considerazioni *de iure condendo*.

Pur ritenendosi che l'attuale sistema non crei inaccettabili vuoti di tutela rispetto ad 'abusi di mercato algoritmici' commessi tramite l'utilizzo di sistemi di negoziazione basati su intelligenza artificiale 'forte', parrebbe opportuno un intervento legislativo in una duplice direzione.

Da un lato, il legislatore dovrebbe rivalutare l'adeguatezza delle regole che governano l'attività di negoziazione algoritmica in relazione a tecnologie che allo stato attuale non hanno la stessa diffusione degli algoritmi di *trading* 'tradizionali', ma di cui si può prospettare il prossimo utilizzo.

Tale rivalutazione dovrebbe tenere nella dovuta considerazione le istanze di progresso tecnologico e considerare se ed entro quali limiti privilegiare la sanzione penale anziché quella amministrativa[628].

---

[626] L. PICOTTI, *Ente*, *op. cit.*, p. 10 "dal punto di vista del diritto penale si impone una risposta negativa alla questione se si possa ipotizzare un'autonoma responsabilità dell'"ente" artificiale come tale, tanto più se portasse addirittura ad escludere quella degli uomini (od "enti" collettivi) che gli "stanno dietro", visto che in mancanza di una personalità e volontà propria, anche la minaccia ed irrogazione di sanzioni non avrebbe senso, dovendo piuttosto essere funzionale ad incidere sul comportamento futuro delle persone fisiche o degli "enti" collettivi che vi stanno dietro".

[627] La responsabilità oggettiva è stata prospettata, invero, solo dalla dottrina di *common law*, cfr. R. CALO, *Robotics and the Lessons of Cyberlaw*, in California Law Review, 2015, vol. 103, issue 3, pp. 554-563.

[628] Sulla necessità di bilanciare questi interessi, con riferimento all'operatività dei sistemi di intelligenza artificiale 'forte' F. CONSULICH, *Intelligenza artificiale e reati finanziari*, *op. cit.*, p. 261. Inoltre, come si è già notato *supra* (cap. I par. 1 nt. 223), l'equilibrio fra innovazione tecnologica e tutela dei diritti fondamentali è alla base della Decisione quadro sull'intelligenza artificiale del Consiglio d'Europa.

Sul ricorso alla sanzione penale, L. PICOTTI, *Categorie tradizionali del diritto penale*, *op. cit.*, p. 8 evidenzia che la Resolution on traditional criminal law categories and AI ha individuato nel diritto penale lo strumento adatto a prevenire e punire i reati commessi da o tramite sistemi di intelligenza artificiale, "muovendo dalla riconosciuta necessità di proteggere, anche con sanzioni penali da minacciare ed applicare a persone umane (fisiche o anche giuridiche), i diritti fondamentali ed i beni giuridici che vengano offesi tramite sistemi di intelligenza artificiale, o con aggressioni a loro danno, visto che tali beni giuridici già beneficiano di una tutela penale che, per la loro meritevolezza, è ritenuta necessaria dagli ordinamenti vigenti".

Dall'altro lato, parrebbe auspicabile un'estensione delle fattispecie di manipolazione del mercato e abuso di informazioni privilegiate, capaci di presidiare con la sanzione penale anche forme di abuso di mercato commesse per colpa.

In proposito, si è dato conto del fatto che l'utilizzo gravemente negligente di algoritmi di *trading* possa dare vita a *crash* di mercato che possono comportare conseguenze estremamente gravose per i mercati finanziari[629].

A fronte di simili ipotesi, occorre dunque interrogarsi sull'opportunità di mantenere il solo presidio amministrativo, per quanto riconducibile alla c.d. *matière pénale*[630].

Pur nella consapevolezza che la sanzione amministrativa, nella sua gradualità e flessibilità, possa risultare certamente adeguata alle specificità del contesto finanziario[631], il Regolamento MAR e la Direttiva MAD II propongono "una decisa valorizzazione dello strumento penale"[632] per la punizione di condotte connotate da particolare gravità.

Rispetto a queste ultime, dunque, occorre chiedersi se sia opportuna una rinuncia *tout court* al magistero punitivo penale[633], considerata la significativa portata offensiva del comportamento.

Le gravi turbative di mercato derivanti da condotte colpose si collocherebbero proprio entro quei casi 'gravi' – insieme alle ipotesi commesse con dolo – rispetto ai quali il legislatore eurounitario individua nella sanzione penale la strumento di contrasto più idoneo.

In questi casi, cioè, l'utilizzo dello strumento automatizzato sarebbe in grado di qualificare il comportamento, pur colposo, in termini più gravi e dotandolo dunque

---

[629] Ci si riferisce, solo per citare alcuni esempi, agli episodi del maggio 2010 nel caso Navinder Sarao che ha interessato il Dow Jones Industrial Average; del 2012 relativo al caso Knight Capitale; del 15 ottobre 2014 c.d. *Great Treasury flash crash*, del settembre 2015 sull'indice FTSE 100 legato a un caso di *fat finger*, che hanno dimostrato come l'utilizzo di algoritmi di *trading* sia una delle principali cause dei *flash crash*. Episodi che F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*, par. 1 definisce "violenti eventi manipolativi".

[630] I contributi sul tema sono, come noto, amplissimi. Senza pretesa di esaustività si rinvia, in particolare a L. MASERA, La nozione costituzionale di materia penale, Torino, Giappichelli, 2018; F. MAZZACUVA, *Le pene nascoste*, Torino, Giappichelli, 2017.

[631] In questo senso, F. CONSULICH, *Manipolazione dei mercati*, *op. cit.*, p. 204; nonché ID, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*, par. 3.

[632] Così F. D'ALESSANDRO, *La manipolazione del mercato*, *op. cit.*, p. 198.

[633] D'altronde, come sottolinea F. CONSULICH, Flash offenders, *op. cit.*, p. 1020, da più parti si avanza l'auspicio di un controllo più severo da parte del diritto, che impieghi anche la sanzione penale, di fronte ai fatti che coinvolgono strumenti di intelligenza artificiale.

di una capacità offensiva di rilievo – anche formalmente – penale e imponendo, di conseguenza, un adeguamento della fattispecie nei seguenti termini.

Art. 185 t.u.f.[634]
Chiunque, diffonde notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, è punito con la reclusione da due a dodici anni e la multa da euro ventimila a cinque milioni.
Se nella realizzazione dei fatti previsti dal presente articolo l'agente si avvale di uno strumento automatizzato o dei sistemi di cui all'art. 3, n. 1) del Regolamento (UE) 2024/1689, la pena è aumentata[635].

Art. 185 *bis* t.u.f.
Qualora i fatti di cui all'art. 185 siano realizzati per colpa, avvalendosi di uno strumento automatizzato o dei sistemi di cui all'art. 3, n. 1) del Regolamento (UE) 2024/1689 si applica la pena della reclusione da tre mesi a quattro anni e con la multa euro diecimila fino a euro un milione e seicentomila.

Art. 184 t.u.f.[636]
1. È punito con la reclusione da due a dodici anni e con la multa da euro ventimila a euro tre milioni chiunque essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo di un 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:

a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;
b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato effettuato ai sensi dell'articolo 11 del regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014;

[634] Le previsioni dei commi successivi rimangono invece immutate.
[635] La previsione di un aumento di pena sarebbe giustificata dalla maggiore gravità dei comportamenti posti in essere tramite sistemi automatizzati.
[636] Le previsioni dei commi 2-5 rimangono invece immutate.

c) raccomanda o induce altri, sulla base di tali informazioni, al compimento di taluna delle operazioni indicate nella lettera a).

Se i fatti di cui al presente articolo sono realizzati avvalendosi di uno strumento automatizzato o dei sistemi di cui all'art. 3, n. 1) del Regolamento (UE) 2024/1689, la pena è aumentata.

Art. 184 *bis* t.u.f.

Qualora i fatti di cui all'art. 184 sono realizzati per colpa, avvalendosi di uno strumento automatizzato o comunque dei sistemi di cui all'art. 3, n. 1), del Regolamento (UE) 2024/1689, si applica la pena con la reclusione da tre mesi a quattro anni e con la multa da euro cinque mila a euro un milione.

Si tratterebbe, in buona sostanza, di introdurre un riferimento all'operatività dei sistemi automatizzati nelle attuali fattispecie facendo ricorso a una clausola generale capace di abbracciare tutte le tecnologie che nel futuro potrebbero operare nei mercati e affiancare alla già esistente ipotesi dolosa una fattispecie colposa autonoma, in cui l'agente fisico risponde per non aver per non aver predisposto le cautele necessarie a prevenire alterazioni *significative* del prezzo degli strumenti finanziari.

L'introduzione della fattispecie penale colposa realizzata tramite l'utilizzo di sistemi algoritmici o sistemi automatizzati, giustificata dalla maggiore offensività di detti comportamenti, comporterebbe la necessità dell'inserimento nella fattispecie amministrativa di una clausola di sussidiarietà che escluda la sanzione amministrativa nel caso in cui il fatto sia commesso utilizzando tali sistemi.

Per tale via, peraltro, si giungerebbe a una valorizzazione della funzione delle sanzioni stesse, nella loro accezione general preventiva – quali strumenti di disincentivo alla violazione di norme giuridiche – scongiurando la possibilità che la sanzione amministrativa pecuniaria venga considerata, più che altro, un 'costo' da pagare per lo svolgimento dell'attività[637].

[637] Con ciò evidentemente non si intende negare la necessità di costruzione di un apparato di soluzioni diversificate – non appiattito esclusivamente sulla sanzione penale – che abbiano un effetto altrettanto preventivo e deterrente, che tuttavia dovrebbero affiancare la sanzione penale con riferimento a casi connotati da minore gravità.

Tale obiettivo, secondo L. CORNACCHIA, *Responsabilità colposa*, *op. cit.*, pp. 16-17 può essere perseguito tramite l'adozione di misure di natura amministrativa o civilistica, oltre che in generale attraverso un ripensamento della responsabilità in termini di *compliance individuale* (tramite, incentivo di "comportamenti conformi agli standard cautelari, anche mediante modelli preventivi

Inoltre, il riconoscimento della rilevanza penale dei comportamenti colposi avrebbe l'ulteriore merito di scongiurare il rischio di stravolgimento della categoria del dolo eventuale talora operato dalla giurisprudenza per i casi in cui non esiste una corrispondente ipotesi colposa"[638]. Tale opzione legislativa consentirebbe, cioè, di limitare la tendenza a considerare rappresentati e voluti dall'agente fatti che, al più, questi *avrebbe dovuto e potuto* rappresentarsi, ma che in effetti non ha voluto.

La soluzione qui prospettata, infine, si inserirebbe in un più ampio processo di crescente valorizzazione della colpa auspicato dalla dottrina con riferimento all'azione dei sistemi di intelligenza artificiale[639].

---

calibrati sulla categoria professionale, sulla sfera di rischio che viene gestita, sul rango del bene protetto" e "cercando di rintuzzare le prassi diffuse negligenti, attraverso accertamenti rapidi delle violazioni anche tramite utilizzo di strumentazioni tecnologiche (ad esempio, prevedere pene elevate e anche sanzioni amministrative […])". Adottando quest'ottica tuttavia occorre evitare il rischio – sempre presente in materia di abusi di mercato – della ben nota 'frode delle etichette' e di creare, di fatto, sanzioni che pur formalmente amministrative hanno natura sostanzialmente penale. Si tratterebbe in questo caso di una soluzione solo apparentemente deflattiva, ma nella sostanza foriera di problematicità ormai ben note e di dubbia compatibilità con i principi fondamentali nazionali e sovranazionali.

[638] Così G. MARINUCCI–E. DOLCINI–G.L. GATTA, *Manuale di diritto penale*, *op. cit.*, p. 401. Inoltre, come rileva F. CONSULICH, Flash offenders, *op. cit.*, pp. 1049-1050 "se l'imputazione dolosa è tendenzialmente inattivata dalla distanza tra fatto concreto compiuto dall'agente artificiale e generiche istruzioni lesive inserite dal programmatore […], quella colposa consente di riconoscere nella negligenza la creazione di un rischio non schermato: se lo specifico evento storico appartiene alla classe di eventi dannosi che potevano essere ipotizzati al momento della creazione del sistema intelligente, vi sono i presupposti per il riconoscimento della responsabilità".

[639] F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale*, *op. cit.*, par. 8 e prima in ID, Flash offenders, *op. cit.*, pp. 1051-1055. Sulla necessità di un ripensamento dell'illecito penale colposo L. CORNACCHIA, *Responsabilità colposa: irrazionalità e prospettive di riforma*, in Arch. Pen., 12 luglio 2022, scettico sulla "criteriologia sinallagmatica danno-centrica" e puramente intimidatoria che caratterizza l'attuale reazione penale ai comportamenti colposi. Al contrario, l'Autore propone di delimitare la responsabilità colposa alle forme di manifestazione più gravi e di rimodulare la responsabilità colposa, da un lato, sanzionando i comportamenti irrispettosi degli standard cautelari cristallizzati dall'esperienza, ma "evitano comunque *in generale* […] di utilizzare la pena detentiva a fronte di eventi infausti che si verifichino nonostante il rispetto degli standard stessi, in considerazione della sua scarsa idoneità preventiva" (p. 3) e dall'altro immaginando soluzioni riparatore più adatte a sanzionare il verificarsi di eventi che "costituiscano la conseguenza non prevista di cautele non osservata scrupolosamente".

BIBLIOGRAFIA

ABBOTT R.–SARCH A., *Punishing Artificial intelligence: Legal Fiction or Science Fiction*, in UC Davis Law Review, 2019, vol. 53, issue 1, pp. 323-384.

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

AIMI A., *Il dolo eventuale alla luce del caso* Thyssenkrupp, in Il libro dell'anno del diritto Treccani 2015, 2015, pp. 127-136.

ALESSANDRI A., *Diritto penale e attività economiche*, Bologna, Il Mulino, 2010

ALESSANDRI A., *Impresa e giustizia penale: tra passato e futuro. Un'introduzione*, in Atti del Convegno di studio "Enrico de Nicola", 14 marzo 2008, Milano, 2009, pp. 11-58.

ALESSANDRI A., SEMINARA S., *Diritto penale commerciale*, *vol. I, I principi generali*, Torino, Giappichelli, 2018.

ALVARO S.–VENTORUZZO M., «High-Frequency Trading*»: note per una discussione*, in *Banca impresa e società*, 2016, vol. 35, issue 3, pp.417-444.

AMATI E., *L'abuso o comunicazione illecita di informazioni privilegiate*, in F. Consulich (a cura di), Reati in materia bancaria e finanziaria, Torino, Giappichelli, 2024, pp. 363-390.

AMATI E., *L'abuso o comunicazione illecita di informazioni privilegiate*, in Mazzacuva N.–Amati E. (a cura di), Diritto penale dell'economia, VI ed., Milano, Wolters Kluwer, 2023, pp. 363-390.

AMORE N., *L'effetto della robotica e dell'IA nell'imputazione giuridica degli eventi infausti*, in N. Amore–E. Rossero, Robotica e intelligenza artificiale nell'attività medica. Organizzazione, autonomia, responsabilità, Bologna, 2023, pp. 101-251.

ANGEL J.J.–HARRIS L.E.–SPATT C.S., *Equity Trading in the 21st Century*, 23 febbraio 2010, in Quarterly Journal of Finance, 2011, vol. 1, issue 1, pp. 1-53.

ANNUNZIATA F., *Intelligenza artificiale e disciplina degli abusi di mercato*, in Atti del XV Convegno Nazionale Orizzonti del Diritto Commerciale. 23-24 febbraio 2024, in https://www.orizzontideldirittocommerciale.it/atti-dellanno-2024/, pp. 1-27.

ANNUNZIATA F., *Artificial Intelligence and Market Abuse Legislation A European Perspective*, Edward Elgar, 2023.

ANNUNZIATA F., *I processi di mercato automatizzati e il trading algoritmico*, in Cian M.–Sandei C., *Diritto del Fintech*, Milano, Wolters Kluwer, 2020, pp. 397-408.

ANTOLISEI F., *Manuale di diritto penale (Parte Generale)*, XVI ed., Milano, Giuffrè, 2003.

ARAGONA V., *Il nuovo diritto penale finanziario "algoritmico": dalla rivisitazione delle categorie classiche alla responsabilità della persona fisica attraverso il rischio artificiale consentito*, Tesi di dottorato, 20 luglio 2022, [10.13119/11385_220159],

ASARO P.M., *Determinism, machine agency, and responsibility*, in Politica & Società, 2014, fasc. 2, pp. 265-292.

ASARO P.M., *A body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics*, in P. Lin – K. Abney – G.A. Bekey (eds), Robot Ethics, Harvard Cambridge, University Press, 2012, pp. 169-186.

ASARO P.M., *Robots and Responsibility from a Legal Perspective*, in Proceedings of 2007 IEEE International Conference on Robotics and Automation, 2007, vol. 4., issue 14, pp. 20-24.

AZZUTTI A., *AI-driven Market Manipulation and Limits of the EU law enforcement regime to credible deterrence*, in ILE Working Paper Series, 2022, vol. 45, pp. 1-32.

AZZUTTI A.–RINGE W.G.–STIEHL H.S., *Machine Learning, Market Manipulation, and Collusion on Capital Markets: Why the "Black Box" Matters*, in University of Pennsylvania Journal of International Law, 2021, vol. 43, issue 1, pp. 79-135.

AZZUTTI A.–RINGE W.G.–STIEHL H.S., *Regulating AI Trading from an AI Life Cycle* Perspective, in Remolina N.– Gurrea-Martinez A. (eds.), Artificial Intelligence in Finance: Challenges, Opportunities and Regulatory Developments, Edward Elgar, 2023, pp. 198-243.

BASILE E., Il "doppio binario" sanzionatorio degli abusi di mercato in Italia e la trasfigurazione del *ne bis in idem* europeo, in Giur. comm., 2019, fasc. 1, pp. 129-141.

BASILE E., *Mini-riforma del* market abuse*: obiettivi mancati ed eterogenesi dei fini del d. lgs. n. 107/2018*, in Dir. Pen. Proc., 2018 fasc. 3, pp. 329-337.

BASILE E., *Riforma del* market abuse*: quando la toppa (parlamentare) è peggiore del buco (governativo)*, in Dir. Pen. Cont., Riv. Trim., 2017, fasc. 11, 228-230.

BASILE F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in Dir. Pen. uomo, 2019, fasc. 10, pp. 1-33.

BASILE F., *Principio di colpevolezza e responsabilità oggettiva*, in R. Garofoli, T. Treu, Il libro dell'anno del diritto 2013, Roma, Treccani, 2013.

BASILE F., *Fisionomia e ruolo dell'agente-modello ai fini dell'accertamento processuale della colpa generica*, in G. Bellantoni–D. Vigoni (a cura di), Scritti in onore di Mario Pisani, Piacenza, La Tribuna, 2011, vol. III, pp. 209-242.

BATHAEE Y., *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, in Harvard Journal of Law & Technology, 2018, vol. 31, issue 2, pp. 889-938.

BECK S., *Sinn und Unsinn von Statusfragen von Statusfragen - Zu Vor - und Nachteilen der Einführung einer elektronischen Person. Die Idee subjektiver*

Rechte, in Hilgendorf E.–Zabel B., Robotik und Gesetzgebung, Berlin-Boston, De Gruyter, 2021, pp. 337-360.

BECK S., *Google Cars, Software Agents, Autonomous Weapons Systems – New Challanges for Criminal Law?*, in Hilgendorf E.–Seidel U. (eds.), Robotics, Autonomics and the Law, Baden-Baden, 2017, 227-252.

BECK S., *Intelligent agents and criminal law – Negligence, diffusion of liability and electronic personhood*, in Robotics and Autonomous Systems, 2016, vol. 86, issue 4, pp. 138-143.

BECK U., *Risikogesellschaft. Auf Dem Weg in Eine Andere Moderne*, Suhrkamp, 1986 (ed italiana, *La società del rischio. Verso una seconda modernità*, Roma, Carocci, 2000, a cura di Walter Privitera).

BERTOLESI R., *Intelligenza artificiale e responsabilità penale per danno da prodotto*, 2019, Tesi di dottorato. Dipartimento Di Scienze Giuridiche "Cesare Beccaria". Università degli Studi di Milano, XXXII Ciclo, https://air.unimi.it/handle/2434/711618.

BORSARI R., *Intelligenza artificiale e responsabilità penale: prime considerazioni*, in Media Laws, 2019, fasc. 3, pp. 262-268.

BRICOLA F., *Profili penali della disciplina del mercato finanziario*, in Banca, borsa e tit. cred., 1990, fasc. I, p. 16 poi in Scritti di diritto penale, vol. II, tomo II, Milano, Giuffrè, 1997, p. 3425-3466.

BRICOLA F., *Il problema della responsabilità penale della società commerciale nel diritto italiano*, in La responsabilità delle persone giuridiche, Atti del Convegno, Messina, 1979, pp. 235-263, poi in Scritti di diritto penale, vol. II, tomo II, Milano, Giuffrè,1997, pp. 3089-3120.

BRICOLA F., *Luci ed ombre nella prospettiva di una responsabilità penale degli enti (nei paesi della C.E.E.)*, in Giur. comm., 1979, I, pp. 647-663, poi in Scritti di diritto penale, vol. II, tomo II, Milano, Giuffrè, 1997. pp. 3063-3088

BRICOLA F., *Responsabilità penale per il tipo e modo di produzione*, in AA.VV., La responsabilità per i danni all'ambiente e ai consumatori, Milano, 1978, p. 75 ss poi in *Scritti di diritto penale*, vol. I, tomo II, Milano, Giuffrè, 1997, pp. 1231-1254.

BRICOLA F., *Il costo del principio «societas delinquere non potest» nell'attuale dimensione del fenomeno societario*, in Riv. it. dir. proc. pen., 1970, pp. 951-1031, poi in Scritti di diritto penale, vol. II, tomo II, Milano, Giuffrè, 1997, pp. 2975-3062.

BROGAARD J.A., *High Frequency Trading and its Impact on Market Quality*, in Northwestern University Kellogg School of Management Working Paper n. 66, pp. 1-75.

BURCHARD C., *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in Riv. it. dir. proc. pen., 2019, fasc. 4, pp. 1909-1942.

CALDWELL M.–ANDREWS J.T.A.–TANAY T.–GRIFFIN L.D., *AI enabled future crime*, in Crime Science, 2020, vol. 9, issue 14, pp.1-13.

CAPPELLINI A., *Profili penalistici delle* self-driving cars, in Dir. Pen. Cont. Riv. Trim.,2019, fasc. 2, pp. 325-353.

CAPPELLINI A., Machina delinquere non potest*? Brevi appunti su intelligenza artificiale e responsabilità penale*, in Criminalia, 2018, pp. 499-520.

CAIVANO V., *L'impatto del* trading *ad alta frequenza sulla volatilità. Evidenza empirica sul mercato italiano*, in Consob Quaderno di finanza n. 80, marzo 2015, pp. 1-34.

CAIVANO V.–CICCARELLI S.–DI STEFANO G.–FRATINI M.–GASPARRI G.–GILIBERTI M.–LINCIANO N.–TAROLA I., *Il* trading *ad alta frequenza. Caratteristiche, effetti, questioni di policy*, in *Consob Discussion Papers n.5*, 2012, pp. 1-60.

CALO R., *Robotics and the Lessons of Cyberlaw*, in California Law Review, 2015, vol. 103, issue 3, pp. 513-563.

CANESTRARI S., La distinzione tra dolo eventuale e colpa cosciente nei contesti a rischio di base «consentito», in Dir. Pen. Cont., 6 febbraio 2013, pp. 1-22.

CANESTRARI S., *Dolo eventuale e colpa cosciente*. Ai confini tra dolo e colpa nella struttura delle tipologie delittuose, Milano, Giuffrè, 1999.

CANESTRARI S., *L'illecito penale preterintenzionale*, Padova, Cedam, 1989.

CASTRONUOVO D., *Principio di precauzione e diritto penale. Paradigmi dell'incertezza nella struttura del reato*, Roma, Aracne, 2012.

CASTRONUOVO D., *Principio di precauzione e beni legati alla sicurezza*, in Dir. Pen. Cont., 2011.

CASTRONUOVO D., *Responsabilità da prodotto e struttura del fatto colposo*, in Riv. It. Dir. Proc. Pen., 2005, fasc. 1, pp. 301-340.

CATENACCI M., I poteri dello Stato e diritto penale, in Almerighi M.–A. Manna (a cura di), I poteri dello Stato e la Costituzione, Roma, Aracne, 2011, pp. 75-86

CHOPRA S.–L.F. WHITE, *A legal theory for autonomous artificial agents*, University of Michigan Press, 2011.

COMANDÈ G., *Intelligenza artificiale e responsabilità tra* liability *e* accountability. *Il carattere trasformativo dell'IA e il problema della responsabilità*, in Analisi giuridica dell'economia, 2019, pp. 168-188.

COMPOSTELLA R., *Auto a guida autonoma e diritto penale. Profili di responsabilità individuale e collettiva*, Napoli, Editoriale Scientifica, 2024.

Comunicazione della Commissione sul principio di precauzione (COM (2000) def.) del 2 febbraio 2000.

CONSOB, *Relazione per l'anno 2018*, Roma, 2019, in https://www.consob.it/documents/1912911/1997967/Rel2018.pdf/482b9ee4-f12e-2696-bfc8-70637e4d404a.

CONSOB, *Relazione per l'anno 2015*, Roma, 2016, in https://www.consob.it/documents/1912911/1988942/rel2015.pdf/a8d80c81-086c-482d-dd2f-a362cfbbf405.

CONSULICH F., *Il diritto penale al tempo dell'intelligenza artificiale. Prospettive punitive nazionali dopo l'*AI Act, in Diritto di difesa, 17 dicembre 2024.

CONSULICH F., *Intelligenza artificiale e reati finanziari*, in Consulich (a cura di), Reati in materia finanziaria, Torino, Giappichelli, 2024.

CONSULICH F., *Manipolazione del mercato e declino del sistema finanziario. Spunti di riflessione a margine del ventesimo anniversario dell'avvio del processo Parmalat*, in Sist. Pen., 4 settembre 2024.

CONSULICH F., Flash offenders*. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti*, in Riv. It. Dir. Proc. Pen., 2022, fasc. 3, pp. 1015–1055.

CONSULICH F., *Rischio consentito*, in Donini M. (diretto da), Il reato colposo. Enciclopedia del diritto, Milano, Giuffrè, 2021, pp. 1102-1135.

CONSULICH F., *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca borsa e titoli di credito*, 2018, fasc. 2, pp. 195-234.

CONSULICH F., *Manipolazione dei mercati e diritto eurounitario*, in Le Società, 2016, fasc. 2, pp. 203-216.

CONSULICH F., *Manipolazione del mercato e disorientamenti dogmatici tra eventi di pericolo e pericolo di eventi*, in Le società, 2011, fasc. 7, pp. 825-830.

CONSULICH F., *La giustizia e il mercato. Miti e realtà di una tutela penale dell'investimento mobiliare*, Milano, Giuffrè, 2010.

CONSULICH F., MUCCIARELLI F.*, Informazione e tutela penale dei mercati finanziari nello specchio della normativa eurounitaria sugli abusi di mercato*, in Le Società, 2016, fasc. 2, pp. 179-191.

CONSULICH F.–MAUGERI M.–MILIA C.–POLI T.N.–TROVATORE G., *AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?*, Quaderno giuridico Consob n. 29, maggio 2023, pp. 1-122.

CORNACCHIA L., *Responsabilità colposa: irrazionalità e prospettive di riforma*, in Arch. Pen., 12 luglio 2022.

CORNACCHIA L., *Concorso di colpe e principio di responsabilità penale per fatto proprio*, Torino, Giappichelli, 2004.

COSME JR. O., *Regulating High-Frequency Trading: The Case for Individual Criminal Liability*, in The Journal of Criminal Law and Criminology, 2019, vol. 109, issue 2, pp. 365-394.

D'ALESSANDRO F., *La manipolazione del mercato*, in Consulich (a cura di), Reati in materia finanziaria, Torino, Giappichelli, 2024, pp. 195-236.

D'ALESSANDRO F., *L'aggiotaggio e la manipolazione del mercato*, in Canzio G.–Cerqua L.–Luparia L., Diritto penale delle società. Accertamento delle responsabilità individuali e processo alla persona giuridica, Padova, Cedam, 2016, pp. 729-816.

D'ALESSANDRO F., *Le false valutazioni al vaglio delle Sezioni Unite: la nomofilachia, la legalità e il dialogo interdisciplinare*, in Cass. Pen., 2016, fasc. 7-8, pp. 2790-2807.

D'ALESSANDRO F., *Regolatori del mercato,* enforcement *e sistema penale*, Torino, Giappichelli, 2014.

D'ALESSANDRO F., *Pericolo astratto e limiti soglia*, Milano, Giuffrè, 2012.

D'ALESSANDRO F., Fattispecie di aggiotaggio e prassi di mercato ammesse, tra esclusione del tipo e cause di giustificazione, in Bertolino M.–Eusebi, L. –Forti, G. (a cura di), Studi in onore di Mario Romano, Napoli, Jovene, 2011, pp. 1817-1882.

DAVOLA E., *Algoritmi decisionali e trasparenza bancaria. Il paradigma dell'inerenza nella regolamentazione delle tecnologie emergenti*, Milano, Utet, 2020.

DE FELICE M., *Decisione robotica negoziale. Nuovi «punti di presa» sul futuro*, in Carleo A. (a cura di), Decisione robotica, Bologna, Il Mulino, 2019, pp. 179-202.

DONINI M., *Imputazione oggettiva dell'evento (diritto penale)*, in Enc. Dir., Annali III, Milano, Giuffrè, 2010, pp. 646-653.

DONINI M., *Imputazione oggettiva dell'evento. "Nesso di rischio" e responsabilità per fatto proprio*, Torino, Giappichelli, 2006.

DONINI M., *Il volto attuale dell'illecito penale*, Milano, Giuffrè, 2004.

DONINI M., *Illecito e colpevolezza nell'imputazione del reato*, Milano, Giuffrè, 1991.

DUNIS C.L.– MIDDLETON P.W.–KARATHANASOPOLOUS A.–THEOFILATOS K.A., *Artificial Intelligence in Financial Markets*, Palgrave Macmillan, 2016.

DUTCH AUTHORITY FOR THE FINANCIAL MARKETS, *Machine Learning in Algorithmic Trading Application by Dutch Proprietary Trading Firms and Possible Risks*, 2023, in https://www.afm.nl/~/profmedia/files/rapporten/2023/report-machine-learning-trading-algorithms.pdf.

ELDER B., *That Citi flash crash revisited*, in Financial Times, 3 maggio 2022, https://www.ft.com/content/3089d32b-1535-4f13-9411-c31b12486e4d

ESMA, *Consultation Paper. Mifid II/MiFIR review report on Algorithmic Trading*, settembre 2021, https://www.esma.europa.eu/sites/default/files/library/esma70-156-4572_mifid_ii_final_report_on_algorithmic_trading.pdf.

ESMA, *Guidelines on systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities*, 2012, in https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_2012_122_en.pdf.

FABOZZI F.J.–FOCARDI S.M.–JONA C., *High Frequency Trading: Methodologies and Market Impact*, Review of future markets, 2010, vol. 19, pp. 7-38.

FIANDACA G., *Sul dolo eventuale nella giurisprudenza più recente, tra approccio oggettivizzante-probatorio e messaggio generalpreventivo*, in Dir. Pen. Cont. Riv. Trim., 2012, fasc. 1, pp. 152-162.

FIANDACA G.–MUSCO E., *Diritto penale. Parte Generale*, IX ed., Bologna, Zanichelli, 2024.

FIERENS M–ROSSELLO S–WAUTERS E., *Setting the Scene: On AI Ethics and Regulation*, in De Bruyne J.–Vanleenhove C (eds) . Artificial Intelligence and the Law, Cambridge University Press, 2021, pp. 49-72.

FINANCIAL CONDUCT AUTHORITY, Final notice 2017: Paul Axel Walter, https://www.fca.org.uk/publication/final-notices/paul-axel-walter-2017.pdf, pp. 1-39.

FINANCIAL INDUSTRY REGULATORY AUTHORITY, *Getting Up to Speed on High-Frequency Trading*, 25 novembre 2015, https://www.finra.org/investors/insights/getting-speed-high-frequency-trading.

FIORE C., *L'azione socialmente adeguata nel diritto penale*, Napoli, Morano, 1966.

FIORELLA A., *Responsabilità penale dei* Tutor *e dominabilità dell'Intelligenza Artificiale. Rischio permesso e limiti di autonomia dell'Intelligenza Artificiale*, in

Giordano R.–Panzarola A.–Police A.–Preziosi S.–Proto M. (a cura di), Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia, Milano, Giuffrè, 2022, pp. 651-664.

FISCHER T.G., *Reinforcement learning in financial markets. A survey*, in FAU Discussion Papers in Economics, 2018, n. 12, Nürnberg, 2018, pp. 1-48.

FLORIDI L., *The European Legislation on AI: a Brief Analysis of its Philosophical Approach,* in Philosophy and Technology, 2021, n.34, pp. 215–222.

FLORIO M.E., *Il dibattito sulla responsabilità penale diretta delle i.a.: "molto rumore per nulla"?*, in Sist. pen., 2024, fasc. 2, pp. 5-18.

FOFFANI L., *Politica criminale europea e sistema finanziario: l'esempio degli abusi di mercato*, in Dir. Pen. Cont., Riv. Trim., 2014, fasc. 3-4, pp. 65-72.

FOFFANI L., *Art. 185 t.u.f.*, in Palazzo F.-Paliero C. E., Commentario breve alle leggi penali complementari, Padova, II ed., 2007.

FOFFANI L., *La nuova disciplina penale dell'"insider trading" e delle frodi nel mercato mobiliare*, in Riv. trim. dir. pen. econ., 1991, pp. 911-952.

FORTI G., *"Accesso" alle informazioni sul rischio e responsabilità: una lettura del principio di precauzione*, in Criminalia, 2006, p. 155-225.

FORTI G., *Colpa ed evento nel diritto penale*, Milano, Giuffrè, 1990.

FRAGASSO B., *Intelligenza artificiale e crisi del diritto penale d'evento: profili di responsabilità penale del produttore di sistemi di i.a.,* in Riv. It. Dir. Proc. Pen., 2024, fasc. 1, pp. 287-305.

FRAGASSO B., *La responsabilità penale del produttore di sistemi di intelligenza artificiale*, in Dir. Pen. cont. Riv Trim., 2023, fasc. 1, pp. 26-45.

GALLO M., *Diritto penale italiano. Appunti di parte generale*, vol. I, III ed., Torino, Giappichelli, 2021.

GALLO M., *Colpa penale (diritto vigente)*, in Enc. Dir., 1960, vol. VI, Milano, Giuffrè, pp. 624-643.

GAMBARDELLA M., *Condotte economiche e responsabilità penal*e, Torino, Giappichelli, 2020.

GARGANI A., *La "flessibilizzazione" giurisprudenziale delle categorie classiche del reato di fronte alle esigenze di controllo penale delle nuove fenomenologie di rischio*, in *Leg. Pen.*, 2011, fasc. 2, pp. 397-425.

GARGANTINI M., *The European Regulation of Securities Exchanges: Regulated Markets in an Evolving Technological and Legal Context*, Torino, Giappichelli, 2022.

GIANNINI A., *Criminal behavior and accountability of artificial intelligence systems*, Maastricht, Eleven Publishers, 2023.

GIUNTA F., *Il diritto penale e le suggestioni del principio di precauzione*, in Criminalia, 2006, pp. 227-247.

GIUNTA F., *Illiceità e colpevolezza nella responsabilità colposa*, Cedam, Padova, 1993.

GLESS S.–SILVERMAN E.–WEIGEND T., *If robots cause harm, who is to blame? Self-Driving Cars and Criminal Liability*, in New Criminal Law Review, 2016, vol. 19, n.3, pp. 412-436.

HOPE B., *How Computers Trawl a Sea of Data for Stock Picks*, in *Wall street Journal*, 2015, in https://perma.cc/JF4K-YWJV.

HALLEVY G., *Liability for Crimes Involving Artificial Intelligence Systems*, Berlin-New York, Springer, 2014.

HALLEVY G., *When Robots Kill. Artificial Intelligence under Criminal Law*, Boston, Northeaster University Press, 2013.

HALLEVY G.*, I, Robot - I, Criminal – When Science Fiction Becomes Reality: Legal Liability of AI Robots Committing Criminal Offenses*, in Syracuse Science & Technology Law Reporter, 2010, vol. 22, n.1., pp. 1-37.

HALLEVY G.*, The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control*, in Akron Intellectual Property Journal, 2010, vol. 4, issue 2, pp. 171-201.

HALLEVY G., *Virtual Criminal Responsibility*, in Original Law Review, 2010, vol. issue 1, pp. 6-27.

HU Y., Robot Criminals, in University of Michigan. Journal Law Reform, 2019, vol. 54, issue 2. pp. 487-531.

IOSCO, *The use of artificial intelligence and machine learning by market intermediaries and asset managers. Final Report*, 2021.

IOSCO, *Principles for Dark Liquidity. Final Report 06/11,* 2011, in http://www.iosco.org/library/pubdocs/pdf/IOSCOPD353.pdf.

KAPLAN J., *Artificial Intelligence: What Everyone Needs to Know*, Oxford, 2016.

KEARNS M.–NEVMYVAKA Y., *Machine Learning for Market Microstructure and High Frequency Trading*, in Easley D.–Lopez de Prado M.–O'Hara M. (eds.), High Frequency Trading, Risk Books, 2013, pp. 91-124.

KIRILENKO A.–KYLE A.S.–SAMADI M.–TUZUN T., *The Flash Crash: High Frequency Trading in an Electronic Market*, in The Journal of Finance, 2017, vol. 72, issue 3, pp. 967-998.

LA VATTIATA F.C., *AI Systems Involved in Harmful Events: Liable Persons or Mere Instruments? An Interdisciplinary and Comparative Analysis*, in BioLaw Journal, 2023, fasc. 1, pp. 485-499.

LA VATTIATA F.C., *Brevi note "a caldo" sulla recente Proposta di Regolamento UE in tema di intelligenza artificiale*, in Dir. Pen. Uomo, 2021, fasc. 6, pp. 140-158.

LAGIOIA F.–SARTOR G., *AI Systems Under Criminal Law: a Legal Analysis and a Regulatory Perspective*, in Philosophy & Technology, vol. 33, 2020, pp. 433-465.

LANZI M., Self driving cars *e responsabilità penale. La gestione del "rischio stradale" nell'era dell'intelligenza artificiale*, Torino, Giappichelli, 2023.

LAUX J.–WACHTER S.–MITTELSTADT B, *Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk,* in Regulation & Governance, 2024, vol. 18, issue 1, pp. 3-32.

LEIS D., *High Frequency Trading: Market Manipulation and Systemic Risks from an EU Perspective*, in https://ssrn.com/abstract=2108344., 2012, pp. 1-81.

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

LIN T.C.W, *The New Market Manipulation*, Emory Law Journal, 2017, vol. 66, pp. 1253-1314.

LIN T.C.W., *The new Investor*, in UCLA Law Review, 2013, vol. 60, pp. 678-735.

LIN T.C.W, *Reasonable Investor(s)*, in Boston University Law Review, 2013, vol. 95, pp. 461-518.

LUCANTONI P., *L'«high frequency trading» nel prisma della vigilanza algoritmica del mercato*, in Analisi Giuridica dell'Economia, Studi e discussioni sul diritto dell'impresa, 2019, fasc. 1, pp. 297-312.

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., 2019, pp. 1-14.

MAGRO M.B., *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, in Leg. pen., 10 maggio 2020, p. 1-22.

MAGRO M.B., Robot*,* cyborg *e intelligenze artificiali*, in Cadoppi A.–Canestrari S.–Manna A.–Papa M., in Cybercrime, Milano, Utet, 2019, pp. 1232-1256.

MAGRO M.B., *Manipolazioni dei mercati finanziari e diritto penale, Una critica al modello di razionalità economica*, Milano, Giuffrè, 2012.

MANAHOV V. –HUDSON R.–GEBKA R., *Does High Frequency Trading Affect Technical Analysis and Market Efficency? And if So, How?*, in Journal of International Financial Markets Institutions and Money, 2014, vol. 28, pp. 131-157.

MANTOVANI F., *Diritto penale. Parte generale*., X ed., Padova, Cedam, 2017.

MARINUCCI G., *La colpa per inosservanza di leggi*, Milano, Giuffrè, 1965 rist. in La colpa. Studi, Milano, Giuffrè, 2013, pp. 164-170.

MARINUCCI G., *Non c'è dolo senza colpa. Morte dell'"imputazione oggettiva dell'evento" e trasfigurazione nella colpevolezza?*, in Riv. it. dir. proc. pen., 1991, fasc. 1, pp. 3-39.

MARINUCCI G.–DOLCINI E., *Corso di diritto penale*, III ed., Milano, Giuffrè, 2001.

MARINUCCI G.–DOLCINI E.– GATTA G.L., *Manuale di diritto penale. Parte Generale*, XIII ed., Milano, Giuffrè, 2024.

MARTÍNEZ-MIRANDA E.–MCBURNEY P.–HOWARD M.J.W., *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.

MARTINS PEREIRA C., *Unregulated Algorithmic Trading: Testing the Boundaries of the European Algorithmic Trading Regime*, in Journal of Financial Regulation, 2020, vol. 6, issue 2, pp. 270–305.

MASERA L., *La nozione costituzionale di materia penale*, Torino, Giappichelli, 2018.

MATTHIAS A., *The responsibility gap: Ascribing responsibility for the actions of learning automata*, in Ethics and Information Technology, 2004, vol. 6, issue 3, pp. 175-183.

MAZZACUVA F., *Le pene nascoste*, Torino, Giappichelli, 2017.

MIEDICO M., Gli abusi di mercato, in A. Alessandri (a cura di), Reati in materia economica, Torino, Giappichelli, 2012, II ed., pp. 305-372.

MILITELLO V., *Rischio e responsabilità penale*, Milano, Giuffrè, 1988.

MIZUTA T., *Can an AI Perform Market Manipulation at Its Own Discretion? A Genetic Algorithm Learns in an Artificial Market Simulation*, Canberra, 2020, pp. 1-6.

MOTTURA C., *Decisione robotica negoziale e mercati finanziari e mercati finanziari. Contrattazione algoritmica, nuovi abusi di mercato, algoritmi di controllo (degli algoritmi)*, in Carleo A., Decisione robotica, Bologna, Il Mulino, 2019, pp. 265-289.

MULLIGAN C., *Revenge Against Robots*, in South Carolina Law Review, 2018, vol. 69, issue 3, p. 579-596.

MUCCIARELLI F., *Mercato finanziario e tutela penale*, in Consulich (a cura di), Reati in materia finanziaria, Torino, Giappichelli, 2024, pp. 111-136.

MUCCIARELLI F., *Materialità e offensività dell'alterazione, investitore ragionevole e giudizi nella manipolazione del mercato*, in Dir. Pen. Cont. Riv. Trim., 2024, fasc. 3, pp. 17-74.

MUCCIARELLI F., *"Doppio binario" sanzionatorio degli abusi di mercato e* ne bis in idem*: prime ricadute pratiche dopo le sentenze della CGUE e la (parziale) riforma domestica*, in Dir. Pen. Cont., 15 marzo 2019.

MUCCIARELLI F., *Gli abusi di mercato riformati e le persistenti criticità di una tormentata disciplina*, in Dir. Pen. Cont. Riv. Trim., 2018, fasc. 3, pp. 174-189.

MUCCIARELLI F., *La nuova disciplina eurounitaria sul* market abuse*: tra obblighi di criminalizzazione e* ne bis in idem, in Dir. Pen. Cont. Riv. Trim., 2015, fasc. 4, pp. 295–324.

MUCCIARELLI F., A*rt. 184*, in Fratini M.–Gasparri G., Il testo unico della finanza, II, Milano, Utet, 2012, pp. 2378-2417.

MUCCIARELLI F., A*rt. 185*, in Fratini M.–Gasparri G., Testo unico della finanza, II, Milano, Utet, 2012, pp. 2392-2303.

MUCCIARELLI F., *Gli illeciti di abuso di mercato, la responsabilità dell'ente e l'informazione*, in Riv. trim. dir. pen. econ., 2008, fasc. 4, pp. 823-860.

MUCCIARELLI F.–BASILE E., Market abuse evolution after the MAD II and the MAR: how Italy amended its legislation in light of Regulation (EU) 596/2014, in Criminal Justice Network, 2018, pp. 1-5.

NAPOLEONI V., *L'*insider trading, in Santoriello C. (a cura di), La disciplina penale dell'economia. Società, fallimento, finanza, vol. I, Torino, Giappichelli, 2008, pp. 633-779.

PADOVANI T., *Colpa per inosservanza di legge ed "impossibilità" di adottare le cautele prescritte*, in *Riv. It. Dir. Proc. Pen.*, 1977, fasc. 2, pp. 767-772.

PAGELLA C., *L'inafferrabile concetto di "connessione sostanziale e temporale sufficientemente stretta": la Cassazione ancora su* ne bis in idem *e* insider trading, in Sist. Pen., 9 gennaio 2020.

PAGALLO U., *Three Roads to Complexity, AI and the Law of Robots: On Crimes, Contracts, and Torts*, in Palmirani M.–Pagallo U.–Casanovas P.–Sartor G. (eds) AI Approaches to the Complexity of Legal Systems. Models and Ethical Challenges for Legal Systems, Legal Language and Legal Ontologies, Argumentation and Software Agents, Heidelberg, Springer, 2012, pp. 48-60.

PAGALLO U., *The Adventures of Picciotto Roboto: AI & Ethics in Criminal Law*, in The Social Impact of Social Computing - Ethicomp 2011, Sheffield, Sheffield Hallam University, 2011, pp. 349-355.

PAGALLO U., *Saggio sui robot e il diritto penale*, in S. Vinciguerra–F. Dassano (a cura di), Scritti in memoria di Giuliano Marini, Napoli, 2010, pp. 595-610.

PALAZZO F., *Corso di diritto penale*, VII ed., Torino, Giappichelli, 2018.

PALIERO C.E*., L'autunno del patriarca. Rinnovamento o trasmutazione del diritto penale dei codici?*, in Riv. It. Dir. Proc. Pen., 1994, fasc. 4, pp. 1220-1250.

PANATTONI B., *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, in Dir. inf., fasc. 1, 2021, pp. 317-368.

PAOLUCCI F., A*lgoritmi e intelligenza artificiale alla ricerca di una definizione: l'esegesi del Consiglio di Stato, alla luce dell'*AI Act, in Quest. giust., 8 aprile 2022.

PAPA M., *Future Crimes: Intelligenza artificiale e rinnovamento del diritto penale*, in Criminalia, 2019, pp. 491-503.

PASQUALE F., *The black box society: the secret algorithms that control money and information*, London, Harvard University Press, 2015.

PASQUALE F., *Law's Acceleration of Finance: Redefining the Problem of High-Frequency Trading*, in University of Maryland Francis King Carey School of Law Legal Studies Research Paper, 2015, vol. 29, pp. 2085-2127.

PEDRAZZI C., *Interessi economici e tutela penale*, 1985, ora in Id, Diritto penale, vol. III - Scritti di diritto penale dell'economia, Milano, Giuffrè, 2003, pp. 187-200.

PEDRAZZI C., *Problemi di tecnica legislativa*, 1979, ora in Id, Diritto penale, vol. III - Scritti di diritto penale dell'economia, Milano, Giuffrè, 2003, pp. 129-156.

PEDRAZZI C., *Problemi del delitto di aggiotaggio*, 1958, ora in Id., Diritto penale, vol. IV - Scritti di diritto penale dell'economia, Milano, Giuffrè, 2003, pp. 3-97.

PEDRESCHI D.–GIANNOTTI F.–GUIDOTTI R.–MONREALE A.–RUGGIERI S.–TURINI F., *Meaningful Explanations of Black Box AI Decision Systems*, Proceedings of the AAAI Conference on Artificial Intelligence, 2019, vol. 33, pp. 9780-9784.

PERINI C., *Il concetto di rischio nel diritto penale moderno*, Milano, Giuffrè, 2010.

PICOTTI L., *Categorie tradizionali del diritto penale e intelligenza artificiale: crisi o palingenesi? Le raccomandazioni dell'*Association Internationale de Droit Pénal *e la rilevanza del recente regolamento europeo sull'intelligenza artificiale*, in Sist. Pen., 31 luglio 2024, pp. 1–20.

PICOTTI L., *Resolution on traditional criminal law categories and AI*, in Picotti-Panattoni (a cura di), Traditional Criminal Law Categories and AI: Crisis or Palingenesis?, in Revue Internationale de Droit Penal, 2023, vol. 94, issue 1, pp. 53-59.

PICOTTI L.*, Ente,* Piergallini C.– Mannozzi G.–Sotis C.–Perini C.–Scoletta M.–Consulich F. (a cura di), Studi in onore di Carlo Enrico Paliero, Milano, Giuffrè, 2022, pp. 1477-1494, nonché in Sist. Pen., 10 luglio 2023, pp. 1-14.

PIERGALLINI C., *Il fatto tipico colposo*, in Paliero C.E. (a cura di), Il sistema penale, Torino, Giappichelli, 2024, pp. 285-324.

PIERGALLINI C., *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato*, in Riv. it. dir. proc. pen., 2020, fasc. 4, pp. 1745–1774.

PIERGALLINI C., *Colpa* (dir. pen.), in Enc. Dir., Annali X, Milano, Giuffrè, 2017, pp. 222-265.

PIERGALLINI C., *Il paradigma della colpa nell'età del rischio: prove di resistenza del tipo*, in Riv. it. dir. proc. pen., 2005, fasc. 4, pp. 1684-1703.

PIERGALLINI C., *Danno da prodotto e responsabilità penale. Profili dommatici e politico-criminali*, Milano, Giuffrè, 2004.

PIERGALLINI C., *Attività produttive e imputazione per colpa: prove tecniche di diritto penale del rischio*, in Riv. It. Dir. Proc. Pen., 1997, fasc. 4, pp. 1473-1495.

POLLICINO O.–DUNN P., Intelligenza artificiale e democrazia, Milano, Bocconi Univerisity Press, 2024.

PROSDOCIMI S., Dolus eventualis. *Il dolo eventuale nella struttura delle fattispecie penali*, Milano, Giuffrè, 1993.

PULITANÒ D., *Diritto penale*, VII ed., Torino, Giappichelli, 2017.

PUORRO A., *High frequency trading: una panoramica*, in *Questioni di Economia e Finanza* n. 198, 2013, pp. 1-41.

RAVAGNANI A.–LILLO F.–DERIU P.–MAZZARISI P.–MEDDA F.–RUSSO A., *Dimensionality reduction techniques to support insider trading detection*, in Consob. Quaderni FinTech, 12 febbraio 2024.

ROMANO M., *Art. 43*, in Commentario sistematico del codice penale, vol. I, III ed., Milano, Giuffrè, 2004, p. 402-442.

RUGA RIVA C., *Principio di precauzione e diritto penale. Genesi e contenuto della colpa in contesti di incertezza scientifica*, in Dolcini E.–Paliero C.E. (a cura di), Studi in onore di Giorgio Marinucci, vol. II, Milano, Giuffrè, 2006, pp. 1743-1777.

RUSSELL P.–NORVIG S.J., *Artificial Intelligence: A Modern Approach*, IV ed., London Pearson, 2020.

RUTA G., *I.A. nei reati economici e finanziari*, in Intelligenza artificiale e giurisdizione penale, Atti del Workshop della Fondazione Vittorio Occorsio, Università Mercatorum, Roma, 19 novembre 2021, pp. 58-75.

SALVADORI I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in Riv. It. Dir. Proc. Pen., 2021, fasc. 1, pp. 83-118.

SCOLETTA M., *Il doppio binario sanzionatorio alla luce del vincolo europeo del* ne bis in idem, in Consulich F. (a cura di) Reati in materia finanziaria, Torino, 2024, pp. 297-320.

SCOLETTA M., *Il principio europeo di* ne bis in idem *e i modelli punitivi "a doppio binario*", in Amalfitano C. - D'Amico M. – Leone S. (a cura di), La Carta dei diritti fondamentali dell'Unione Europa nel sistema integrato di tutela, Torino, 2022, pp. 315-361.

SCOLETTA M., *Uno più uno anche a Roma può fare due: la illegittimità costituzionale del doppio binario punitivo in materia di diritto d'autore*, in Sist. Pen., 23 giugno 2022.

SCHWARTZ R.A.−BYRNE J.A.−STEMPEL E., *Rapidly Changing Securities Markets: Who Are the Initiators?*, Springer, 2017.

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 Law Review, 2015, vol. 67, issue 1, pp. 221-293.

SEMINARA S., *Diritto penale commerciale. Il diritto penale del mercato mobiliare*, vol. III, II ed., Torino, Giappichelli, 2022.

SEMINARA S., *L'informazione privilegiata*, in Cera M.–Presti G. (a cura di), Il testo unico finanziario, Vol. II, Bologna, Zanichelli, 2020, pp. 2124-2165.

SEMINARA S., *La riforma dei reati di false comunicazioni sociali*, Dir. pen. proc., 2015, fasc. 7, pp. 813-824.

SEMINARA S., *Informazione finanziaria e mercato: alla ricerca di una strategia del controllo penale amministrativo*, in Analisi Giuridica dell'Economia, Studi e discussioni sul diritto dell'impresa, 2006, fasc. 2, pp. 255-278.

SEMINARA S., *L'evoluzione europea del diritto penale del mercato finanziario nella prospettiva italiana*, in Canestrari S.−Foffani L. (a cura di), Il diritto penale nella prospettiva europea, 2005, pp. 219-253.

SEMINARA S., Insider trading *e diritto penale*, Milano, Giuffrè, 1989.

SEVERINO P., *Intelligenza artificiale e diritto penale*, in Ruffolo U. (a cura di), Intelligenza artificiale. Il diritto, i diritti, l'etica, Milano, Giuffrè, 2020, pp. 531-545.

SGUBBI F., *La manipolazione del mercato*, in Sgubbi F.–Fondaroli D.–Tripodi A., Diritto penale del mercato finanziario. Abuso di informazioni privilegiate, manipolazione del mercato, ostacolo alle funzioni di vigilanza della Consob, falso in prospetto. Lezioni, II ed., Padova, Cedam, 2013, pp. 71-112.

SGUBBI F., *Abusi di mercato*, in *Enc. Giur.*, Annali II, Tomo II, Milano, 2009.

SILVA C., *La proporzionalità della pena in materia di abusi di mercato. Profili problematici di un sindacato diffuso di ri-equilibrio sanzionatorio*, in Sist. Pen., 2023.

SIMMLER M.–MARKWALDER N*., Guilty Robots? - Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence*, in Criminal Law Forum, 2019, issue 30, pp. 1-31.

STELLA F., *Giustizia e modernità. La protezione dell'innocente e la tutela delle vittime*, Milano, Giuffrè, III ed., 2003.

STRAMPELLI G., *L'informazione societaria a quindici anni dal t.u.f.: profili evolutivi e problemi*, in Riv. soc., 2014, fasc. 5, pp. 991-1059.

STRAMPELLI G.–BALP G., *Preserving Capital Markets Efficiency in the High-Frequency Trading Era*, in Bocconi Legal Studies Research Paper, 2018, pp. 1-58.

SURDEN H., *Artificial Intelligence and Law: An Overview*, in Georgia State University Law Review, 2019, vol. 35, issue 4, pp. 1305-1137.

SUTTON R.S.–BARTO A.G., *Reinforcement Learning: an introduction*, MIT Press, Cambridge, 2017.

TRELEAVEN P.–GALAS M.–LALCHAND V., *Algorithmic trading review,* in Communications of the ACM, 2013, vol. 56, issue 11, pp. 76-85.

TRIPODI A., *Gli illeciti amministrativi in tema di abusi di mercato*, in Consulich F. (a cura di), Reati in materia finanziaria, Torino, Giappichelli, 2024, pp. 273-296.

TRIPODI A., *Uno più uno (a Strasburgo) fa due. L'Italia condannata per violazione del ne bis in idem in tema di manipolazione del mercato*, in Dir. pen. cont., 9 marzo 2014.

TRONCONE P., *Il sistema dell'intelligenza artificiale nella trama grammaticale del diritto penale. Dalla responsabilità umana alla responsabilità delle macchine pensanti:* in inatteso return trip effect, in Cass. Pen., 2022, fasc. 9, pp. 3287-3304.

U.S. SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, *AI in the Real World. Hedge Funds' Use of Artificial Intelligence in Trading,* 2024, https://www.hsgac.senate.gov/wp-content/uploads/2024.06.11-Hedge-Fund-Use-of-AI-Report.pdf.

U.S. SECURITIES AND EXCHANGE COMMISSION, *Artificial Intelligence (AI) and Investment Fraud: Investor Alert*, 25 gennaio 2024, in https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/artificial-intelligence-fraud.

U.S. SECURITIES AND EXCHANGE COMMISSION, Press Release. SEC Charges New York-Based High Frequency Trading Firm With Fraudulent Trading to Manipulate Closing Prices: First High Frequency Trading Manipulation, Case, SEC. & EXCH. COMM'N (Oct. 16, 2014), https://www.sec.gov/news/press-release/2014-229#.VEOZlfldV8E.

U.S. SECURITIES AND EXCHANGE COMMISSION, *Concept Release on Equity Market Structure*, in Exchange Act Release No. 34-61,358, 75 Fed. Reg. 3594, 3598 (proposed Jan. 21, 2010).

VENEZIANI P., *Regole cautelari "proprie" ed "improprie" nella prospettiva delle fattispecie colpose causalmente orientate*, Padova, Cedam, 2003.

VENTORUZZO M., *Qualche nota sul cosiddetto "insider di sé stesso" alla luce del Regolamento UE sugli abusi di mercato*, in Le Società, 2018, fasc. 6, pp. 739-751.

VERSTEIN A., *Benchmark Manipulation*, in Boston College Law Review, vol. 56, issue 1, pp. 215-272.

VIGANÒ F., Ne bis in idem *e pluralità di sistemi sanzionatori per lo stesso fatto*, in Rivista delle società, 2023, fasc. 1, pp. 189-207.

VIGANÒ F., *Doppio binario sanzionatorio e* ne bis in idem*: verso una diretta applicazione dell'art. 50 della carta? (a margine della sentenza Grande Stevens della Corte edu)*, in Dir. Pen. Cont. Riv. Trim., 2014, fasc. 3-4, pp. 219-238.

VIGANÒ F., *La Cassazione chiude il caso della scalata Antonventa (e perde una preziosa occasione per fare un po' di chiarezza sui delitti di aggiotaggio)*, in Pen. cont., 7 aprile 2013.

VIGANÒ F., *Il dolo eventuale nella giurisprudenza recente*, in Il libro dell'anno del diritto 2013 Treccani, 2013, pp. 118-127.

WEIGEND T., *Convicting Autonomous Weapons? Criminal Responsibility of and for AWS under International Law*, in Journal of International Criminal Justice, 2023, vol. 21, issue 5, pp. 1137-1154.

ZHANG Z.–ZOHREN S.–ROBERTS S., *Deep Reinforcement Learning for* Trading, in The Journal of Financial Data Science, 2020, vol. 2, issue 2, pp. 25-40.

ZIRULIA S., *Esposizione a sostanze tossiche e responsabilità penale*, Milano, Giuffrè, 2018.