UNIVERSITÀ DEGLI STUDI DI GENOVA SCUOLA DI SCIENZE SOCIALI

Dipartimento di Giurisprudenza

Corso di Laurea Magistrale in Giurisprudenza

Tesi di laurea in

Diritto Penale

Commerciale

INTELLIGENZA ARTIFICIALE E MANIPOLAZIONE DEL MERCATO

La discussa rilevanza penale delle operazioni di High Frequency Trading

Relatore:

Chiar.mo Prof. Federico Consulich

Candidato: *Valentina Cotugno*

Anno Accademico 2022/2023

INDICE

INTRODUZIONE

Il mito delle macchine "intelligenti" ha iniziato ad aleggiare nella letteratura sin dalla metà del secolo scorso. Negli ultimi anni quello che, fino a poco tempo fa, poteva rappresentare solo uno stravagante scenario fittizio è iniziato a diventare reale.

L'incredibile progresso tecnologico degli ultimi decenni ha portato alla progressiva evoluzione del concetto di algoritmo ed ha consentito di giungere alla creazione di vere e proprie "intelligenze artificiali".

I giuristi sono quindi stati costretti a confrontarsi con complesse sfide interpretative in scenari del tutto nuovi. Sia il legislatore sia l'interprete stanno oggi affrontando problemi mai posti precedentemente nell'ambito del diritto.

Infatti, attraverso avanzate tecniche di apprendimento, la macchina "intelligente" può imparare dall'esperienza e dai dati che ricava dall'ambiente esterno, migliorando progressivamente le proprie prestazioni e capacità, anche decisionali. In molti casi l'uomo si limita a indicare un obiettivo che il sistema di intelligenza artificiale (IA) perseguirà in maniera autonoma.

Le conseguenti interferenze dei moderni sistemi di IA con il diritto costituiscono una problematica trasversale e riguardano, in relazione ad aspetti diversi, tutti i settori dell'ordinamento.

È tuttavia nell'ambito penale che si manifestano le principali criticità. La sempre più estesa autonomia e l'opacità dei meccanismi decisionali dei sistemi di IA possono infatti entrare in tensione con i tradizionali principi di personalità e colpevolezza che caratterizzano la responsabilità penale.

Occorre chiedersi se i sistemi di IA che materialmente realizzano fattispecie di reato possano ancora essere considerati strumenti nelle mani dell'uomo, oppure se agiscano, di fatto, in modo sostanzialmente indipendente dal volere umano.

La problematica descritta si accentua nel momento in cui le intelligenze artificiali costituiscono cosiddette *black boxes*, ossia sistemi descrivibili solo nel comportamento esterno e nei quali i meccanismi decisionali che portano l'agente artificiale a realizzare un determinato comportamento rimangono imperscrutabili, anche da parte del programmatore.

È stato evidenziato in dottrina che tali caratteristiche di alcuni sistemi di IA possono, pertanto, creare un pericoloso vuoto di tutela in campo penale.

Uno dei primi settori che si è dovuto confrontare con le problematiche legate a tale "*responsibility gap"* è quello dei reati legati ai mercati finanziari.

Ci si riferisce in particolare al compimento di condotte manipolative del mercato attraverso sistemi di intelligenza artificiale utilizzati per il *trading* ad alta frequenza.

In tale ambito si riscontrano infatti tutti i principali problemi che rendono complessa la repressione penale dei comportamenti attuati attraverso sistemi di IA.

Il presente lavoro si concentra sul fenomeno, ormai estremamente diffuso, dell'*High Frequency Trading* (HFT): una modalità di contrattazione che utilizza un sistema di IA per operare sul mercato. L'operatività degli HFTs si caratterizza per un'estrema velocità di contrattazione accompagnata dall'immissione di enormi quantità di ordini nei mercati. Inoltre, i sistemi di intelligenza artificiale utilizzati per la contrattazione ad alta frequenza vengono spesso dotati della capacità di apprendere dai propri comportamenti precedenti e dalle relative reazioni del mercato. In questo modo possono sviluppare delle strategie di *trading* che presentano tutte le caratteristiche per poter essere definite manipolative.

Verranno quindi presentate le varie dinamiche di responsabilità che si sono evidenziate in diversi casi giudiziari, specialmente statunitensi: da un semplice malfunzionamento del sistema, fino alla programmazione specifica dell'algoritmo con intenti manipolativi. Tuttavia, l'ipotesi che verrà approfondita maggiormente riguarda il problematico caso nel quale il sistema di HFT apprende *autonomamente* le strategie manipolative.

Tali tematiche verranno analizzate in primo luogo sotto un profilo più generale, prendendo spunto dalle riflessioni della dottrina statunitense, che per prima si è trovata ad affrontare la questione.

Successivamente, si passerà ad una trattazione più approfondita, strettamente legata al diritto penale italiano. In questa sezione, a seguito dell'analisi della norma che nel nostro ordinamento incrimina la manipolazione del mercato (art. 185 d.l. n.58/1998 Testo unico in materia di intermediazione finanziaria), la trattazione si concentrerà sulla descrizione puntuale di come le problematiche legate alle *black boxes* e al *responsibility gap* si intersechino con le norme e i principi del diritto penale italiano, in un contesto già di per sé complesso come quello dei mercati finanziari.

Verranno quindi esposte le principali soluzioni prospettate dalla dottrina, alla luce del panorama giuridico attuale e futuro, tenendo però presente che la rivoluzione tecnologica e

culturale apportata dall'intelligenza artificiale renderà comunque necessario, per l'interprete e per il legislatore, un generale ripensamento di molti settori del diritto.

CAPITOLO I
L'INTELLIGENZA ARTIFICIALE

SOMMARIO: 1.1 Definizione e classificazioni. – 1.1.1 Le modalità di apprendimento della macchina: *machine learning*, *deep learning* e reti neurali. – 1.1.2 La proposta di Regolamento Europeo sull'IA e la classificazione dei sistemi sulla base del rischio. – 1.2 L'interferenza dell'intelligenza artificiale con il diritto penale sostanziale: *machina delinquere potest*? – 1.2.1 Il *Comportamento emergente* della macchina e la sopravvenienza di un *responsibility gap*: il problema della *Black Box*. – 1.2.2 Le soluzioni proposte: a) la responsabilità diretta dell'IA: la teoria di Hallevy e le critiche; b) due opzioni possibili: il divieto di utilizzo oppure la gestione del rischio consentito.

1.1 Definizione e classificazioni

Attribuire un significato al termine "intelligenza artificiale" può risultare un compito particolarmente complesso tenuto conto della velocità con cui il progresso tecnologico muta in questo ambito.

Il termine è stato coniato dallo scienziato John McCarthy dell'Università di Stanford, organizzatore del primo evento su questo tema: il *Darmouth Summer Research Project on Artificial Intelligence* del 1956. In questo contesto, i "sistemi intelligenti" erano definiti come strumenti capaci di eseguire compiti normalmente associati all'intelligenza umana.[1] L'agente di intelligenza artificiale veniva quindi inteso, in questo primo momento, come una macchina capace di emulare in parte l'agire umano.

Tuttavia, questo parallelismo è stato da subito scoraggiato proprio per le pericolose implicazioni logiche cui avrebbe condotto: già Alan Turing, nel celebre saggio "*Computing Machinery and Intelligence",* affermava che il concetto di "intelligenza" negli anni successivi sarebbe stato inevitabilmente modellato e adattato per ricomprendere forme di intelligenza diverse e nuove, come quelle degli agenti artificiali. Il celebre scienziato, infatti, sosteneva che la domanda "se le macchine potessero pensare" fosse troppo priva di senso per poter essere discussa: sarebbe stato necessario definire in modo puntuale il concetto di "macchina" e di "pensiero".[2] Touring, infatti, scriveva: «sono convinto che entro la fine del

[1] M. GABBRIELLI, *Dalla logica al deep learning: una breve riflessione sull'intelligenza artificiale*, in *XXVI lezioni di diritto dell'intelligenza artificiale* a cura di U. Ruffolo, Torino, Giappichelli, 2020, p.21.

[2] B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automazione artificiale,* in *Diritto dell'Informazione e dell'informatica* (II), fasc.2, 2021, p. 317.

secolo l'uso delle parole e la generale opinione pubblica colta saranno cambiate tanto da fare in modo che si potrà parlare di macchine che pensano senza timore di essere contraddetti.»[3]

Effettivamente oggi l'evoluzione tecnologica è stata tale da rendere indiscutibile l'esistenza di cosiddetti *Agenti di Intelligenza Artificiale* (agenti di IA). A questo proposito, si può partire dalla definizione di "agente intelligente" basata sulle caratteristiche riassunte nell'acronimo inglese *PAGE (Percepts, Actions, Goals, Environment)*: un agente può definirsi "intelligente" in questo senso se, dato un determinato ambiente, utilizza percezioni per compiere azioni in vista di un obbiettivo da perseguire.[4]

Gli agenti artificiali possono essere di diversi tipi e vengono classificati in agenti e sotto-agenti a seconda delle loro peculiarità, sempre tenendo presente la modulazione delle caratteristiche e della composizione PAGE. Ad esempio, possiamo avere "agenti fisici", realizzati con sensori e attuatori, dotati quindi di una struttura fisica (o *hardware*) oppure agenti detti "temporali", che utilizzano informazioni basate sul tempo per raccogliere input e modificare i comportamenti successivi, spesso sprovvisti di una struttura fisica e costituiti da soli *software.*

Sulla base delle caratteristiche dell'agente e in particolare del grado di autonomia dello stesso possiamo in questa sede anticipare una prima classificazione degli agenti artificiali.

Innanzitutto, possiamo distinguere tra: agenti "automatizzati" e agenti artificiali "autonomi". I primi pongono in essere, in base agli algoritmi che ne definiscono la struttura interna, una o più azioni nelle modalità prestabilite: l'agire del *software* è predeterminato dal programmatore e in questo senso è "automatico". I secondi invece riescono ad adattare il loro processo decisionale in relazione ad elementi esterni per migliorare il raggiungimento dei risultati prestabiliti.[5]

A seconda del livello di automazione quindi si possono distinguere in generale quattro classi di agenti artificiali autonomi (a.a). Il primo livello comprende gli a.a. che operano in modo automatico e sono soggetti ad un controllo da parte dell'uomo. Gli a.a di secondo livello sono programmati con algoritmi deterministici che possono già risolvere problemi previsti dagli sviluppatori e sono in grado di prendere decisioni autonome di fronte a

[3] A. TURING, *Calcolatori e intelligenza*, in *L'io della mente*, a cura di D. R. Hofstadter, D. C. Dennet , Milano, 1981, p. 64.
[4] Sito web: intelligenzaartificiale.it
[5] I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale,* in *Riv. it. dir. proc. pen*, fasc.1, marzo 2021, p.83.

situazioni prestabilite. Al terzo livello troviamo agenti *semi-autonomi* dotati di algoritmi di apprendimento automatico (*machine learning*) in grado di modificare e correggere i propri comportamenti in base alla loro esperienza. Infine, il livello più elevato di autonomia si raggiunge con i sistemi multi-agente in cui, grazie all'*Internet of Things*, i vari agenti di IA possono interagire tra loro e con oggetti, adeguando quindi i loro comportamenti all'ambiente in cui si trovano ad operare.[6]

In conseguenza alla diffusione esponenziale di questi tipi di tecnologia, le istituzioni dell'Unione Europea hanno iniziato a prestare attenzione a questo fenomeno e alle criticità derivanti dalla mancanza di una disciplina unitaria a livello europeo. La risposta è stata una proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale. Tale proposta è stata avanzata nel 2021 e, attualmente, deve essere approvata.

Il progetto è quello di creare, attraverso un *I.A. Act*, una disciplina europea armonizzata in materia di sistemi di intelligenza artificiale che coinvolga tutti i settori di applicazione di questa tecnologia: dall'identificazione biometrica delle persone o gli aeromobili militari a guida autonoma fino ai *software* utilizzati dagli istituti di credito per predire il grado di solvibilità dei clienti.

Il contenuto del Regolamento sarà analizzato in maniera più approfondita in seguito.[7] Ai fini del presente paragrafo, può essere utile però anticipare la definizione di "sistema di intelligenza artificiale" offerta dalla norma: nell'art. 3 del Regolamento un sistema di intelligenza artificiale viene definito come «*un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono;*»[8]

L'allegato I infatti elenca le tecniche e gli approcci di intelligenza artificiale dividendoli in tre tipologie:

---

[6] *Ibidem.*

[7] Si veda § 1.1.2

[8] *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione*, 2021, eur-lex.europa.eu

a) Approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (deep learning);

b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti;

c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione.[9]

Per completezza occorre evidenziare che l'art. 4 prevede che l'allegato I potrà essere modificato e integrato con atti delegati della Commissione, per adeguarsi allo sviluppo tecnologico.

In definitiva, possiamo affermare che l'intelligenza artificiale consiste in un ramo dell'informatica che studia la progettazione e la programmazione di sistemi, sia *hardware* che *software,* dotati di caratteristiche e capacità che vengono considerate tipicamente umane quali, ad esempio, percezioni visive, spazio-temporali e decisionali.[10]

1.1.1 Le modalità di apprendimento della macchina: *machine learning, deep learning* e reti neurali

Definito quindi a livello generale il concetto di intelligenza artificiale, ci si può soffermare sui meccanismi che permettono alla macchina di "apprendere": si parla a questo proposito di *machine learning* (ML).

Semplificando, si può affermare che, attraverso questi algoritmi di apprendimento, la macchina impara dall'esperienza e dai dati dell'ambiente esterno, migliorando progressivamente le proprie prestazioni e capacità.[11]

Esistono tre principali modalità di apprendimento, che differiscono sia per gli algoritmi utilizzati, sia in base allo scopo per il quale il sistema di IA viene programmato.[12]

---

[9] *Ibidem.*

[10] Sito web: intelligenzaartificiale.it

[11] *Ibidem.*

[12] Per la descrizione di tutti i meccanismi di apprendimento della macchina si veda: A. AZZUTTI, W. G. RIING, H. S. STIHEL, *Machine learning, Market Manipulation and Collusion on capital markets why the "Black Box" matters*, in *University of Pennsylvania Journal of International Law,* 2021.

Una prima tipologia è detta *supervised learning*: all'algoritmo vengono forniti dati empirici già classificati, nozioni specifiche codificate, modelli ed esempi che permettono alla macchina di creare un vero e proprio *database*. La macchina viene "addestrata" attraverso l'abbinamento di *outputs* attesi a diversi *clusters* di dati. Di conseguenza quando essa si troverà ad affrontare un problema non farà altro che scegliere il tipo di risposta più adeguata tra quelle già fornite: in questo caso quindi l'*output* generato dalla macchina è del tutto prevedibile. L'apprendimento supervisionato infatti è detto anche *rules based.* Questo tipo di tecnologia viene utilizzato soprattutto per finalità di classificazione di grandi quantità di dati o di previsione statistica di eventi futuri.

Una seconda categoria di apprendimento della macchina consiste nell'*unsupervised machine learning:* in questo caso alla macchina non viene fornita una classificazione o un insieme di regole, ma semplicemente la possibilità di attingere a una grande quantità di dati. Dovrà essa stessa dedurre dei modelli sulla base delle informazioni raccolte, e una volta catalogati i dati imparare il loro significato, il loro utilizzo e adattare il proprio comportamento di conseguenza. Questa modalità di apprendimento è sicuramente maggiormente efficiente, ma inizia a presentare alcuni problemi di trasparenza e di prevedibilità proprio perché, da una parte, non è noto esattamente sulla base di quali scelte la macchina arrivi alla classificazione; d'altra parte, l'*output* non fa più parte di un elenco di opzioni possibili, ma viene trovato in autonomia dalla macchina.

La terza tipologia di apprendimento è detta *reinforcement learning*: il programma impara attraverso processi di *trial-error* in un ambiente incerto e dinamico. Alla macchina viene fornito un obbiettivo da perseguire e viene dotata di una serie di strumenti che le permettono di comprendere le caratteristiche dell'ambiente in cui si trova ad operare: sensori, telecamere, GPS o altri sistemi che consentano di raccogliere dati ed effettuare le scelte più opportune per il perseguimento dell'obbiettivo.

L'ultima metodologia di apprendimento descritta è senza dubbio la più evoluta ed efficace, ma anche quella che presenta maggiori problematicità dal punto di vista della prevedibilità del risultato.

Recentemente, inoltre, è stata sviluppata una nuova tecnologia che interessa i sistemi di IA e che, applicata alla tipologia di ML più avanzata, dà origine ad uno scalino ulteriore nello sviluppo delle macchine intelligenti. Si tratta del *deep learning*: un sistema che,

basandosi sul funzionamento della mente umana, emulata attraverso vere e proprie *reti neurali artificiali*, cerca di ricrearne i vari livelli di astrazione.

Un cervello umano, infatti, quando riceve una nozione, la approfondisce e la astrae; si immagini poi di ricevere una definizione di *un'altra* nozione che presuppone la prima: a questo punto la mente umana raccoglie l*'input* della prima informazione e la elabora insieme alla seconda, trasformandola ed astraendola sempre di più. Allo stesso modo il *deep learning* riproduce questo meccanismo su più livelli in un sistema di intelligenza artificiale: semplicemente i dati non sono forniti dall'uomo, ma sono appresi grazie ad algoritmi di calcolo statistico.[13]

Si tratta quindi di un sistema che, riuscendo a classificare sia i dati in entrata che in uscita, sostanzialmente elabora una capacità, simile a quella umana, di creare conoscenze su livelli non lineari e, tramite questa abilità, apprende e perfeziona funzionalità sempre più complesse.

Si arriva quindi allo stadio più evoluto dei sistemi di IA: il *deep reinforcement learning.* La già ampia autonomia permessa dall'apprendimento rinforzato viene qui accentuata dalla capacità di astrazione e dal ragionamento su più livelli che caratterizzano il *deep learning*. Il concetto verrà approfondito in seguito (1.2.1); in questa sede occorre anticipare che, ovviamente, con l'aumentare dell'autonomia della macchina, della sua efficienza e complessità, cresce anche l'opacità nel funzionamento della stessa e risulta sempre più difficile, se non impossibile, prevedere con precisione gli *outputs* delle operazioni.

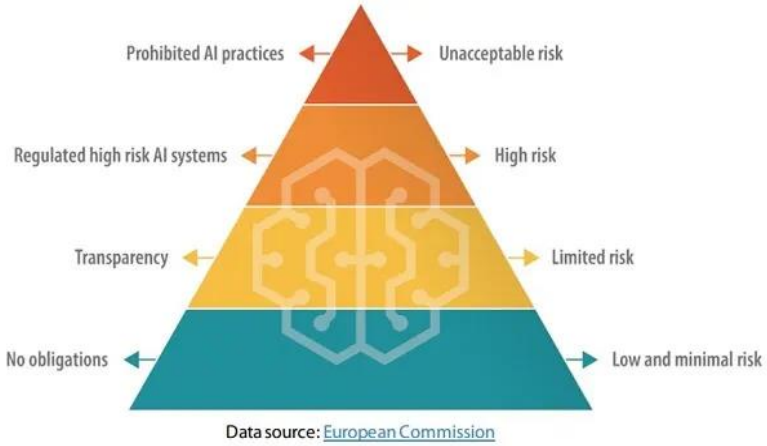
1.1.2 La proposta di Regolamento Europeo sull'IA e la classificazione dei sistemi sulla base del rischio

Descritto brevemente il funzionamento dei sistemi di IA, appare opportuno concentrarsi sulle norme giuridiche che caratterizzano la loro disciplina. A questo proposito si riporta all'attenzione la già citata proposta di Regolamento Europeo sull'IA, comunemente detta *IA Act.*

[13] Y. BATHAEE, *The Artificila Intelligence Black Box and the failure of intent and causation,* in *Harvard Journal of Law & Technology* Volume 31, Number 2 Spring, 2018.

Ai fini della presente trattazione, risulta particolarmente interessante l'impostazione del Regolamento, il quale segue un *risk-based regulatory approach:* vengono stabiliti obblighi giuridici proporzionali al grado di rischio che comporta l'utilizzo dei diversi sistemi di IA.[14]

La proposta infatti divide i vari sistemi di intelligenza artificiale sostanzialmente in quattro categorie, corrispondenti ad altrettanti livelli di rischio.



Al vertice della piramide troviamo le "Pratiche di intelligenza artificiale vietate", disciplinate nel Titolo II. Si tratta di attività ritenute non compatibili con i valori Unione oppure eccessivamente pericolose in quanto creano un rischio inaccettabile in relazione ai diritti fondamentali della persona. Alcuni esempi possono essere: "*l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico*;"[15] oppure *"l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto"*[16], seppur con limitate eccezioni. Un aspetto interessante consiste nel fatto che il legislatore europeo non ha voluto utilizzare, per denominare questa categoria, il termine "sistemi di IA", preferendo invece il termine più generico di "pratiche", proprio per

[14] B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automazione artificiale, cit.*

[15] Art. 5 lett. a, *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione,* 2021, eur-lex.europa.eu

[16] Art. 5 lett. d, *ibidem.*

sottolineare la distanza che l'Unione vuole creare rispetto a queste modalità di utilizzo dell'intelligenza artificiale.

Il secondo livello comprende i sistemi denominati "ad alto rischio", disciplinati nel Titolo III. Il Regolamento dettaglia i vari campi di applicazione e le varie attività dei sistemi di IA rientranti in questa categoria. A titolo esemplificativo si citano le attività di gestione della migrazione, dell'asilo e del controllo delle frontiere, l'amministrazione della giustizia e dei processi democratici, l'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo, le attività di contrasto.[17]

I sistemi ad alto rischio dovranno essere conformi a determinati requisiti. Innanzitutto, dovrà essere istituito, attuato e documentato un sistema di gestione dei rischi. Si tratta di un processo iterativo continuo eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio che richiede un aggiornamento costante e sistematico.[18]

Inoltre, i dati usati per l'addestramento, la convalida e la prova dovranno rispettare caratteristiche di pertinenza, rappresentatività, completezza.

Il Regolamento impone, inoltre, che i sistemi di IA ad alto rischio dovranno essere progettati e sviluppati con capacità che consentano la registrazione automatica degli eventi (*log*) durante il loro funzionamento, utile per ricostruire quanto accaduto in caso di particolari eventi o anche solo per facilitare il monitoraggio successivo all'immissione sul mercato.

Sono disciplinati anche alcuni obblighi di trasparenza e di fornitura di informazioni all'utente per permettere di interpretare *output* e di utilizzare il sistema.

L'articolo 14 inoltre specifica il concetto di "sorveglianza umana": «*I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui il sistema di IA è in uso.*»

Sempre per quanto riguarda questa categoria di sistemi, il legislatore europeo ha delineato un meccanismo di certificazioni al cui vertice è posta un'autorità di notifica, designata o istituita da ogni Stato membro. Questa è responsabile della predisposizione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione degli organismi di valutazione della conformità e si occuperà del loro monitoraggio.[19] L'autorità

[17] ALLEGATO III, *ibidem.*
[18] Art. 9, *ibidem.*
[19] Art. 30, *ibidem.*

di notifica, quindi, verifica che gli organismi abbiano i requisiti organizzativi e di indipendenza necessari per procedere all'attività di valutazione della conformità dei sistemi, e ne monitora l'operato.

Tali organismi invece si occupano di verificare la conformità dei sistemi di IA ad alto rischio rispetto ai requisiti previsti dal regolamento, secondo una procedura dettagliata, diversa per vari tipi di sistemi. Rilasciano quindi un certificato di conformità e al prodotto viene apposta la marcatura CE.

Per quanto concerne i "sistemi ad alto rischio", un ultimo aspetto interessante da analizzare consiste nella previsione di un "monitoraggio successivo all'immissione sul mercato", disciplinato nel Titolo VII. I fornitori, infatti, devono istituire e documentare un sistema di monitoraggio successivo all'immissione sul mercato che sia proporzionato alla natura delle tecnologie di intelligenza artificiale e ai rischi del sistema di IA ad alto rischio. Il monitoraggio consiste nel raccogliere, documentare e analizzare attivamente e sistematicamente i dati pertinenti forniti dagli utenti o raccolti tramite altre fonti sulle prestazioni dei sistemi di IA ad alto rischio, per tutta la durata del loro ciclo di vita e consente al fornitore di valutare la costante conformità dei sistemi di IA ai requisiti di cui al titolo III. [20]

La proposta di Regolamento prevede poi una terza categoria di sistemi di IA che si potrebbero definire "a medio rischio" o "a rischio limitato". Per questi sistemi sono stati previsti solo degli obblighi di trasparenza. Ad esempio, è previsto che «i sistemi di IA destinati a interagire con le persone fisiche siano progettati e sviluppati in modo tale che le persone fisiche siano informate del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo.»[21]

Infine, alla base della piramide immaginata, ci sono i sistemi di IA che non sono menzionati nel Regolamento, che sono stati reputati dal legislatore europeo, se non esenti da rischi, quantomeno implicanti rischi minimi e quindi non necessitanti una particolare disciplina.

[20] Art 61, *ibidem.*
[21] Art 52, *ibidem.*

1.2 L'interferenza dell'intelligenza artificiale con il diritto penale sostanziale: *machina delinquere potest*?

Dopo aver delineato, seppur in modo schematico, il funzionamento dei sistemi di intelligenza artificiale e le prospettive di regolamentazione, appare opportuno soffermarsi sulla rilevanza di questo fenomeno tecnologico in relazione al diritto penale sostanziale.

Infatti, nell'attuale società, l'utilizzo di sistemi di IA è ormai molto diffuso e in alcuni settori si prospetta una crescita quasi totalizzante.

D'altra parte, diventando parte del vivere umano, le cosiddette "macchine intelligenti" hanno iniziato ad essere utilizzate anche per scopi illeciti. Si pensi ad esempio agli attacchi di *spear phishing*: messaggi di posta elettronica fraudolenti elaborati attraverso algoritmi di IA che analizzano le abitudini degli utenti online e, personalizzando la truffa, la rendono molto più difficile da contrastare.[22] Un altro esempio può essere legato ai *social bot*[23] che contribuendo alla proliferazione *dell'hate speach* e alimentando campagne di disinformazione, si rendono talvolta protagonisti di diffamazione o molestie.[24]

Per quanto riguarda il diritto penale, la domanda fondamentale è se i sistemi di IA che materialmente compiono fattispecie di reato possano ancora essere considerati strumenti nelle mani dell'uomo, oppure se, a causa della sempre maggior autonomia, agiscano di fatto in modo sostanzialmente indipendente dal volere umano. Si pensi ad esempio ad un incidente stradale cagionato dall'eccessiva velocità del conducente che abbia esiti mortali per un passante. In questo caso, una volta accertata la colpa (o eventualmente il dolo) del soggetto alla guida, nessuno dubiterebbe né della sua responsabilità penale né tantomeno della natura di mero strumento dell'automobile. Un discorso più problematico potrebbe però riguardare le cosiddette *self-driving cars.* In realtà ad oggi i veicoli in commercio che vengono chiamate "auto a guida semi-automatica" non presentano particolari problemi sotto questo profilo: al massimo l'automobile sarà in grado di auto-guidarsi in condizioni ordinarie, ma il conducente ne conserverà i comandi, per governare situazioni di emergenza. Sono già funzionanti, tuttavia, automobili realmente automatiche in cui scompaiono pedali e volante

---

[22] I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale, cit.*

[23] In merito ai *social bots* si tratterà in modo più approfondito al paragrafo 3.4, in relazione ad aspetti maggiormente legati alla manipolazione del mercato.

[24] A tal proposito esemplare la vicenda del social Twitter "Tay" di Microsoft, che ha rapidamente imparato dall'interazione con gli altri utenti a dirigere *twitters* osceni ad un'attivista femminista.
R. BORSARI, *Intelligenza artificiale e responsabilità penale: le prime considerazioni,* in *Media Laws,* 2019.

e chi si trova all'interno del veicolo versa nella condizione di passeggero.[25] A questo punto, a che titolo potrebbero imputarsi le conseguenze di un eventuale incidente e a chi? Si potrebbe ipotizzare una colpa del soggetto che ha programmato, prodotto o assemblato l'auto, ma in quel caso si dovrebbe dimostrare che l'evento è stato causato da un malfunzionamento della macchina o da una decisione di programmazione riconducibili ad una colpa.

Si può quindi anticipare ciò che si tratterà in modo più approfondito nel paragrafo seguente: il problema della *black box* e del *responsibility gap*. Con il termine *black box*, infatti, ci si riferisce all'imperscrutabilità dei profondi meccanismi e degli aspetti decisionali alla base dei sistemi di IA più avanzati, in particolare in relazione al *deep learning*. Questo aspetto crea problemi legati ad una crisi dei concetti penalistici, come l'elemento soggettivo o la causalità, che potrebbe comportare un pericoloso vuoto di tutela, un cosiddetto *responsibility gap*.

Esistono inoltre ulteriori problematiche relative all'interferenza dell'intelligenza artificiale con il diritto penale. Non legato esclusivamente a questo ambito, ma sicuramente qui particolarmente accentuato, è il cosiddetto "*many-hands-problem"*: il caso in cui la responsabilità penale è da distribuirsi tra diversi "operatori" (programmatori, sviluppatori, collaudatori, produttori, utilizzatori, ecc.) il cui agire concorre, sul versante causale, a produrre l'evento lesivo e in alcuni casi si somma a quello dell'agente artificiale.[26]

Si può concludere quindi che il tradizionale assunto, elaborato già dalla dottrina tedesca sul finire dell'Ottocento e riaffermato come ovvietà in epoca contemporanea, *machina delinquere non potest*, potrebbe iniziare a vacillare. La crescente autonomia dei sistemi di IA, le problematiche connesse al concetto di *black box*, gli svariati problemi di accertamento e il conseguente vuoto di tutela che inizia a stagliarsi come prospettiva per i prossimi decenni ha, infatti, spinto qualche autore ad ipotizzare un sistema di imputazione penale che preveda la perseguibilità e punibilità della macchina come soggetto di diritto.[27]

---

[25] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato,* in *Riv. it. dir. proc. pen.*, vol.63, N°4, 2020.

[26] I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale, cit.*

[27] *infra* paragrafo 2.2.2.

1.2.1 Il *Comportamento emergente* della macchina e la sopravvenienza di un *responsibility gap*: il problema della *Black Box*

Partendo quindi dalla definizione del concetto di *black box,* si può affermare che, nella teoria dei sistemi, un "*modello black box*" consiste in un sistema descrivibile essenzialmente nel suo comportamento esterno, ovvero solo per come reagisce in uscita (*output*) a una determinata sollecitazione in ingresso (*input*), ma il cui funzionamento interno è non visibile o ignoto. È possibile studiarne il comportamento solo attraverso l'osservazione delle risposte che vengono fornite a determinate sollecitazioni.

I sistemi di IA più sofisticati, ad esempio quelli basati sul *deep learning*, sono *black boxes.*

Inoltre, queste tipologie di sistemi presentano un'ulteriore caratteristica che potrebbe sollevare alcuni aspetti problematici dal punto di vista penalistico. Una delle più importanti implicazioni dell'autonomia artificiale, infatti, risiede nella possibilità che tali sistemi possano elaborare soluzioni inaspettate al problema loro assegnato. Tali condotte autonome sono state definite come *comportamento emergente*. [28]

L'insieme di queste due caratteristiche rende, pertanto, il comportamento del sistema di IA da una parte, appunto, potenzialmente imprevedibile anche per gli stessi programmatori e, dall'altra, difficilmente ricostruibile *ex-post* proprio a causa dell'opacità del modello *Black Box*.[29]

Tutto ciò incide in modo significativo sulle dinamiche concernenti la responsabilità penale, nei casi in cui un agente artificiale compie un fatto di reato. I due principali elementi di frizione sono la causalità e l'elemento soggettivo.

Sotto il primo profilo, si può evidenziare che la mancanza di trasparenza nel funzionamento della macchina potrebbe impedire una puntuale ricostruzione della catena causale che ha portato all'evento di reato. Inoltre, c'è chi ha sostenuto che in realtà il danno sul piano causale non sia da ricondurre al fattore umano, ma ad un cosiddetto *fattore robotico*, derivante dal comportamento emergente della macchina, inteso come fattore causale sopravvenuto, interruttivo del nesso causale. [30] Si potrebbe obbiettare, che lo stesso

---

[28] B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automazione artificiale, cit.*

[29] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato,* in *Riv. it. dir. proc. pen.*, vol.63, N°4, 2020.

[30] Y. BATHAEE*, The Artificila Intelligence Black Box and the failure of intent and causation, cit.*

designer è consapevole di questa imprevedibilità dell'*output*. Appellarsi all'interruzione del nesso causale, quindi, non sembra corretto in quanto l'elemento robotico non si è in realtà interposto tra la condotta e l'evento penalmente rilevante, introducendo un rischio qualitativamente diverso da quello *ab origine* concepito.[31] Il comportamento del sistema di IA, invece, costituisce il naturale sviluppo dell*'input*.

È dal punto di vista dell'elemento soggettivo, invece, che si riscontrano le principali criticità. L'utilizzatore della macchina, infatti, potrebbe obbiettare ad un'eventuale contestazione, che il fatto di reato compiuto dal sistema di IA è in realtà totalmente frutto dell'autonomia dell'agente artificiale e, in quanto tale, neppure prevedibile. Di conseguenza l'utilizzatore potrebbe essere considerato incolpevole in relazione all'evento finale prodotto. Un ragionamento simile potrebbe essere avanzato anche da chi ha programmato il sistema di IA: in questo caso, tuttavia, alcuni autori ritengono più facile ipotizzare un rimprovero di natura colposa per non aver inserito nella costruzione del programma un'architettura tale da ostacolare la possibilità che l'agente sviluppasse un "comportamento criminale".[32]

L'obbiezione principale a questa ricostruzione è che se ogni evento cagionato dal sistema, di per sé imprevedibile, venisse rimproverato all'agente perché, *ab initio genericamente prevedibile*, si assisterebbe ad una degenerazione del paradigma colposo che porterebbe ad un'intollerabile semplificazione probatoria: basterebbe una semplice constatazione dell'evento cagionato dal sistema, per un'automatica imputazione nei confronti del "creatore" dello stesso.[33] Questa strada risulterebbe impraticabile proprio a causa di un eccessivo avvicinamento ad una responsabilità oggettiva.

Pertanto, data l'impossibilità di ricostruire un paradigma colposo in capo alle persone fisiche coinvolte nel reato, si potrebbe creare un pericoloso vuoto di tutela penalistica, perché secondo gli ordinari schemi logici del diritto penale, spesso, non si riuscirebbe ad individuare un soggetto responsabile. Questo problema è stato definito dalla dottrina come *responsibility gap* e potrebbe comportare gravi conseguenze in vista del prossimo futuro tecnologico: da tale assunto deriverebbe una pericolosa deresponsabilizzazione per coloro che progettano, sviluppano, producono e utilizzano sistemi di IA dotati di ampia autonomia. Per tale motivo,

---

[31] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato,* in *Riv. it. dir. proc. pen.*, vol.63, N°4, 2020.

[32] B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automazione artificiale, cit*.

[33] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato, cit*.

attraverso diverse soluzioni si è cercato di trovare schemi giuridici che potessero aggirare le problematiche predette, garantendo quindi forme di tutela. Di tali proposte si tratterà nel seguente paragrafo.

In ogni caso, risulta necessario precisare che i problemi penalistici in questione non possono essere liquidati con una semplice constatazione di un generale vuoto di tutela. Da una parte, infatti, potrebbero rilevare, a livello di dissertazione teorica, sia le peculiarità del sistema di IA in relazione al suo ambito di applicazione, sia la formulazione testuale della fattispecie di reato. Questi elementi potrebbero, infatti, portare a ragionamenti e conclusioni differenti. D'altra parte, per quanto riguarda la fattispecie concreta, non è da trascurare l'eventualità in cui gli elementi probatori raccolti possano condurre al superamento, sul piano dell'accertamento, di problematiche dogmatiche apparentemente insormontabili.[34] Si tratterà in seguito il declinarsi di questi aspetti, accennati in questa sede in via generale, nell'ambito della fattispecie oggetto del presente lavoro: il reato di manipolazione del mercato realizzato attraverso sistemi di High Frequency Trading.

1.2.2 Le soluzioni proposte

a) La responsabilità diretta dell'IA: la teoria di Hallevy e le critiche

Rispetto alle problematiche relative al *responsibility gap*, sono state ipotizzate diverse soluzioni. Alcune di queste, in realtà provenienti da una minoritaria dottrina di *common law,* cercano di superare le difficoltà di imputazione proponendo una responsabilità penale diretta della macchina.

Il primo e principale sostenitore di questa teoria è Gabriel Hallevy, avvocato e professore di Diritto Penale presso l'*Ono Academic College* in Israele, che ritiene che in realtà non vi sia alcun motivo per cui i meccanismi di imputazione penale tipici del *common law* non possano operare anche nei confronti di agenti artificiali intelligenti che compiono fatti di reato.[35]

L'autore, innanzitutto, ritiene che l'elemento oggettivo del reato, l'*actus reus* – inteso in realtà in termini meramente materialistici negli ordinamenti di *common law*– possa essere perfettamente rappresentato da un sistema di IA, sia per quanto riguarda una condotta attiva,

[34] Si veda a titolo esemplificativo il caso Coscia, trattato *infra* al § 3.2.2.
[35] G. HALLEVY, *Liability for Crimes Involving Artificial Intelligence Systems*, Berlino, 2015, 47 ss.

come ad esempio il movimento di un braccio robotico, sia per quanto riguarda un'omissione della macchina.

In secondo luogo, per quanto riguarda il profilo psicologico, secondo Hallevy, i sistemi di IA di ultima generazione potrebbero avere caratteristiche tali da far sì che il loro agire possa integrare alcune forme di *mens rea,* in particolare la *negligence* o addirittura il *general intent*, categoria dottrinale che comprende *intention*, *knowledge* e *recklessness*.[36]

Infatti, i sistemi di IA più avanzati, acquisendo dati dal mondo esterno e rielaborandoli, "si rappresentano" la realtà. Inoltre, grazie a processi di *decision making*, questi agenti artificiali riescono a valutare la probabilità che un determinato evento possa verificarsi e direzionano il proprio operato di conseguenza: in questo senso possono "prevedere" e "volere" un determinato risultato. Infine, si potrebbe configurare una *recklessness* quando il sistema non abbia considerato una possibilità che invece avrebbe dovuto essere compresa in base ai dati raccolti, oppure in caso di semplice errore di calcolo.

Per l'autore, quindi, è superfluo che le macchine non possano provare emozioni o sentimenti: questi sarebbero irrilevanti ai fini del dolo.

Hallevy, infine, pone un parallelismo tra la convinzione che le macchine non possano essere ritenute penalmente responsabili di un reato e il tradizionale, diffuso scetticismo rispetto alla responsabilità penale delle persone giuridiche. L'assioma *societas delinquere non potest* è stato, come è noto, superato, ma solo dopo un lungo percorso iniziato negli ordinamenti di *common law* che ha portato all'affermazione di una *corporate liability.* Una delle tradizionali argomentazioni contro la responsabilità penale gli enti consisteva nell'affermare che una società non potesse avere *"a body to kick and a soul to be damned"*[37]; invece i sistemi di IA spesso hanno un *hardware* e quindi un metaforico "corpo" su cui infliggere la pena.

L'autore, in conclusione, ritiene che già attualmente vi sarebbero tutti i presupposti per poter creare un sistema di responsabilità penale diretta della macchina: l'unico ostacolo sarebbe lo stesso pregiudizio antropocentrico che un tempo si opponeva anche alla responsabilità penale delle persone giuridiche.

---

[36] R. BORSARI, *Intelligenza artificiale e responsabilità penale: le prime considerazioni,* in *Media Laws*, 2019.

[37] Espressione attribuita a Edward Thurlow (1731-1806), Lord Chancellor of Great Britain, divenuta nota nel dibattito angloamericano sulla *corporate liability*.

Le numerose critiche che sono state sollevate nei confronti di questa teoria della responsabilità diretta della macchina possono essere riassunte in tre principali obbiezioni. [38]

Il primo punto riguarda l'assenza del requisito della colpevolezza in capo agli agenti artificiali intelligenti: essi non sono liberi di autodeterminarsi, di porsi obbiettivi egoistici e di perseguirli anche a costo di ledere beni giuridici altrui. Sono invece guidati dalle istruzioni di programmazione, nonostante il loro comportamento abbia un margine di imprevedibilità. Pertanto, l'agire dei sistemi di IA non può essere definito colpevole, nel senso di rimproverabile.

In secondo luogo, si obbietta ad Hallevy che il sistema da lui costruito porterebbe a una perdita del senso e delle funzioni della pena. Anche se, in seguito ad una condanna della macchina, si volesse infliggere persino lo spegnimento o la distruzione della stessa, tale sanzione non risponderebbe a nessuna funzione tipica della pena. Le macchine, infatti, non possono provare timore e quindi non si assolverebbe a nessuno scopo dissuasivo. Inoltre, verrebbe meno anche la funzione rieducativa in quanto il sistema di IA non è in grado di apprendere alcunché dalla sanzione irrogata, se non attraverso un'implementazione dei meccanismi di *machine learning*, che comunque non potrebbe essere imposta senza il consenso del destinatario. A questo proposito c'è però chi, pur in minoranza, sostiene che una sanzione inflitta a un sistema di IA potrebbe costituire per la macchina un dato che le consentirebbe di apprendere le conseguenze di un comportamento sbagliato. I meccanismi di *deep learning* potrebbero così favorire "l'addestramento" della macchina, in un'ottica quasi rieducativa.[39]

Infine, l'ultima critica riguarda la fallacia del parallelismo con la *corporate liability.* Infatti, la società, pur essendo una persona giuridica e, in quanto tale, un'entità fittizia e materialmente inesistente, è comunque costituita da persone fisiche. Il sistema di IA, invece, spesso ha una vera e propria fisicità. Inoltre, l'uomo si limita a crearlo e programmarlo, ma non costituisce un elemento necessario per l'esistenza della macchina. Questa scissione tra soggetto "creatore" e "creato" si manifesta nel fatto che, a differenza di quanto avviene per

[38] Per le critiche alla ricostruzione di Hallevy si vedano tra gli altri: A. CAPPELLINI, *Machina delinquere non potest,* in www.discrimen.it, 2019; R. BORSARI, *Intelligenza artificiale e responsabilità penale: le prime considerazioni,* in *Media Laws*, 2019; C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato,* in *Riv. it. dir. proc. pen*, vol.63, N°4, 2020.

[39] U. RUFFOLO, *XVI lezione: machina delinquere potest*, in *XXVI lezioni di diritto dell'intelligenza artificiale* a cura di U. Ruffolo, Torino, Giappichelli ed., 2020, p.295.

le società, qualunque afflizione si imponga al soggetto artificiale non è di per sé in grado di intaccare gli interessi delle persone fisiche che si trovano alle sue spalle.

b) Due opzioni possibili: il divieto di utilizzo oppure la gestione del rischio consentito

Data quindi l'inapplicabilità, ad oggi, della teoria della responsabilità diretta del sistema di IA, alcuni autori si sono interrogati sulle ulteriori eventuali soluzioni rispetto al descritto vuoto di tutela che si staglia nel prossimo futuro.

Le strade prospettate sono sostanzialmente due. Da una parte troviamo il divieto *tout court* dell'attività, ispirato a logiche di precauzione in relazione a possibili danni imprevedibili e ingovernabili. In questo modo però, si rischierebbe di bloccare il progresso tecnologico e, soprattutto, di rinunciare a tutti i benefici sociali che deriverebbero dall'utilizzo e dallo sviluppo della robotica e dell'intelligenza artificiale.

La seconda via, invece, prevede la regolamentazione del fenomeno attraverso l'individuazione e la gestione di un'area di rischio consentito.

Questa strategia in realtà è comunemente utilizzata per disciplinare ambiti e fenomeni del vivere sociale che sono caratterizzati da fattori particolarmente pericolosi. In realtà, ogni azione comporta un rischio, quindi il problema sarà costituito dalla gradazione del rischio, dal tollerabile all'inammissibile.

Con l'espressione "rischio consentito" generalmente si indicano due concetti differenti. Da una parte si fa riferimento ad attività pericolose, ma la cui esecuzione è lecita se l'agente osserva determinati accorgimenti. Dall'altra, invece, ci si riferisce ad un'area più ridotta in cui in cui confluiscono condotte pericolose non completamente schermabili da cautele: si tratta del rischio che residua dall'adozione di tutte le profilassi del caso.[40] Il secondo significato è quello maggiormente rilevante in questo contesto: il rischio consentito consisterebbe, infatti, in un'area individuata dal legislatore all'interno della quale la responsabilità sociale di determinati eventi dannosi verrebbe sopportata da quest'ultimo senza procurare conseguenze penalistiche per alcun agente.

Nell'individuare il perimetro dell'ammissibile, e quindi stabilire il confine tra la liceità o illiceità di una condotta, il legislatore dovrà tenere conto di numerosi fattori, quali l'utilità

[40] F. CONSULICH, *Rischio Consentito,* in *Enc. dir.,* p.1102 ss, Giuffrè, 2021.

che deriverebbe da quella condotta, la frequenza del danno e la sua misura. Inoltre, è indubbia l'influenza che avrà in questa scelta la sensibilità politica del momento.[41]

Nel delimitare quindi l'area del rischio occorre dare precise regole di comportamento a contenuto cautelare, necessarie anche per garantire la prevedibilità della responsabilità penale in relazione alla scelta di avviare un'attività pericolosa. Tuttavia, il legislatore non può prevedere ed esplicitare ogni singola cautela, sicché assume estrema importanza l'attività di organi tecnici, sotto forma di linee guida, *soft laws* e raccomandazioni.

Nell'ambito dell'intelligenza artificiale, quindi, la strada che sembra trovare maggior favore sembra proprio quella di consentire il fenomeno, favorire il progresso tecnologico e beneficiare degli innumerevoli vantaggi che ne derivano, ma al contempo disciplinarlo, ponendo delle norme cautelari e stabilendo un confine al di là del quale il rischio non può più essere accettato.

In dottrina, alcuni autori suggeriscono un sistema di autorizzazioni in relazione alla produzione, al commercio e all'utilizzo di questi sistemi[42], altri invece propongono di focalizzarsi sulle fasi di *design* e produzione formulando dei regimi di imputazione della responsabilità penale nell'ambito dell'IA che superino, almeno in parte, le problematiche menzionate precedentemente. [43]

In ogni caso sembra che la strategia normativa del rischio consentito, almeno come primo livello di soluzione del problema, sia stata accolta con favore dalle Istituzioni dell'Unione. Essa, quando si è trovata a regolamentare per la prima volta il fenomeno dell'IA, ha strutturato l'intero regolamento proprio sulla base di un *risk-based approach.* [44]

---

[41] *Ibidem.*

[42] I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale, cit*.

[43] B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automazione artificiale, cit*.

[44] *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione*, 2021, eur-lex.europa.eu

CAPITOLO II
HIGH FREQUENCY TRADING

SOMMARIO: 2.1 Dal trading algoritmico a quello ad alta frequenza – 2.1.1 Gli interventi regolatori che hanno portato all'esplosione del fenomeno; le "*dark pools*"– 2.1.2 L'identificazione e la definizione degli High Frequency Traders– 2.2 Il funzionamento del trading ad alta frequenza e le principali strategie utilizzate – 2.2.1 Le strategie più aggressive: *Pinging*, *Layering*, *Spoofing* e *Quote Stuffing* – 2.3 Gli effetti distorsivi e i rischi del trading ad alta frequenza – 2.3.1 Flash Crash: 10 maggio 2010, il caso Dow Jones – 2.3.2 I fenomeni successivi e il recente *flash crash* di Stoccolma (maggio 2022) – 2.4 Il quadro giuridico europeo per il trading ad alta frequenza

2.1 Dal trading algoritmico a quello ad alta frequenza

Dopo aver analizzato le principali caratteristiche dei sistemi di IA, ci si può soffermare sulle applicazioni di tali tecnologie all'ambito finanziario, in particolare in relazione alle operazioni di compravendita sul mercato azionario.

A questo proposito appare opportuno citare, come precursore del *trading* ad alta frequenza*,* il fenomeno dei *SOES bandits*, diffusosi negli anni '90 soprattutto sul *Nasdaq*. Si trattava di *traders* che effettuavano centinaia di operazioni al giorno con lo scopo di trarre vantaggio da minime oscillazioni di prezzo degli strumenti finanziari o dai ritardi nell'aggiornamento dei prezzi.[1]

Successivamente, con l'evoluzione tecnologica e lo sviluppo di *hardware* sempre più potenti, si diffonde una nuova tipologia di *trading*: il *Trading Algoritmico* (AT).

Attraverso questo metodo, i parametri relativi al compimento delle operazioni sono determinati da algoritmi che, specificando *timing*, prezzo e quantità degli ordini, eliminano la componente emotiva e comportamentale dell'attività.[2]

L'High frequency Trading (HFT) è un particolare tipo di trading algoritmico, caratterizzato dall'incredibile velocità con cui vengono analizzati i dati o segnali del mercato, utilizzati poi per inviare o aggiornare un gran numero di ordini entro un tempo brevissimo.[3] Si tratta di un sistema programmato in modo tale da eseguire le proprie strategie

[1] A. PUORRO, *High Frequency Trading: una panoramica,* in *Questioni di Economia e Finanza (Occasional Papers)*, CONSOB, 2013.
[2] *Ibidem.*
[3] Direttiva 2014/65/UE del Parlamento europeo e del Consiglio (MIFID II), Considerando n. 61.

in maniera autonoma: tale sistema analizza il mercato e trasmette migliaia di ordini di acquisto e di vendita al secondo. Al contempo, inserisce ordini di cancellazione o sostituzione che si adattano immediatamente al flusso informativo disponibile.[4] La velocità di questi sistemi è tale che le operazioni possono essere eseguite in tempistiche riconducibili ad ordini di grandezza di micro-secondi: centomila volte più velocemente di un battito di ciglia.[5]

Il profitto del sistema di HFT è il risultato di una velocità operativa che permette di sfruttare sbilanciamenti di liquidità o piccole inefficienze di prezzi, non percepibili per gli operatori ordinari: rispetto alla singola operazione il guadagno è minimo, ma diventa ingente tenuto conto dell'enorme mole di scambi effettuati ogni secondo.

Questo vantaggio competitivo di tipo tecnologico è il prodotto della coesistenza di due differenti caratteristiche: bassa latenza (*Low Lantency*) e *Co-Location*.[6]

Per latenza si intende il tempo necessario per tramutare una decisione economica in un'effettiva contrattazione. A questi fini si prendono in considerazione diversi momenti. Innanzitutto, la velocità con cui i *traders*, dopo aver ricevuto un dato dal mercato, lo processano e lo sfruttano per compiere scelte di investimento; in secondo luogo, il tempo di predisposizione dell'ordine e della sua ricezione da parte del *broker*; ancora, il tempo di processazione da parte del *broker* e dell'invio dell'ordine alla piattaforma di contrattazione; infine, il tempo tra la ricezione da parte del mercato e il momento in cui il mercato lo divulga.[7]

I sistemi di HFT riescono a ridurre al minimo il tempo di latenza e quindi a sfruttare inefficienze e opportunità dei mercati, altrimenti nemmeno percettibili.

La caratteristica della *Co-Location* invece è relativa alla vicinanza fisica del *trader* ad alta frequenza ai *server* del mercato. Gli ordini di borsa, infatti, sono semplicemente impulsi elettrici che, pur viaggiando a velocità altissime, trovano un limite nello spazio. Il fatto che l'*harware* di un sistema di HFT sia fisicamente più vicino ai *server* del mercato rispetto a

[4]F.J. FABOZZI, S.FOCARDI, C.JONAS, *Investment Management after the Global Financial Crisis*, The Research Foundation of CFA Institute, 2010.
[5] O. KAYA, *High-frequency trading, reaching the limits*, Research Briefing Global financial markets, Deutsche Bank Research, Frankfort, 2016.
[6] A. PUORRO, *High Frequency Trading: una panoramica, cit.*
[7] *Ibidem.*

quello, sempre ad alta frequenza e ugualmente potente, di un suo concorrente costituisce un vantaggio notevole in termini di profittabilità.[8]

I principali mercati hanno, quindi, iniziato a fornire un particolare tipo di servizio: i locali adiacenti ai *server* vengono concessi in locazione alle agenzie di *trading,* proprio per il collocamento di sistemi ad alta frequenza.[9]

I due aspetti appena visti, congiuntamente all'estrema potenza degli *hardware* degli HFT, sono alla base del vantaggio tecnologico che tali sistemi porta ad essere estremamente più competitivi rispetto al tradizionale *trader* fisico.

2.1.1 Gli interventi regolatori che hanno portato all'esplosione del fenomeno; le "dark pools"

Da un punto di vista storico possiamo dire che il primo intervento regolatore che ha favorito lo sviluppo del *trading* ad alta frequenza è stata la decisione della *Securities and Exchange Commission* (SEC) che ha permesso, all'inizio degli anni '90, l'utilizzo degli *Electronic Communications Networks* (ENC). Si tratta di un sistema di trading diverso e alternativo ai mercati regolamentati che, utilizzando una rete elettronica che abbina automaticamente gli ordini, permette a venditori e compratori di incrociare le proprie offerte senza dover passare attraverso i tradizionali servizi di *broker-dealer.* [10]

Tuttavia, la principale debolezza di questi sistemi consisteva nel fatto che tra gli ECN e i mercati regolamentati fosse presente una cosiddetta *chinese wall*: i due sistemi di negoziazione rimanevano separati e indipendenti, senza nessun obbligo di trasmettere gli ordini. La conseguenza rilevante consisteva nel fatto che il miglior prezzo presente sull'ECN poteva non essere anche quello presente in generale sul mercato, portando alla creazione di possibili quotazioni diverse per gli stessi strumenti finanziari.

Tale inefficienza è stata eliminata con un intervento normativo negli Stati Uniti. Il *Regulation National Market System* del 2005 ha risolto il problema con due disposizioni specifiche: la *Sub Penny Rule* e la *Order Protection Rule.*

La *Sub Penny Rule*, o *Rule 612*, "*vieta ai partecipanti al mercato di visualizzare, classificare o accettare quotazioni, ordini o indicazioni di interesse in qualsiasi titolo NMS*

[8] *Ibidem.*
[9] Il primo e più grande mercato ad offrire accordi di *co-location* è stato *NYSE Euronext*, ma il servizio si è subito diffuso in tutti i più importanti mercati mondiali.
[10] A. PUORRO, *High Frequency Trading: una panoramica, cit.*

con un incremento inferiore a $0,01 se la quotazione, l'ordine o l'indicazione di interesse ha un prezzo pari o superiore a $1,00 per azione. Se la quotazione, l'ordine o l'indicazione di interesse ha un prezzo inferiore a $1,00 per azione, l'incremento minimo del prezzo è di $0,0001."[11] Lo scopo è quello di ridurre e rendere univoco il minimo incremento possibile dei prezzi delle azioni. Restringendo il *bid-ask spread*, è possibile sfruttare il minimo intervallo possibile di profitto: il rischio, in una strategia di *trading* di questo tipo diminuisce e, di conseguenza, il fenomeno si diffonde.[12]

L'*Order Protection Rule* è finalizzata a prevenire il fenomeno del *trade-through*, ossia l'esecuzione di operazioni a prezzi inferiori alle quotazioni protette.[13] A tal fine, la regola impone che ogni ordine immesso su un mercato regolamentato o su un ECN debba essere necessariamente eseguito al NBBO (*National Best Bid Offer*).[14]

Nel mercato europeo alcune di queste innovazioni sono state introdotte dalla Direttiva Europea 2004/39/EC (MIFID). In particolare, è stato rimosso l'obbligo di concentrazione degli scambi nei soli mercati regolamentati, aprendo la strada alle *Multilateral Trading Facilities* (MTF), assimilabili agli ECN statunitensi. Inoltre, è stato inserito l'obbligo della *best execution* che impone ai *broker* di cercare le opzioni più favorevoli per eseguire gli ordini dei clienti nell'ambito del contesto di mercato prevalente.[15]

Un'ulteriore innovazione che ha favorito lo sviluppo dell'HFT è la creazione dello *Smart Order Reuting* (SOR). A causa dell'obbligo di concludere le operazioni al NBBO (o al *best price* in Europa), si è reso infatti necessario un sistema che potesse connettere tutte le *trading venues*, mercati regolamentati e non, per comparare, in modo automatico e in tempo reale, i prezzi e le quantità degli strumenti finanziari. Il SOR quindi, in base ad un *set* di regole, garantisce l'esecuzione degli ordini al prezzo migliore presente su tutti i mercati, riducendo al minimo l'inefficienza del sistema.[16]

---

[11] Disponibile al seguente link https://www.sec.gov/divisions/marketreg/subpenny612faq.htm

[12] T. ČUK, A. VAN WAEYENBERGE, *European Legal Framework for Algorithmic and High Frequency Trading (Mifid 2 and MAR), A Global Approach to Managing the Risks of the Modern Trading Paradigm,* in Cambridge University Press, Cambridge**,** 2018.

[13] Disponibile al seguente link https://www.sec.gov/divisions/marketreg/nmsfaq610-11.htm

[14] Il NBBO consiste nel miglior prezzo di acquisto e vendita di uno strumento finanziario presente in qualsiasi momento sull'intero mercato, compresi gli ECN. Già nel 1997 la SEC era intervenuta per migliorare la trasparenza del mercato inserendo l'obbligo per i Market Maker di mostrare quale fosse il NBBO (obbligo del *Limit Order Display*).

[15] In Investopedia.com

[16] A tal fine il SOR permette anche di scomporre lo stesso ordine a livello quantitativo tra diverse *trading venus* per eseguire ogni frazione dell'ordine stesso al miglior prezzo disponibile in quel momento.

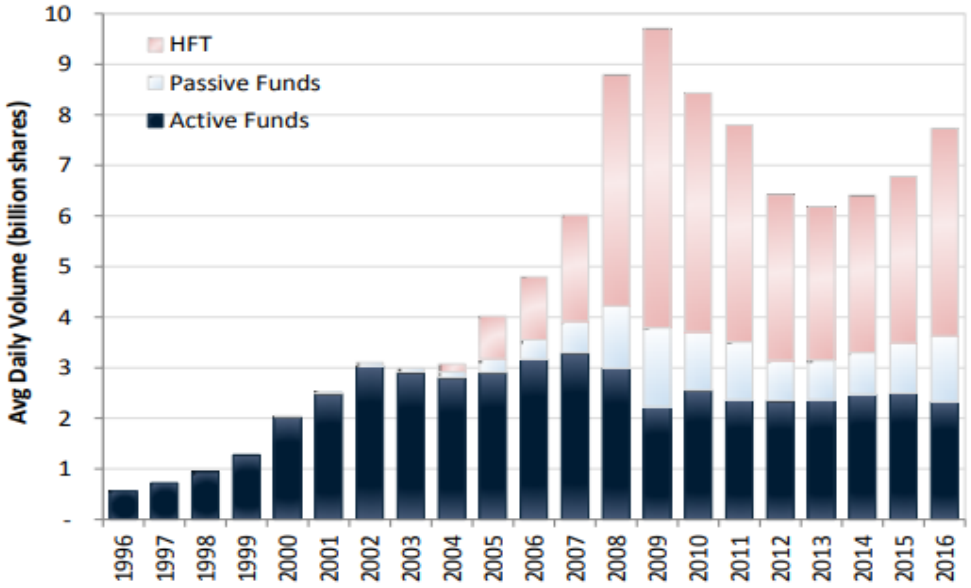
È da tenere presente che in seguito all'abolizione da parte dei governi nazionali (tramite la *Regulation NMS*, negli Stati Uniti, o della direttiva MIFID, in UE) dell'obbligo di concentrazione degli scambi nei mercati regolamentati, le banche hanno iniziato a creare varie piattaforme di negoziazione alternative, dotate di una regolamentazione molto meno severa e caratterizzate da anonimato e mancanza di trasparenza. Si tratta delle cosiddette *Dark Pools*. Tali *trading venues* permettono all'operatore di decidere volumi, prezzi e quantità dell'ordine, senza l'obbligo di informare gli altri operatori: queste informazioni rimangono private. Il sistema è molto utile per gli investitori istituzionali che possono sfruttare l'anonimato per immettere ordini di grandi dimensioni senza il pericolo di un impatto sul mercato. Infatti, quando nei mercati regolamentati un investitore istituzionale immette un ordine di ingenti dimensioni, crea un movimento del mercato a suo sfavore, soprattutto quando si tratta di titoli poco liquidi. Nelle *dark pools* invece questo succede in misura molto minore, perché non si sa chi sta effettuando la transazione e a che prezzo.[17]

Le caratteristiche delle *dark pools* permettono di massimizzare il profitto delle strategie di investimento utilizzate dai sistemi di HTF, i quali sfruttano le asimmetrie informative e gli arbitraggi, ovviamente amplificati dalla poca trasparenza offerta da queste *trading venues*. Pertanto, la diffusione di queste piattaforme di negoziazione ha portato all'esplosione del fenomeno dei sistemi di trading ad alta frequenza.[18]

Dai primi anni duemila, infatti, la diffusione dei sistemi di HFT è cresciuta esponenzialmente e, in seguito ad un breve ridimensionamento del fenomeno dopo l'entusiasmo iniziale, si è assistito ad un nuovo incremento dei volumi. Si può affermare che oggi il trading ad alta frequenza occupi un ruolo tutt'altro che marginale nei mercati finanziari globali.

[17] E. MARRO, *Quanto c'entra la finanza ombra con il crollo delle borse?,* 2016, ilsole24ore.com
[18] *Ibidem.*

Scomposizione volume degli scambi negli Stati Uniti



(Fonte: Credit Suisse Trading Strategy, 2017)

Quota di scambi HFT sul totale degli scambi azionari

Stati Uniti	55%
Europa	35%
Giappone	28%
Australia	20%
Canada	18%
Asia	12%
Brasile	6%

(Fonte: Banca d'Italia, 2013)

2.1.2 L'identificazione e la definizione degli High Frequency Traders

Seguendo le definizioni proposte in letteratura, l'HFT è un *trading* di tipo prevalentemente proprietario, con periodi di detenzione molto brevi. È caratterizzato dall'invio di un grande numero di ordini che vengono cancellati quasi subito, dall'assunzione di posizioni neutre alla fine della giornata di contrattazione e dall'utilizzo di servizi di collocazione per ridurre i tempi di latenza.[19]

[19] A. BOUVERET, C. GUILLAUMIE, C. A. ROQUEIRO, C. WINKLER, S. NAUHAUS, *High-frequency trading activity in EU equity markets*, Economic Report, ESMA, 2014.

Mancando, tuttavia, un sistema di identificazione univoco per questo fenomeno, esistono diversi tipi di approccio che tengono in considerazione solo alcune delle caratteristiche menzionate. In particolare, l'ESMA, nell'ambito di uno studio relativo all'attività di High frequency Trading nei mercati azionari, descrive due principali opzioni: un approccio diretto e un approccio indiretto. [20]

Tra gli approcci diretti possiamo identificare due metodologie per identificare gli High Frequency Traders: distinguere sulla base della tipologia primaria di *business* oppure in relazione all'uso di servizi utili a minimizzare la latenza.

L'identificazione sulla base della tipologia primaria di *business* prende in considerazione solo le imprese che realizzano un HFT "puro", quindi che svolgono esclusivamente questo tipo di attività. Restano di conseguenza escluse tutte quelle imprese impegnate anche in altre attività, come l'*investment banking*. Questa strategia prevede un elemento di sottostima da una parte, ma dall'altra anche di sovrastima perché gli HFT "puri" possono comunque operare con strategie non ad alta frequenza.

Una seconda strada prevede invece di identificare i *traders* ad alta frequenza sulla base dell'utilizzo delle infrastrutture di *co-location* che permettono di minimizzare la latenza. Anche in questo caso le statistiche potrebbero risultare distorte perché tali servizi potrebbero essere utilizzati da altri soggetti, ad esempio da *brokers* che operano esclusivamente per i propri clienti (*agent trading*) per offrire loro strategie di *best execution*, mentre invece l'HFT si caratterizza in quanto negoziazione per conto proprio. La soluzione potrebbe essere quella di focalizzarsi solo sul trading proprietario, ma risulta particolarmente difficile dato che il *flag* per il *trading* proprietario o per l*'agency trading* non sono del tutto coerenti tra le diverse piattaforme di negoziazione e tra i vari stati.

Gli approcci indiretti invece si basano sull'analisi del *trading* effettuato dal partecipante al mercato. Possiamo distinguere tre metodologie: *Intraday inventory management, Lifetime of orders* e *Message traffic.*

Utilizzando la prima strategia, si considerano le operazioni effettuate nella giornata di contrattazione e le posizioni raggiunte dai singoli operatori. Ad esempio, potrà essere identificato come HFT un partecipante al mercato che abbia chiuso le posizioni in un breve arco temporale, le cui contrattazioni abbiano volumi molto elevati e che, il giorno dopo, acquisti strumenti finanziari con quotazioni simili a quelli già acquistati.

[20] *Ibidem.*

Il metodo basato sul *Lifetime order* consiste nell'analisi di tutto ciò che succede nell'arco temporale che va dall'immissione dell'ordine alla sua esecuzione. Sarà identificato come HFT quindi un operatore che chiude le posizioni in frazioni di secondo.

Infine, si può analizzare la quantità di ordini generata attraverso il *Message traffic.* Quest'ultima strategia è effettivamente alla base di un indicatore di mercato molto utilizzato negli Stati Uniti, particolarmente efficace nel verificare la presenza e la diffusione del fenomeno di negoziazioni ad alta frequenza. Si tratta dell'*order to trade ratio* (OTR), che misura il rapporto tra il numero di ordini immessi rispetto a quelli eseguiti, e viene calcolato sia per il singolo operatore che in forma aggregata in relazione al mercato.[21] La maggior parte delle strategie di *trading* degli HFT consiste infatti nell'immissione e cancellazione di ordini; pertanto, attraverso l'OTR è possibile determinare la diffusione e la concentrazione degli operatori ad alta frequenza.

In realtà l'ESMA appare contraria all'utilizzo del OTR per identificare gli HFT, in quanto questo potrebbe portare ad alcune alterazioni statistiche per tre ordini di motivi. In primo luogo, questo approccio non rivelerebbe tutte le strategie del trading ad alta frequenza; ad esempio, quelle basate sull'arbitraggio statistico potrebbero non presentare un OTR elevato. In secondo luogo, anche gli algoritmi utilizzati dalle imprese per l'*agency trading* per conto di investitori istituzionali possono presentare un OTR elevato e quindi essere erroneamente qualificati come HFT. In terzo luogo, alcune imprese potrebbero aver eseguito solo poche operazioni nonostante l'invio di ordini, soprattutto quando la negoziazione ha per oggetto strumenti finanziari poco liquidi.[22]

ESMA, nel suo rapporto, dichiara di utilizzare invece un approccio "misto": considererà sia le stime effettuate con un approccio diretto, in particolare *HFT flag*, sia quelle realizzate con l'approccio indiretto del *Lifetime of orders*.

2.2 Il funzionamento del trading ad alta frequenza e le principali strategie utilizzate

Analizzate le caratteristiche del trading ad alta frequenza, appare opportuno soffermarsi brevemente sui meccanismi operativi di tali sistemi nei mercati.

---

[21] A. PUORRO, *High Frequency Trading: una panoramica, cit*.

[22] A. BOUVERET, C. GUILLAUMIE, C. A. ROQUEIRO, C. WINKLER, S. NAUHAUS, *High-frequency trading activity in EU equity markets*, Economic Report, ESMA, 2014.

Il fondamento di queste strategie consiste nello sfruttamento dei cosiddetti "arbitraggi di latenza": inefficienze del mercato che portano a divergenze di prezzo per lo stesso strumento finanziario. Grazie alla capacità degli HFT di ridurre al minimo i tempi di latenza, gli arbitraggi vengono utilizzati per ottenere guadagni sostanzialmente privi di rischio.[23]

I meccanismi di *machine learning* alla base del funzionamento dei sistemi di *trading* ad alta frequenza comportano una costante ricerca di strategie diverse e nuove: risulta difficile individuare e classificare tutti i meccanismi operativi utilizzati. Tuttavia, data la tendenza dei sistemi di IA ad "imparare" dal comportamento degli altri operatori del mercato, si è riusciti a identificare alcune strategie che risultano frequenti in questo tipo di *trading*.

Una di queste, ad esempio, consiste nel *Trading on news* (o *Momentum trading*), strategia che si basa sullo sfruttamento dell'effetto che notizie e dati macroeconomici hanno sui mercati. Tale tecnica è comunemente utilizzata anche da operatori fisici; tuttavia, la caratteristica dell'estrema velocità permette ai sistemi di HFT di prendere posizione prima degli altri operatori del mercato. Ovviamente occorre che il sistema di IA abbia accesso ad un continuo flusso informativo, esterno rispetto al mercato, da cui trarre strategie operative. In particolare, il trader ad alta frequenza associa determinate strategie operative a *pattern* di parole presenti nelle notizie.[24]

Spesso, inoltre, gli HFT si avvalgono di servizi di *Flash Trading.* Alcuni ENC, infatti, permettono agli operatori ad alta frequenza, che abbiano sottoscritto tale servizio, di visionare, prima degli altri operatori, gli ordini immessi sul mercato che si discostino dal NBBO. Si tratta di una sorta di "prelazione" che accentua l'asimmetria informativa che si viene a creare tra gli HFT e i *traders* fisici.

Un'ulteriore strategia viene denominata *Liquidity Detenction*: il sistema di HFT, con una serie di piccoli ordini, va a determinare le posizioni di altri operatori del mercato. In particolare, lo scopo è quello di individuare e poi far scattare gli *stop loss* e *take profit*.[25]

---

[23] Per la descrizione delle strategie di *trading* ad alta frequenza si veda A. PUORRO, *High Frequency Trading: una panoramica, cit*.

[24] *Ibidem.*

[25] Alcuni ordini immessi sul mercato possono essere condizionati da clausole di *stop loss* e *take profit.*
Lo *stop loss* è finalizzato a contenere le perdite: al raggiungimento di un determinato livello di prezzo, è prevista la chiusura automatica dell'ordine.
Il *take profit* ha lo scopo di chiudere automaticamente una posizione in profitto al raggiungimento di livello tecnico particolare, generalmente costituito da un determinato guadagno ottenibile. Permette quindi di eliminare il rischio ulteriore.

2.2.1 Le strategie più aggressive: *Pinging*, *Layering*, *Spoofing* e *Quote Stuffing*

Alcune strategie utilizzate dagli HFT si trovano al centro delle critiche rivolte a tali sistemi di *trading*, in quanto estremamente aggressive. Tali meccanismi, infatti, potrebbero portare ad effetti distorsivi del mercato e ipoteticamente integrare condotte manipolative.

Il *Quote Stuffing,* ad esempio*,* consiste nell'immissione e nella contestuale cancellazione di un'enorme quantità di ordini, tale da comportare un inevitabile rallentamento del funzionamento del mercato, il quale necessita di più tempo del normale per processare tale mole di informazioni. Anche gli altri operatori del mercato, che non siano ad alta frequenza, si trovano in difficoltà nel gestire l'immenso afflusso di ordini. Tutto ciò non fa altro che aumentare la possibilità di sfruttare arbitraggi di latenza.[26]

Un'altra tecnica di negoziazione particolarmente discussa viene denominata *Momentum Ignition*: viene creato un *momentum*, ossia un *trend* di mercato che viene sfruttato dall'HFT per trarre profitti grazie al vantaggio competitivo derivante dalla velocità del sistema. A differenza del *trading on news*, in questo caso il *momentum* viene artificiosamente prodotto dal sistema di IA che prende una posizione aggressiva in relazione ad un prezzo già instabile, creando quindi il *trend*.[27]

Vi è poi un insieme di quattro strategie (*Pinging*, *Spoofing*, *Smoking* e *Layering*) che sono accomunate dalla caratteristica di essere basate sui *limit orders*. Si tratta di ordini di acquistare o vendere ad un determinato prezzo "limite" o ad un prezzo più vantaggioso.[28] Attraverso l'immissione e la cancellazione ripetuta di tali *limit orders*, l'HFT riesce a creare artificiosamente condizioni di mercato a lui favorevoli e a sfruttare la propria superiorità tecnologica per trarre profitti, a discapito degli altri partecipanti del mercato che vengono tratti in inganno da situazioni non rispondenti alla realtà.

Per comprendere il funzionamento di tali strategie si può considerare il seguente esempio, riferito alla tecnica dello *Spoofing*. Il trader algoritmico immette in un mercato una

---

L'utilizzo di ordini condizionati consente di eliminare la componente comportamentale di ordini di investimento, ma d'altra parte rende le posizioni prevedibili e vulnerabili rispetto alle strategie ad alta frequenza descritte.

[26] J. FISHER, A. CLIFFORD, F. DINSHAW AND N. WERLE, *Criminal forms of high frequency trading on the financial markets*, in *Law and Financial Markets Review*, Vol. 9, No. 2, London School of Economics, London, 2015.

[27] A. PUORRO, *High Frequency Trading: una panoramica, cit.*

[28] sul punto il sito www.investopedia.com al seguente link: http://www.investopedia.com/terms/l/limitorder.asp

grande quantità di ordini di vendita di azioni ABC ad un prezzo leggermente differente dal prezzo corrente. Gli altri venditori seguono il *trend* e il prezzo si abbassa, a questo punto lo "*spoofer*" velocemente cancella gli ordini di vendita prima che possano essere eseguiti e acquista, invece, una grande quantità delle stesse azioni, ad un prezzo più basso rispetto a quello iniziale. L'HFT compie, in seguito, la stessa operazione nel senso opposto: immette una grande quantità di ordini di acquisto per far salire il prezzo, li cancella prima della loro esecuzione e vende a prezzo più alto. Il guadagno per ogni operazione, singolarmente considerata, è minimo, ma considerando l'enorme mole di operazioni eseguite costantemente dal sistema, risulta comunque ingente.[29]

Un'altra strategia interessante è il *pinging*. A questo proposito occorre tenere presente che spesso i grandi investitori possono tentare di ridurre l'impatto sul mercato dell'immissione di ordini di dimensioni considerevoli, utilizzando tecniche dette di "*ordini iceberg*", che frazionano l'ordine in una serie di ordini più piccoli. L'algoritmo di HFT, attraverso il *pinging,* riesce sostanzialmente a "rintracciare l'iceberg" e determinare se l'investitore ha ordini di riserva a prezzi meno aggressivi che non vengono visualizzati. Il trader ad alta frequenza inonda il mercato di "*ping*", ossia ordini "immediati o annullati", che si avvicinano al prezzo visualizzato dell'*iceberg* nel tentativo di trovare il prezzo limite degli ordini di riserva nascosti.

L'asimmetria informativa che si viene a creare permette poi all'HFT di utilizzare ulteriori strategie predatorie come il "traino dell'*iceberg*" che si ottiene forzando, per ogni azione, l'esecuzione più vicina al prezzo limite dell'ordine. Questa strategia aumenta l'impatto sul prezzo del grande ordine, consentendo all'impresa HFT di trarre profitto agendo come controparte dell'investitore istituzionale ad un prezzo leggermente diverso. [30]

2.3 Gli effetti distorsivi e i rischi del trading ad alta frequenza

Per quanto riguarda gli effetti dell'utilizzo dei sistemi di HFT sui mercati, si registrano opinioni contrapposte.

Una parte degli studiosi ha evidenziato alcuni effetti positivi nelle contrattazioni ad alta frequenza, tra cui ad esempio un aumento della liquidità a disposizione dei partecipanti

[29] J. FISHER, A. CLIFFORD, F. DINSHAW AND N. WERLE, *Criminal forms of high frequency trading on the financial markets*, *cit.*
[30] *Ibidem*.

al mercato oppure un incremento dell'efficienza informativa dei prezzi derivante da aumento dei collegamenti *intermarket*. [31]

In dottrina risulta, invece, diffusa la convinzione della pericolosità derivante dai numerosi effetti distorsivi causati dai sistemi di HFT.[32] A questo proposito possono essere analizzati alcuni dei principali rischi derivanti dalla presenza massiva di *traders* ad alta frequenza sui mercati.

Un primo importante svantaggio è costituito dall'aumento del "rischio sistemico", ossia il rischio di collasso di un intero sistema finanziario o di un intero mercato. A tal proposito è stato rilevato da un rapporto del luglio 2011 del Comitato tecnico dell'International Organization of Securities Commissions (IOSCO) che la forte interconnessione tra i mercati, derivante dalla diffusione dei sistemi di HFT, implica una rapida trasmissione di eventuali "*shock*" da un mercato all'altro, amplificando di conseguenza il rischio sistemico.[33] Tale fattore risulta alla base del fenomeno del *Flash Crash*: un improvviso crollo, apparentemente immotivato, dei prezzi di uno o più strumenti finanziari, seguito da un repentino rimbalzo nei minuti immediatamente successivi.[34]

L'aumento del rischio sistemico deriva dalla compresenza di numerosi fattori. Innanzitutto, l'HFT intensifica la volatilità: gli algoritmi sono in grado di reagire istantaneamente alle condizioni di mercato, quindi, durante le fasi tumultuose dei mercati, possono ampliare i loro *bid-ask spread* o interrompere temporaneamente le negoziazioni, riducendo così la liquidità ed esacerbando la volatilità.[35] Un altro aspetto che concorre ad aumentare il rischio sistemico consiste nell'accentuazione di un'asimmetria informativa tra l'operatore algoritmico ad alta frequenza e l'operatore fisico: in particolare attraverso il servizio di *flash trading*, ma in generale anche grazie alla sua estrema velocità, l'HFT ottiene un vantaggio informativo concretizzabile in un guadagno a bassissimo rischio.[36] Infine, è possibile evidenziare che l'aumento di liquidità[37] derivante dall'alta presenza su un mercato

---

[31] J. ANGELS, L. HARRIS, C. SPATT, *Equity Trading in the 21st Century*, in *Marshall School of Business Working Paper* No. FBE 09-10, Los Angeles, 2010.
[32] Si veda investopedia.com, E. PICARDO, *4 Big Risks of Algorithmic High-Frequency Trading*, 2022.
[33] *Ibidem*.
[34] Il fenomeno del Flash Crash verrà approfondito nei paragrafi seguenti.
[35] Si veda investopedia.com, E. PICARDO, *4 Big Risks of Algorithmic High-Frequency Trading*, 2022.
[36] A. PUORRO, *High Frequency Trading: una panoramica, cit.*
[37] Per *liquidità* in questo contesto si fa riferimento all'insieme delle proposte di acquisto o vendita presenti sui *book* di negoziazione, delle proposte di acquisto o vendita che arrivano sul mercato e dei volumi associati alle proposte di acquisto o di vendita. Tale valore è positivo per la stabilità del mercato.

di sistemi di negoziazione ad alta frequenza, in realtà è del tutto apparente. L'alto numero di ordini costantemente immessi sul mercato comporta un inevitabile aumento di liquidità, ma da questo non derivano effetti di stabilizzazione del mercato; infatti, tale liquidità viene definita "liquidità ombra" poiché molte strategie del *trading* ad alta frequenza prevedono una quasi immediata cancellazione degli ordini prima della loro esecuzione.[38]

Un secondo rischio derivante dall'alta presenza di HFTs sul mercato deriva dai possibili difetti dell'algoritmo. Un celebre esempio a questo proposito è quello del caso *Knight Capital*, un *market maker* che ha perso 440 milioni di dollari in un periodo di 45 minuti nell'agosto del 2012, a causa di un errore nell'algoritmo che ha portato la società vicino alla bancarotta. [39] Le ingenti perdite sono derivate innanzitutto dall'incredibile velocità con cui vengono effettuate le operazioni ad alta frequenza, che rende quasi impossibile identificare l'errore dell'algoritmo prima che si realizzino danni importanti; inoltre, altri HFTs presenti sul mercato hanno captato con i loro algoritmi il *trend* derivante dall'errore informatico e l'hanno sfruttato a loro vantaggio.

Un ulteriore svantaggio derivante dai sistemi di HFT consiste in fenomeni di selezione avversa. Si pensi, ad esempio al *pinging*: gli HFTs individuano le strategie di *trading* degli altri partecipanti al mercato, inducendoli poi ad effettuare operazioni che, in mancanza delle simulazioni, non avrebbero intrapreso. Questo accentua un fenomeno di selezione avversa a danno di operatori meno evoluti. Tutto ciò, insieme agli episodi di insolita volatilità, porta inevitabilmente ad una diffusa perdita di fiducia nel mercato.[40]

2.3.1 Flash Crash: 10 maggio 2010, il caso Dow Jones

Il Flash crash è un fenomeno che consiste in un'improvvisa e spesso immotivata discesa dei prezzi di uno o più strumenti finanziari seguita da un rimbalzo nei minuti immediatamente successivi. Nonostante queste brusche oscillazioni di prezzo esistessero anche prima della presenza degli HFT sui mercati, senza dubbio gli agenti artificiali che operano ad alta frequenza hanno incrementato enormemente la portata del fenomeno: capita quindi che una variazione in qualche modo notevole dell'andamento delle contrattazioni (che può essere dovuta all'immissione di un ordine di grandi dimensioni, oppure ad un semplice

[38] A. PUORRO, *High Frequency Trading: una panoramica, cit.*
[39] Si veda investopedia.com, E. PICARDO, *4 Big Risks of Algorithmic High-Frequency Trading*, 2022.
[40] *Ibidem*.

errore umano) venga sfruttata dagli algoritmi attraverso strategie di *momentum trading*. In questo modo le conseguenze distorsive nel mercato aumentano e questo attira altri operatori ad alta frequenza che non fanno altro che incrementare questo effetto "palla di neve".[41]

Il primo episodio di grande risonanza in cui il fenomeno del *flash crash* è stato abbinato al *trading* ad alta frequenza ha avuto luogo il 6 maggio del 2010 e ha coinvolto i maggiori indici azionari statunitensi. Il crollo è stato tale che per qualche minuto la discesa ha tenuto un ritmo di 1% al minuto, arrivando a provocare una perdita di quasi il 10%, in parte poi cancellata grazie a una provvidenziale breve interruzione delle contrattazioni.[42] Le indagini effettuate dalle autorità statunitensi hanno evidenziato che il *flash crash* è stato innescato da una grossa vendita di *futures* E-mini SP500 da parte di un fondo d'investimento; tale operazione ha prodotto poi un enorme effetto a catena provocando ingenti perdite per molti investitori in diversi mercati. È stato rilevato che, oltre a rendere immensamente più veloce e incontrollato il crollo, l'alta presenza di HFT sul mercato ha contribuito alla diffusione del *trend* su diverse piattaforme di contrattazione, ampliandone quindi gli effetti.[43]

Per quanto riguarda la causa scatenante del *crash* inizialmente si pensò ad un errore; solo cinque anni dopo, il Dipartimento di Giustizia statunitense ha avviato un procedimento penale nei confronti di Navinder Singh Sarao, *trader* londinese, per aver messo in atto pratiche abusive, realizzate con algoritmi di HFT, che hanno contribuito a destabilizzare i mercati e cagionare il crollo. Sarao avrebbe infatti utilizzato un programma algoritmico manipolativo, progettato per realizzare la pratica dello *spoofing* in relazione a *futures* E-mini SP500, che ha poi scatenato il dannoso effetto a catena. Non risulta chiaro se il trader avesse l'intenzione di scatenare il *flash crash,* fenomeno alquanto imprevedibile e comunque dalle conseguenze ancora poco note all'epoca, ma senza dubbio ne ha tratto vantaggio dato che gli inquirenti ritengono che Sarao abbia ottenuto all'incirca un guadagno di 40 milioni di dollari.[44]

---

[41] A. PUORRO, *High Frequency Trading: una panoramica, cit*.

[42] J. FISHER, A. CLIFFORD, F. DINSHAW AND N. WERLE, *Criminal forms of high frequency trading on the financial markets*, *cit*.

[43] F.LILLO, S. MARMI, *Il calcolo della velocità,* in *Il Sole 24 Ore,* disponibile al seguente link https://st.ilsole24ore.com/art/tecnologie/2011-05-19/calcolo-velocita-152033.shtml?uuid=AaDTcbYD&refresh_ce=1

[44] J. FISHER, A. CLIFFORD, F. DINSHAW AND N. WERLE, *Criminal forms of high frequency trading on the financial markets*, *cit*.

2.3.2 I fenomeni successivi e il recente flash crash di Stoccolma (maggio 2022)

Il *flash crash* del 2010 non è stato un caso isolato. Solo tre anni dopo, infatti, si è verificato un nuovo crollo: gli indici azionari statunitensi hanno registrato in pochi secondi una perdita maggiore dell'1%, per poi tornare sui livelli iniziali nei successivi cinque minuti. Questo improvviso movimento è stato causato, questa volta, da un elemento esterno al mondo finanziario: un *hacker* è riuscito ad accedere all'account *twitter* dell'*Associated Press* e a divulgare la notizia di un attacco alla Casa Bianca e del ferimento del presidente Obama. Il panico dei mercati è stato subito individuato dai sistemi di HFT che hanno iniziato a sfruttare il *trend* ribassista. La notizia è poi stata fortunatamente smentita nei minuti successivi.[45]

Si sono susseguiti diversi fenomeni di questo tipo nell'ultimo decennio: le cause scatenanti sono state varie e le conseguenze sono state più o meno gravi a seconda del tempo che la piattaforma di negoziazione ha impiegato per sospendere le contrattazioni.

L'episodio più recente ha avuto luogo il 2 maggio 2022 ed è partito dalla Borsa di Stoccolma, coinvolgendo Copenaghen, Helsinki e Oslo per poi propagarsi a tutti i principali listini europei.

Si può affermare che il *crash* sia avvenuto in un momento di particolare difficoltà dei mercati: le Banche Centrali avevano appena iniziato a sospendere le politiche monetarie che avevano sostenuto le Borse negli anni precedenti e questo, sommato al rallentamento economico globale, al conflitto in Ucraina e all'inflazione crescente, non ha fatto altro che rendere i mercati particolarmente reattivi a tali fenomeni. Il crollo è durato solo qualche minuto e le chiusure, pur negative, non sono state particolarmente allarmanti: Milano -1,63%, Parigi -1,99% e Francoforte -1,45%.[46] L'epicentro è stato subito individuato nella Borsa di Stoccolma e nel giro di poche ore la causa del crollo è risultata essere un semplice errore umano. Infatti, dopo che Nasdaq Stockholm ha escluso problemi tecnici o attacchi informatici al sistema, la banca Citigroup si è assunta la responsabilità del crollo: «Questa mattina uno dei nostri trader ha compiuto un errore nell'inserire una transazione**.** Nell'arco di qualche minuto, abbiamo identificato l'errore e lo abbiamo corretto».[47]

---

[45] A. PUORRO, *High Frequency Trading: una panoramica, cit.*

[46] Disponibile al seguente link https://www.finanzaonline.com/notizie/flash-crash-europa-scatenato-da-errore-trading-desk-citigroup-panico-alla-borsa-di-stoccolma-ecco-cosa-e-successo

[47] M. LONGO, *Un flash crash travolge i listini, ma pesano più Fed e Cina*, Il Sole 24 Ore, 3 maggio 2022.

Questo esposto consente quindi di affermare che, sebbene le cause dei *flash crashes* siano varie e di diversa natura (dalla condotta manipolativa realizzata attraverso algoritmi di HFT, a notizie di cronaca o semplici errori di digitazione), la presenza crescente di sistemi di contrattazione ad alta frequenza sui mercati porta ad accentuare la velocità con cui il crollo si propaga e ad amplificarne le conseguenze.

2.4 Il quadro giuridico europeo per il trading ad alta frequenza

La regolamentazione del *trading* ad alta frequenza, per quanto riguarda l'Unione Europea, è contenuta nella direttiva 2014/65/UE (MIFID II). Tale direttiva si concentra principalmente su due aspetti dell'HFT: le disposizioni che concernono l'accesso al mercato e quelle che regolano l'attività di monitoraggio degli algoritmi.[48]

Le tematiche che riguardano l'accesso al mercato sono legate alle autorizzazioni necessarie per operare nelle sedi di negoziazione, alla *co-location* e alla dimensione minima dei *tick.*

Ai sensi dell'art 2 della presente direttiva le società che compiono HFT devono essere autorizzate dalle autorità di regolamentazione; a questi fini *"l"autorità competente dello Stato membro d'origine dell'impresa di investimento può prescrivere che quest'ultima fornisca, su base regolare o ad hoc, una descrizione della natura delle proprie strategie di negoziazione algoritmica, dettagli sui parametri o sui limiti di negoziazione a cui il sistema è soggetto".* Non è necessario che il codice dell'algoritmo venga depositato: la sua attività sarà tracciata mediante l'utilizzo di un sistema detto Legal Entity Identifier ("LEI").[49]

I servizi di co-locazione possono risultare problematici dal punto di vista della concorrenza data la loro inclinazione ad attribuire un vantaggio notevole in termini di velocità di esecuzione dell'ordine. Per tale motivo, Mifid II ha previsto, all'art 48, che le piattaforme di negoziazione possano offrire questo servizio, anche a tariffe differenti, a condizione di garantire trasparenza, equità e condizioni non discriminatorie.

---

[48] Gli aspetti legati alla manipolazione del mercato e alla sua ridefinizione alla luce del *trading* algoritmico sono invece contenuti nel Regolamento (UE) n. 596/2014 del Parlamento Europeo e del Consiglio (MAR) di cui si tratterà in seguito

[49] Si tratta di un codice alfanumerico di venti caratteri basato sullo Standard ISO 17442 sviluppato dall'Organizzazione Internazionale per la Normazione (ISO). È collegato a informazioni di riferimento chiave che permettono di avere un'identificazione chiara e univoca delle persone giuridiche che partecipano alle transazioni finanziarie.

Alcuni piccoli *traders* invece di utilizzare la *co-location*, si collegano al mercato attraverso un fornitore di Accesso Elettronico Diretto (DEA): tale funzionalità consente ai clienti di immettere le proprie proposte di negoziazione direttamente nella piattaforma di mercato. Secondo la disciplina prevista da Mifid II, i fornitori di DEA devono effettuare controlli adeguati in relazione agli algoritmi e saranno responsabili delle attività dei loro clienti.[50]

Un altro aspetto che influenza la velocità di negoziazione è la dimensione minima dei *tick*, ossia il più piccolo incremento di prezzo consentito per un prodotto finanziario. *Tick* troppo piccoli potrebbero incoraggiare gli HFT a creare volatilità non necessaria. Nella direttiva viene effettuato un tentativo di armonizzazione delle dimensioni dei *tick*: le sedi di negoziazione dovranno applicare i regimi di dimensione minima previsti dall'ESMA.[51] È inoltre previsto un obbligo per le *trading venues* di imporre un rapporto massimo tra ordini inviati e operazioni effettivamente eseguite.

Per quanto riguarda invece le disposizioni concernenti il monitoraggio degli algoritmi, la direttiva prevede varie procedure di controllo sia precedenti all'utilizzo sia in tempo reale.

L'art 17 descrive a questo proposito i vari adempimenti a carico delle imprese di investimento che effettuano negoziazione algoritmica. Da una parte, infatti occorre realizzare *controlli dei sistemi e del rischio efficaci e idonei per l'attività esercitata volti a garantire che i propri sistemi di negoziazione siano resilienti e dispongano di sufficiente capacità, siano soggetti a soglie e limiti di negoziazione appropriati e impediscano l'invio di ordini erronei o comunque un funzionamento dei sistemi tale da creare un mercato disordinato o contribuirvi.* D'altra parte, tali imprese devono garantire dei controlli idonei a evitare che i sistemi di negoziazione possano essere utilizzati per finalità contrarie al regolamento (UE) n. 596/2014 (MAR) o alle regole di una sede di negoziazione a cui esse sono collegate, e quindi sostanzialmente evitare che i sistemi effettuino attività di manipolazione del mercato.

Su queste basi, secondo alcuni autori la responsabilità per eventuali eventi di disturbo potrebbe essere attribuita a tutte le persone rilevanti a tutti livelli gerarchici, dallo

[50] Divisione Mercati, Ufficio Vigilanza Infrastrutture di Mercato, *Mappatura delle sedi di negoziazione in Italia dopo l'entrata in vigore di MiFID II/MiFIR*, CONSOB, ottobre 2018.
[51] Art 48 Direttiva 2014/65/UE del Parlamento europeo e del Consiglio (MIFID II).

sviluppatore, al *trader*, al supervisore delle negoziazioni, nonché alla direzione dell'impresa.[52]

Dal punto di vista delle sedi di negoziazione invece l'art 48 di Mifid II prevede che "*i mercati regolamentati dispongano di sistemi, procedure e dispositivi efficaci, anche chiedendo ai membri o ai partecipanti di realizzare prove adeguate degli algoritmi e fornendo ambienti per facilitare la realizzazione di tali prove, per garantire che i sistemi algoritmici di negoziazione non possano creare o contribuire a creare condizioni di negoziazione anormali sul mercato e per gestire qualsiasi condizione di negoziazione anormale causata da tali sistemi algoritmici di negoziazione, tra cui sistemi per limitare il rapporto tra ordini non eseguiti e operazioni inserite nel sistema da un membro o partecipante* (per evitare lo *spoofing*)*, per poter rallentare il flusso di ordini in caso di rischio che sia raggiunta la capacità del sistema* (per evitare il *quote stuffing*) *e per limitare la dimensione minima dello scostamento di prezzo che può essere eseguita sul mercato e garantirne il rispetto.*

Per consentire la ricostruzione *ex post* dell'attività di *trading,* è inoltre previsto che le imprese e le sedi in tutta Europa debbano sincronizzare i loro orologi e registrare l'attività e conservare i dati per cinque anni.[53]

[52] T. ČUK, A. VAN WAEYENBERGE, *European Legal Framework for Algorithmic and High Frequency Trading (Mifid 2 and MAR), A Global Approach to Managing the Risks of the Modern Trading Paradigm*, Cambridge University Press, Cambridge, 2018.

[53] Divisione Mercati, Ufficio Vigilanza Infrastrutture di Mercato, *Mappatura delle sedi di negoziazione in Italia dopo l'entrata in vigore di MiFID II/MiFIR*, CONSOB, ottobre 2018.

CAPITOLO III
LA RESPONSABILITA' PENALE PER GLI ABUSI DI MERCATO REALIZZATI CON SISTEMI DI HFT.

SOMMARIO: 3.1 I diversi livelli di autonomia dei sistemi di *trading* ad alta frequenza – 3.2 Le differenti dinamiche di responsabilità – 3.2.1 *Operational failure* – 3.2.2 *Market abuse by design* – 3.2.3 I comportamenti di agenti artificiali autonomi – 3.3 L'opacità del modello *Black Box* e la crisi dei concetti penalistici – 3.3.1 Le soluzioni adottate in altri ordinamenti – 3.4 Una breve parentesi: la manipolazione del mercato realizzata attraverso i *social bots* – 3.4.1 L'utilizzo dell'intelligenza artificiale sulle piattaforme social per manipolare il mercato: il caso di Twitter

3.1 I diversi livelli di autonomia dei sistemi di trading ad alta frequenza

Nel capitolo precedente è stato evidenziato come alcune strategie del *trading* ad alta frequenza possano dare luogo a condotte manipolative, ad esempio attraverso lo *spoofing*. Occorre ricordare che gli HFT non sono altro che sistemi di intelligenza artificiale e quindi sono soggetti alle problematiche relative alla mancanza di trasparenza e al *responsibility gap*, dovuti alla *black box.* Appare quindi opportuno analizzare come questi aspetti (precedentemente definiti a livello generale nel capitolo I), si estrinsechino nell'ambito del *trading* ad alta frequenza.

Una prima necessaria considerazione è che non tutti i sistemi di contrattazione algoritmica godono dello stesso livello di autonomia.[1]

I primi *traders* algoritmici erano basati su sistemi *ruled-based*: la macchina veniva "istruita" attraverso *clusters* di regole e dati e il suo funzionamento era del tutto prevedibile.[2]

In seguito, sono nati i primi sistemi basati sul *supervised learning* in grado di analizzare una grande mole di dati pre-lavorati e fornire come *output* previsioni molto precise in relazione alle operazioni da effettuare. Si tratta di strumenti tuttora utilizzati che non presentano particolari problemi poiché permane un importante controllo umano

[1] A. AZZUTTI, W. G. RIING, H. S. STIHEL, *Machine learning, Market Manipulation and Collusion on capital markets why the "Black Box" matters*, in *University of Pennsylvania Journal of International Law*, 2021.
[2] I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale,* in *Riv. it. dir. proc. pen*, fasc.1, marzo 2021, p.83.

nell'attività della macchina: sia in relazione ai dati forniti che alla realizzazione effettiva dell'operazione che risulta condizionata da una scelta dell'operatore.[3]

Gli aspetti più problematici, invece, riguardano i sistemi di HFT più recenti basati sull'apprendimento non supervisionato e sul *reinforcement learning*. Tali sistemi analizzando dati "grezzi" forniti, riescono a dedurre dei modelli comportamentali all'interno del mercato e ad identificare opportunità di *trading.* Attraverso l'apprendimento rinforzato, la macchina riesce ad imparare, con processi di *trial and error*, anche in ambienti incerti e dinamici quale può essere un mercato.[4]

L'ultimo scalino nell'evoluzione di questi sistemi è relativo ai casi in cui viene utilizzata la tecnologia del *deep learning* (DL)[5] su algoritmi di *reinforcement learning* (RL): in questi casi con il DL si individuano correlazioni latenti, mentre con il RL il sistema decide quali operazioni effettuare in vista di un obbiettivo.[6]

Appare evidente quindi che, nelle ultime evoluzioni dei sistemi di HFT, lo spazio di manovra dell'agente umano è alquanto ristretto se non inesistente: la macchina analizza da sola il mercato, impara strategie di *trading*, monitora l'andamento dei titoli in tempo reale ed effettua autonomamente le operazioni che, secondo le previsioni realizzate, sono migliori al fine di massimizzare il profitto.[7]

In questo contesto è difficile che l'operatore umano possa realizzare un effettivo controllo sull'operato della macchina,[8] anche a causa delle problematiche relative alla *black box* precedentemente esposte.[9]

Allo stesso modo, il programmatore non ha la possibilità di prevedere il comportamento della macchina, una volta che sarà inserita in un sistema complesso quale un mercato. Mentre in laboratorio il programmatore ha sotto controllo tutti gli aspetti tranne il comportamento del sistema testato (che però può ragionevolmente prevedere), in un sistema aperto, come il mercato, non è chiaro come la macchina analizzerà i dati forniti,

---

[3] A. AZZUTTI, W. G. RIING, H. S. STIHEL, *Machine learning, Market Manipulation and Collusion on capital markets why the "Black Box" matters, cit.*
[4] *Ibidem.*
[5] Si veda § 1.1.1.
[6] K. ARULKUMARAN, M. P. DEISENROTH, M. BRUNDAGE, A. A. BHARATH, *A Brief Survey of Deep Reinforcement Learning*, in *IEEE Signal Processing Magazine*, 2017.
[7] Y. BATHAEE, *The Artificila Intelligence Black Box and the failure of intent and causation,* in *Harvard Journal of Law & Technology* Vol. 31, No. 2, 2018.
[8] B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automazione artificiale,* in *Diritto dell'Informazione e dell'informatica* (II), fasc.2, 2021, p. 317.
[9] Si veda § 1.2.1

quali strategie apprenderà e quali scelte riterrà più vantaggiose. Questo problema, detto *"curse of dimensionality"* si realizza quando un agente RL è chiamato ad apprendere da un ambiente troppo grande e in continua evoluzione.[10]

Un altro aspetto rilevante è relativo alle difficoltà che, in questo campo, incontra la letteratura di finanza computazionale. Se infatti in generale la ricerca sul ML è in una fase di grande sviluppo, per i sistemi di HFT si sta procedendo più lentamente: ad esempio, a differenza di altri campi di applicazione dell'AI, non esiste ancora un chiaro *benchmark* per valutare e confrontare gli algoritmi per il *trading* finanziario. In questo campo, infatti, l'evoluzione tecnologica è portata avanti tendenzialmente da imprese di investimento che, da una parte godono di diritti di proprietà intellettuale su tali prodotti e dall'altra, non hanno nessun interesse a rendere pubblici i dettagli riguardanti la natura degli algoritmi, il ruolo dei dati empirici utilizzati, così come le informazioni sul processo di apprendimento.[11]

3.2 Le differenti dinamiche di responsabilità

Si può quindi affermare che i sistemi di HFT più evoluti possono realizzare condotte abusive. Molti ordinamenti, infatti, puniscono la manipolazione del mercato, sia sul piano informativo (diffusione di informazioni false o fuorvianti), sia sul piano operativo, attraverso operazioni o altri artifizi.[12] A seconda della normativa di riferimento vi potranno essere delle differenze nella descrizione della fattispecie di reato suscettibili di portare a conclusioni parzialmente diverse.[13]

Una problematica comune consiste nel fatto che, essendo la condotta materialmente realizzata dalla macchina, alcuni concetti penalistici in senso lato trasversali, come quello di *negligence*, *intent* o *causation*, potrebbero entrare in crisi, per effetto dei problemi legati alla *black box*.[14]

---

[10] A. AZZUTTI, W. G. RIING, H. S. STIHEL, *Machine learning, Market Manipulation and Collusion on capital markets why the "Black Box" matters, cit.*
[11] *Ibidem.*
[12] J. FISHER, A. CLIFFORD, F. DINSHAW AND N. WERLE, *Criminal forms of high frequency trading on the financial markets*, in *Law and Financial Markets Review*, Vol. 9, No. 2, London School of Economics, London, 2015.
[13] Per la descrizione dettagliata del reato previsto dalla normativa italiana si veda il Capitolo IV. Alcune normative straniere saranno analizzate in un'ottica comparata al 3.3.1.
[14] Y. YADAV, *The Failure of Liability in Modern Markets*, in Virginia Law Review, vol. 102, 2016.

Non si può tuttavia giungere frettolosamente alla conclusione per cui in nessun caso in cui un sistema di HFT realizzi condotte abusive sia possibile prevedere la responsabilità penale di una persona fisica. Nei seguenti paragrafi, si delineerano diverse dinamiche di responsabilità, partendo dall'analisi di alcuni casi.

3.2.1 *Operational failure*

Il primo scenario di responsabilità riguarda il caso in cui un evento dannoso venga causato da un sistema di HFT in conseguenza ad un errore di sistema.

Il caso più famoso di questo tipo è sicuramente quello che ha coinvolto la celeberrima società *Knight Capital* nel 2012; l'impresa di investimento ha compiuto due errori tecnologici critici che hanno portato a un malfunzionamento dei sistemi di *trading*, causando una pressione massiccia sul mercato e un conseguente disordine in relazione ai prezzi di alcuni titoli.[15] Prima che i tecnici riuscissero a rimediare all'errore, *Knight Capital* aveva già accumulato 460 milioni di dollari di perdite, che portarono la società alla bancarotta e alla successiva acquisizione da parte di una concorrente.[16]

Questo caso non comporta particolari problemi dal punto di vista della responsabilità. Infatti, la US Securities and Exchange Commission (SEC) ha sostenuto accuse basate sulla violazione della "*market access rule*", concluse poi con un "patteggiamento" il pagamento, da parte della società di una sanzione di 12 milioni di dollari.[17] La *rule* richiede ai *broker-dealer* con accesso al mercato o che forniscono accesso al mercato di "*controllare in modo appropriato i rischi associati all'accesso al mercato in modo da non mettere a repentaglio la propria condizione finanziaria, quella degli altri partecipanti al mercato, l'integrità delle negoziazioni sui mercati dei titoli e la stabilità del sistema finanziario*".[18] Un'indagine della SEC ha rilevato che *Knight Capital* non disponeva di adeguate misure di salvaguardia per limitare i rischi posti dal suo accesso ai mercati e non è riuscita, di conseguenza, a impedire l'immissione di milioni di ordini errati; non ha inoltre condotto adeguate verifiche dell'efficacia dei suoi controlli. Il caso riguarda quindi una responsabilità di tipo colposo

[15] Si veda https://www.sec.gov/news/press-release/2013-222
[16] A. AZZUTTI, W. G. RIING, H. S. STIHEL, *Machine learning, Market Manipulation and Collusion on capital markets why the "Black Box" matters, cit.*
[17] Si veda https://www.sec.gov/news/press-release/2013-222
[18] Exchange Act Rule 15 c3-5

che, nel caso di specie, trova un riscontro nelle norme statunitensi. Addirittura, Daniel M. Hawke, capo dell'Unità Abusi di Mercato della *SEC Enforcement Division*, ha aggiunto che i *broker-dealer* dovrebbero esaminare ogni componente dei loro sistemi e chiedersi cosa succederebbe in caso di malfunzionamento del componente e quali reti di sicurezza siano state predisposte per limitare il danno tale malfunzionamento che potrebbe causare.[19]

3.2.2 *Market abuse by design*

Una differente dinamica di responsabilità si realizza nel caso in cui le perturbazioni del mercato derivino da algoritmi consapevolmente creati per scopi illeciti.[20] La capacità manipolativa in questi casi può derivare sia dalla fase di progettazione, sia dalla fase di "formazione" dell'algoritmo: i tecnici possono infatti fornire al sistema di IA esempi e dati, all'interno di ambienti simulati, che permettono alla macchina di "scoprire" tecniche manipolative finalizzate alla massimizzazione del profitto.[21]

Uno degli esempi più eclatanti in questo campo riguarda il caso di Athena Capital, società statunitense che nel 2014 è stata sanzionata dalla SEC per aver manipolato il mercato attraverso degli algoritmi di *high frequency tranding*.[22] Tra giugno e dicembre 2009, infatti, Athena ha utilizzato un suo algoritmo, denominato *Gravy*, per realizzare la pratica manipolativa nota come *"marking the close"*: qualche secondo prima della chiusura dei mercati è stata inserita una grande quantità di ordini di acquisto o di vendita, in modo che il sistema non riuscisse ad assorbirli e il prezzo di chiusura risultasse alterato.[23] Questa pratica ha permesso ad una società di dimensioni moderate di dominare il mercato negli ultimi secondi della giornata di negoziazione. Apparve inoltre evidente che Athena fosse perfettamente consapevole dell'impatto sui prezzi del proprio *trading*, tanto da definirlo nelle e-mail interne "*owning the game*". La società ha quindi accettato di pagare una sanzione da 1 milione di dollari per risolvere le accuse della SEC.

La vicenda appena descritta si è conclusa attraverso l'irrogazione di una sanzione amministrativa. Immaginandola però calata sul piano penale, emergerebbero rilevanti

[19] Si veda https://www.sec.gov/news/press-release/2013-222
[20] A. AZZUTTI, W. G. RIING, H. S. STIHEL, *Machine learning, Market Manipulation and Collusion on capital markets why the "Black Box" matters, cit.*
[21] Y. YADAV, *The Failure of Liability in Modern Markets*, cit.
[22] Si veda https://www.sec.gov/news/press-release/2014-229
[23] Si veda https://definitions.uslegal.com/m/marking-the-close/

problemi, in particolare per quanto riguarda la prova dell'"*intent*" della persona fisica rispetto al comportamento manipolativo della macchina. Tale prova è particolarmente difficile da ottenere da parte delle autorità pubbliche, anche in relazione alle limitate competenze e capacità tecnologiche possedute rispetto a quelle delle grandi società di investimento.[24]

La prima condanna penale per manipolazione del mercato realizzato attraverso sistemi di HFT è relativa al caso Coscia. Michael Coscia è infatti stato condannato delle autorità statunitensi per la condotta di *spoofing* realizzata dai suoi sistemi di HFT. In questo caso il problema della prova del dolo è stato superato grazie alla testimonianza dal programmatore, Jeremiah Park, che ha dichiarato che il signor Coscia avrebbe richiesto che «i programmi agissero come un'esca, che sarebbe stata utilizzata per alterare il mercato».[25]

In tali circostanze appare quindi evidente che il problema della responsabilità penale potrebbe porsi solo a livello di accertamento, mentre non si crea un effettivo "*responsibility gap*" dal momento che l'algoritmo viene utilizzato come mero strumento per realizzare una condotta illecita *ab origine* voluta dall'agente.

3.2.3 I comportamenti di agenti artificiali autonomi

Il terzo scenario è probabilmente il più problematico a livello di responsabilità penale: si tratta di casi in cui i sistemi di IA utilizzati dai *traders* ad alta frequenza scoprono autonomamente, in virtù dei meccanismi di *machine learning* più avanzati, strategie manipolative e le realizzano sul mercato.

A questo proposito appare opportuno citare uno tra i vari studi che hanno dimostrato empiricamente la possibilità di sistemi di *trading,* governati dall'IA, di scoprire autonomamente strategie di mercato manipolative.[26] Presso l'Università di Tokyo, infatti, è stata svolta una ricerca con l'obbiettivo di capire se un sistema di IA riuscisse effettivamente ad apprendere strategie manipolative in quanto percepite come migliori strategie di investimento, nonostante il programmatore non avesse alcuna intenzione di effettuare

[24] A. AZZUTTI, W. G. RIING, H. S. STIHEL, *Machine learning, Market Manipulation and Collusion on capital markets why the "Black Box" matters, cit.*
[25] Y. BATHAEE, *The Artificila Intelligence Black Box and the failure of intent and causation, cit*.
[26] T. MIZUTA, *Does an Artificial Intelligence Perform Market Manipulation With Its Own Discretion? – A Genetic Algorithm Learns in An Artificial Market Simulation*, SPARX Asset Management Co. Ltd., Tokyo, 2020.

manipolazioni. È stato quindi costruito un modello con un simulatore di mercato e vari agenti in cui è stato inserito l'IA *trader*.[27]

Si è concluso che il sistema di IA effettivamente può imparare strategie di investimento manipolative se opera in una simulazione di mercato che permette al *trader* di apprendere automaticamente l'impatto delle sue operazioni sui prezzi di mercato. Invece, se il metodo di apprendimento è basato sul *backtesting*[28]*,* il sistema di IA non ha questa possibilità perché non ha l'occasione di scoprire che le operazioni manipolative creano profitti dato che i prezzi di mercato sono fissati come dati storici reali. L'autore dello studio, Takanobu Mizuta, afferma, infatti: «*non dobbiamo preoccuparci che un trader IA esegua manipolazioni di mercato a propria discrezione senza l'intenzione dell'uomo, purché utilizzi il backtesting umano*.»[29] Tuttavia, i sistemi di ML più avanzati basano il loro apprendimento sui dati ricavati direttamente dal mercato e dall'impatto delle operazioni sui prezzi e sui comportamenti degli altri operatori.

Questo fenomeno si lega al problema già precedentemente esposto del *responsibility gap* come effetto della *black box*: ci si chiede a quale titolo potrebbe rispondere l'utilizzatore o il programmatore del sistema nel momento in cui l'agente di IA realizza condotte illecite che non erano prevedibili *ex ante*, e rispetto alle quali non è possibile nemmeno ricostruire un decorso causale nitido per effetto della mancanza di trasparenza legata ai sistemi di *machine learning*.[30]

Tale crisi dei concetti penalistici, intesi come *intent* e *causation*, si analizzerà nel seguente paragrafo in via generale ed in relazione ad un modello di imputazione tipicamente anglosassone. Un'analisi specifica di tali problematiche incentrata sul panorama normativo italiano, invece, verrà approfondita nel Capitolo IV.

3.3 L'opacità del modello *Black Box* e la crisi dei concetti penalistici

[27] *Ibidem.*
[28] Il *backtesting* è il metodo generale per verificare il rendimento di una strategia o di un modello a posteriori; viene valutata la fattibilità di una strategia di *trading* scoprendo come si sarebbe evoluta, utilizzando i dati storici. Si veda https://www.investopedia.com/terms/b/backtesting.asp
Un trader AI viene solitamente valutato tramite *backtesting*: viene stimato il profitto che si sarebbe raggiunto se il trader AI avesse operato in un determinato momento, utilizzando i dati storici dei prezzi di mercato.
[29] *Ibidem.*
[30] A. AZZUTTI, W. G. RIING, H. S. STIHEL, *Machine learning, Market Manipulation and Collusion on capital markets why the "Black Box" matters, cit.*

A livello processuale negli USA vengono utilizzati cosiddetti *test*, in relazione a elementi essenziali del reato, quali appunto il dolo o la causalità. Si tratta di percorsi logici, simili ad esempio ai "modelli causali" italiani, che si sono sviluppati nel corso dei secoli per aiutare i tribunali e le giurie a frammentare la condotta umana ed evincere se, in una determinata fattispecie concreta, possa configurarsi l'elemento soggettivo oppure possa essere provato il nesso causale.[31] Si analizzerà quindi come la complessità dei modelli *black box*, provochi il fallimento di questi *tests*, sollevando un enorme interrogativo in relazione alle prospettive future della responsabilità penale in ambienti sempre più governati da sistemi di IA.

Partendo dall'elemento soggettivo, si può affermare che nella maggior parte degli ordinamenti, il reato di manipolazione del mercato richiede l'*intent*[32] dell'agente di cagionare il danno o per lo meno di effettuare la condotta manipolativa.[33]

Negli Stati Uniti le Corti federali hanno in generale definito la manipolazione del mercato come "*intentional or willful conduct",* progettata per ingannare o frodare gli investitori controllando o modificando artificiosamente i prezzi degli strumenti finanziari.[34]

Quindi, nel caso in cui questa condotta venga materialmente realizzata da sistemi di IA attraverso l'HFT, l'intenzionalità sarà molto difficile da provare. Gli *intent tests* richiedono una certa capacità da parte degli utenti fisici di prevedere gli effetti della loro condotta sul mercato o sui prezzi. Tuttavia, appare già complesso dimostrare che le operazioni compiute dall''HFT abbiano avuto un impatto illegittimo sui prezzi, a maggior ragione, risulta difficile provare che l'impresa che utilizza l'algoritmo avesse intenzione di provocare tale impatto.[35] Inoltre, la velocità con cui i sistemi di IA eseguono le transazioni crea un alto grado di imprevedibilità, soprattutto in mercati in cui la presenza di *traders* ad alta frequenza è rilevante: la rapida interazione con la piattaforma di negoziazione e con altri

---

[31] *Ibidem.*

[32] L*'intent* è un concetto di diritto americano che in senso lato può essere assimilato al dolo italiano. Nell'ambito della concezione dualistica del reato, tipica degli ordinamenti di *common law*, questo sarebbe composto da due elementi: *mens rea* e *actus reus*. La *mens rea*, intesa come elemento soggettivo, ricomprende la categoria di *intent*. Esistono reati che richiedono un *general intent* ed altri che prevedono uno *specific intent*. Mentre lo *specific intent* appare del tutto assimilabile al dolo specifico italiano, quella del *general intent* risulta una categoria molto più sfumata, che certamente ricomprende il dolo generico, ma sembra estendersi anche a casi in cui sia sufficiente una *knowledge*, *recklessness*, o *negligence*. Si veda in https://www.law.cornell.edu/wex/intent

[33] A. AZZUTTI, W. G. RIING, H. S. STIHEL, *Machine learning, Market Manipulation and Collusion on capital markets why the "Black Box" matters, cit.*

[34] Y. BATHAEE, *The Artificila Intelligence Black Box and the failure of intent and causation, cit.*

[35] *Ibidem.*

HFT amplia l'effetto di contagio e può causare rapidi movimenti di prezzo.[36] Il test dell'*intent*, in questo caso, fallirebbe sia per il programmatore che per l'utilizzatore: nessuno dei due avrebbe potuto prevedere come si sarebbe comportato l'algoritmo e quali operazioni avrebbe concluso.

Inoltre, dal punto di vista del *designer* sarebbe molto facile difendersi da un'eventuale accusa, obbiettando l'assenza di *intent*. Si prenda ad esempio un algoritmo progettato per effettuare transazioni legittime per il 90% del tempo e per realizzare *spoofing* il 10%. Sarà molto difficile dimostrare che si tratti di un "*market abuse by design"* poiché il programmatore potrebbe sostenere che invece l'algoritmo è stato progettato per effettuare operazioni lecite e potrebbe portarne milioni di esempi.[37] Per effetto della *black box* appare impossibile ricostruire *ex post* i meccanismi decisionali della macchina e quindi capire se le operazioni manipolative sono state realizzate dal sistema autonomamente o per effetto di una programmazione illecita.[38]

Si è visto come in determinati casi questo problema possa essere superato da alcune risultanze probatorie che rendono il dolo quasi indubitabile. Nel caso Coscia, ad esempio, si è giunti alla condanna proprio grazie alla testimonianza del programmatore.[39] Tuttavia, se un HFT non è chiaramente progettato per uno scopo illegale, l*'intent test* fallisce ogni volta che non si riesce a dimostrare che il *designer* o l'utilizzatore aveva previsto gli effetti del comportamento dell'algoritmo.

Si potrebbe obbiettare che il programmatore avrebbe dovuto adottare accorgimenti opportuni per impedire che la macchina potesse eventualmente effettuare operazioni manipolative. Tuttavia, dato il problema della mancanza di trasparenza dei sistemi di IA, risulta impossibile verificare che il blocco sia stato effettivamente inserito o, ammettendo che sia stato reso operativo, accertare il motivo per cui non abbia funzionato. In ogni caso, il rimprovero potrebbe essere al massimo di natura colposa.[40]

In molti settori l'*intent* ha la funzione di limitare la punibilità ai soli casi in cui sussista effettivamente una volontà finalizzata a commettere una concotta illecita. Il fatto che, per effetto delle problematiche legate alla *black box,* i vari *tests* falliscano provoca un

[36] Y. YADAV, *The Failure of Liability in Modern Markets*, in Virginia Law Review, vol. 102, 2016.
[37] Y. BATHAEE, *The Artificila Intelligence Black Box and the failure of intent and causation,* cit.
[38] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato,* in *Riv. it. dir. proc. pen.*, vol.63, N°4, 2020.
[39] *Supra* 3.2.2
[40] Y. BATHAEE, *The Artificila Intelligence Black Box and the failure of intent and causation, cit.*

ampliamento della portata limitativa del dolo, che, secondo alcuni autori, forse va oltre la *ratio* della stessa:[41] in alcuni casi si crea un vuoto di tutela penalistica in relazione a condotte effettivamente dannose.[42]

Anche per quanto riguarda la causalità il sistema americano prevede dei *tests* che possono essere messi in crisi dai sistemi di *black box*.

Uno di questi è definito *test* della "*proximate cause"* e consiste nel chiedersi se il risultato della condotta realizzata dall'agente fosse o meno prevedibile da una persona ragionevole.[43] Si esclude quindi che una persona possa essere ritenuta penalmente responsabile quando la sua condotta ha causato un evento che non rientra nella sfera del rischio prevedibile; un concetto che riecheggia la tematica italiana del fattore eccezionale interruttivo del nesso causale.[44] In caso di condotte manipolative realizzate da sistemi di IA, questo *test* potrebbe fallire poiché, come già visto, le problematiche legate alla *black box* rendono impossibile prevedere il comportamento della macchina. Per effetto della loro velocità i sistemi di HFT possono infatti creare fenomeni come i *flash crashes,* la cui genesi causale è spesso un mistero.[45] Si potrebbe quindi sostenere che, poiché il comportamento della macchina risulta non prevedibile nemmeno da parte del programmatore, a maggior ragione lo sarà per una persona ragionevole.[46] Tuttavia, alcuni autori italiani sostengono che il comportamento della macchina non costituisce un fattore terzo eccezionale rispetto alla condotta dell'agente; chi programma il sistema di IA, infatti, sa di costruire un sistema il cui comportamento sarà in parte imprevedibile, ma i cui effetti si estrinsecheranno all'interno di un'area di rischio comunque conosciuta.[47]

Altri tipi di *tests* sulla causalità sono riconducibili al concetto di *conduct-nexus causation*, assimilabile al nesso causale tra la condotta e l'evento. A causa della mancanza di trasparenza dei sistemi di IA, è impossibile ricostruire *ex post* ogni passaggio che ha

---

[41] *Ibidem.*

[42] Problematiche analoghe si pongono in diversi ambiti di applicazione dei sistemi di IA: ad esempio nel campo della medicina di precisione che prevede l'utilizzo di macchinari governati da software autonomi. Si veda W. NICHOLSON, *Medical Malpractice and Black-Box Medicine*, in *Big Data, Health Law, and Bioethics* in Cambridge University Press, U of Michigan Public Law Research Paper No. 536, 2017

[43] Y. BATHAEE, *The Artificila Intelligence Black Box and the failure of intent and causation, cit.*

[44] C.F GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale*, p.255, Giuffrè, Milano 2020

[45] Si veda § 2.3.1

[46] Y. BATHAEE, *The Artificila Intelligence Black Box and the failure of intent and causation, cit.*

[47] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato,* in *Riv. it. dir. proc. pen*, vol.63, N°4, 2020

portato alla realizzazione dell'evento.[48] Dal punto di vista della condotta del programmatore del sistema di HFT, è molto difficile provare che i dati e le istruzioni fornite alla macchina, anche in sede di "formazione", siano stati effettivamente utilizzati poi come base per compiere quelle determinate operazioni manipolative.[49]

3.3.1 Le soluzioni adottate in altri ordinamenti

Per cercare di superare le problematiche enunciate nel precedente paragrafo, alcuni ordinamenti hanno adottato diverse soluzioni per perseguire penalmente le persone fisiche anche quando la condotta manipolativa sia compiuta da sistemi di HFT.

Ad esempio, negli USA nel 2010 è stato approvato il *Dodd-Frank Wall Street Reform and Consumer Protection Act* ("Dodd-Frank") che, tra le altre cose, ha vietato espressamente la pratica dello "*spoofing*".

La sezione 747 del *Dodd-Frank Act* ha modificato la sezione 4c(a)(5)(C)[50] del Commodities Exchange Act ("CEA"), atto normativo che trova applicazione solo nell'ambito dei mercati delle materie prime. La nuova normativa proibisce "*qualsiasi negoziazione, pratica o condotta (...) che abbia il carattere o sia comunemente nota agli operatori del settore come 'spoofing' (fare un'offerta o un'offerta con l'intento di cancellare l'offerta o l'offerta prima dell'esecuzione)*".[51] Si tratta di una fattispecie che può essere realizzata indipendentemente dall'utilizzo di sistemi di HFT, ma che, nella pratica, è sostanzialmente legata alla negoziazione ad alta frequenza.

Il *Dodd-Frank Act* ha permesso al Dipartimento di Giustizia (DOJ) di perseguire penalmente le violazioni "consapevoli" di molte disposizioni della CEA. Tali reati hanno un periodo di prescrizione di cinque anni e pene che possono arrivare fino ad un massimo di dieci anni di reclusione e una sanzione di un milione di dollari.[52]

---

[48] Y. BATHAEE, *The Artificila Intelligence Black Box and the failure of intent and causation, cit*.
[49] *Ibidem*.
[50] 7 U.S. Code 6(c)(5)
[51] https://www.federalregister.gov/documents/2010/11/02/2010-27547/antidisruptive-practices-authority-contained-in-the-dodd-frank-wall-street-reform-and-consumer
[52] J. CAVOLI, W. CHARLES, C. EVANS, E. CLARKE, K. GIAMPAOLO, C. MARINKOVIC, *Spoofing Under US and UK Law,* Milbank, 2021, disponibile presso https://www.milbank.com/en/news/spoofing-under-us-and-uk-law.html?utm_source=mondaq&utm_medium=syndication&utm_content=inarticlelink&utm_campaign=article

In realtà, permangono comunque le problematiche relative al fallimento degli *intent* o *causation tests* esposte nel precedente paragrafo, ma nella pratica si può affermare che l'inserimento specifico dello *spoofing* tra le pratiche vietate ha contribuito all'aumento delle condanne per questo fenomeno.[53] Caso per caso, infatti, il DOJ ha affrontato le suddette problematiche sul piano dell'accertamento e in alcuni casi è riuscito a superarle a livello probatorio.

Per quanto riguarda i mercati azionari invece lo spoofing può essere perseguito mediante l'applicazione di alcune norme generali relative alla manipolazione del mercato, preesistenti al 2010. In particolare, la sec. 9(a) del *Securities and Exchange Act* (SEA) prevede una serie di specifici comportamenti vietati, perché appunto suscettibili di distorcere artificiosamente il mercato.

Nell'elenco, la condotta che sembra maggiormente affine allo *spoofing* è descritta al punto (2) e prevede "*il compimento, anche d'intesa con altri operatori, di transazioni finanziarie che creano l'apparenza di un mercato attivo di un titolo, o ne deprimono o accrescono il prezzo, allo scopo di indurre l'acquisto o la vendita dello stesso strumento da parte di terzi*."[54]

Occorre a questo punto premettere che, sia nel *Securities and Exchange Act* che nel *Commodities Exchange Act*, le condotte penalmente perseguibili non sono descritte da fattispecie incriminatrici uniche, composte da un precetto comportamentale e da una conseguenza sanzionatoria. Viene infatti adottata una tecnica normativa per la quale gli *Acts* elencano una serie di comportamenti contrari al diritto e vi è poi una norma incriminatrice generale che punisce la violazione di tutte o di alcune disposizioni elencate.[55] Si tratta della sec. 32(a)[56] nella SEA e delle sec. 6(b) e 6(d)[57] nella CEA.

---

[53] J. CAVOLI, K. GIAMPAOLO, E. CLARKE, Milbank LLP, *A Practice Guide on the Law of Spoofing in the Derivatives and Securities Markets*, Wolter Kluwer Legal and regulatory U.S.| Whitepaper, 2021

[54] SEA sec. 9 (a)(2)

[55] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare,* Giuffrè Ed., Milano, 2010.

[56] SEA sec. 32 (a) recita: "*Any person who willfully violates any provision of this title (other than section 30A), or any rule or regulation thereunder the violation of which is made unlawful (...) shall upon conviction be fined not more than $5,000,000, or imprisoned not more than 20 years, or both (...)"*

[57] 7 U.S. Code sec. 13(a) – 13(b). In questo caso il meccanismo sanzionatorio è parzialmente differente. Infatti, in primo luogo l'autorità, accertata la violazione, emette un'ordinanza in cui ordina di cessare o desistere da tale violazione e in cui condanna al pagamento di una "*civil penality*". In caso di inottemperanza dell'ordinanza, il responsabile potrà essere perseguito penalmente. La norma, infatti, recita: "*if any registered entity, or any director, officer, agent, or employee of any registered entity otherwise is violating or has violated any of the provisions of this chapter or any of the rules, regulations, or orders of the Commission thereunder, the Commission may, upon notice and hearing on the record and subject to appeal (...), make and enter an*

Un'ulteriore norma che può essere applicata in caso di *spoofing* è contenuta alla sec. 10(b) SEA, la quale viene però sostanzialmente ricalcata nella sec. 6(c)(1) CEA[58] e quindi viene applicata sia nei mercati azionari che nei mercati delle materie prime. Tale norma sancisce come illecito qualsiasi comportamento o espediente decettivo o ingannevole che contravvenga alle regole che la SEC (o la Commodity Futures Trading Commission per quanto riguarda la sec 6(c)(1) CEA) abbia emanato. La norma, quindi, rinvia alla disciplina regolamentare fissata dalle autorità di settore per la definizione di gran parte del comportamento penalmente rilevante. Probabilmente, infatti, quando è stato emanato il SEA del 1934, le disposizioni che descrivono le condotte manipolative sono state volutamente descritte in termini generici in modo che si potessero adattare a quelle strategie non ancora prevedibili che avrebbero potuto essere escogitate.[59]

Merita inoltre di essere citato il fatto che in relazione alla condotta di *spoofing*, il Dipartimento di Giustizia in alcuni casi ha iniziato a contestare anche la frode telematica o la frode bancaria (che in determinate circostanze godono di una prescrizione decennale) sulla base di alcuni statuti contenuti del Titolo 18 dell'U.S. Code; statuti preesistenti al *Dodd-Frank Act* del 2010, ma che non erano mai stati utilizzati in relazione allo *spoofing.*[60]

Per quanto riguarda invece il Regno Unito, non esiste uno specifico reato di *spoofing.* Tuttavia, tale condotta è riconducibile ad alcuni reati previsti da *Financial Services Act* del 2012 (FSA) e il *Fraud Act* del 2006, nonché alle fattispecie previste dal MAR, il regolamento UE sugli abusi di mercato (596/2014), come importato nel diritto britannico in seguito alla Brexit.[61]

In realtà per quanto riguarda la manipolazione del mercato, prima dell'entrata in vigore dell'FSA, il reato era previsto dalla *section 397* del *Financial Service and Market Act*

---

order directing that such registered entity, director, officer, agent, or employee shall cease and desist from such violation, and assess (...) in any case of manipulation or attempted manipulation in violation of section 9, 15, 13b, or 13(a)(2) of this title, a civil penalty of not more than $1,000,000 for each such violation. If such registered entity, director, officer, agent, or employee, after the entry of such a cease and desist order and the lapse of the period allowed for appeal of such order or after the affirmance of such order, shall fail or refuse to obey or comply with such order, such registered entity, director, officer, agent, or employee shall be guilty of a misdemeanor and, upon conviction thereof, shall be fined not more than $500,000 or imprisoned for not less than six months nor more than one year, or both (...)"

[58] 7 U.S. Code sec. (9)(1) recita: "*It shall be unlawful for any person, directly or indirectly, to use or employ, or attempt to use or employ, (...) any manipulative or deceptive device or contrivance, in contravention of such rules and regulations as the Commission shall promulgate by not later than 1 year after July 21, 2010(...)"*

[59] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare,* cit.

[60] J. CAVOLI, W. CHARLES, C. EVANS, E. CLARKE, K. GIAMPAOLO, C. MARINKOVIC, *Spoofing Under US and UK Law*, cit.

[61] *Ibidem.*

(FSMA) che prevedeva la prova dell'*inducement*, ossia del fatto che l'imputato avesse indotto un'impressione falsa o fuorviante in relazione al mercato. Questo rendeva la normativa sostanzialmente inapplicabile ai casi in cui il reato fosse commesso attraverso l'HFT.[62]

Nel 2012 poi la fattispecie è stata modificata con la *section* 90 della FSA 2012 e attualmente recita:

> *1.Una persona che compie un atto o mette in atto un comportamento che crei un'impressione falsa o fuorviante in merito al mercato, al prezzo o al valore degli investimenti rilevanti commette un reato se*
>
> *a) intende creare l'impressione*
>
> *b) il caso rientra nel comma (2) o (3) (o in entrambi)*
>
> *2. Il caso rientra nel precedente comma se la persona intende, creando l'impressione, indurre un'altra persona ad acquistare, cedere, sottoscrivere o sottoscrivere gli investimenti o ad astenersi dal farlo o ad esercitare o astenersi dall'esercitare qualsiasi diritto conferito dagli investimenti.*
>
> *3. Il caso rientra nel comma 1 se la persona sa che l'impressione è falsa o fuorviante o è incauto al riguardo e se ha l'obbiettivo di ottenere un guadagno (per sé o per altri), o causare una perdita ad altri, creando l'impressione (o è consapevole che la creazione dell'impressione è suscettibile di produrre tali risultati).*

Quindi con la sec. 90 gli elementi oggetto di prova da parte del *prosecutor* sarebbero: il fatto che l'imputato abbia compiuto la condotta o vi abbia concorso, il fatto che tale condotta abbia causato un'impressione falsa o fuorviante in relazione al mercato e l'elemento soggettivo che può essere sia una vera e propria intenzionalità che una semplice "imprudenza".

Si possono quindi distinguere cinque ipotesi:[63]

I. L'imputato intendeva indurre un'altra persona a intraprendere, o ad astenersi dall'intraprendere, un'attività di mercato.

---

[62] J. FISHER, A. CLIFFORD, F. DINSHAW AND N. WERLE, *Criminal forms of high frequency trading on the financial markets*, in *Law and Financial Markets Review*, Vol. 9, No. 2, London School of Economics, London, 2015.

[63] *Ibidem*.

II. L'imputato sapeva che l'impressione era falsa o fuorviante e intendeva ottenere un guadagno o causare una perdita.

III. L'imputato sapeva che l'impressione era falsa o fuorviante, ed era consapevole che la creazione dell'impressione avrebbe facilmente comportato un guadagno, una perdita o un rischio di perdita.

IV. L'imputato è stato imprudente nel ritenere che l'impressione fosse falsa o fuorviante e intendesse ottenere un guadagno o di causare una perdita.

V. L'imputato è stato imprudente nel ritenere che l'impressione fosse falsa o fuorviante ed era consapevole che la creazione dell'impressione avrebbe facilmente comportato un guadagno, una perdita o un rischio di perdita.

La nuova normativa rende quindi più facile per l'accusa provare la colpevolezza dell'imputato anche nei casi in cui il reato sia commesso attraverso sistemi di HFT.

Una diversa accusa che può essere contestata in caso di *spoofing* nel Regno Unito prevede l'applicazione della *section* 2 del Fraud Act 2006, per la quale è necessario dimostrare che l'imputato ha fraudolentemente creato una falsa rappresentazione con la quale intendeva ottenere un guadagno (per sé o per un'altra persona), o causare una perdita, o esporre un'altra persona a un rischio di perdita.[64]

Tali reati sono attualmente puniti con una sanzione pecuniaria illimitata e/o con la reclusione fino a 7 anni, per la s.90 FSA, e fino a 10 anni per il reato di frode.[65]

3.4 Una breve parentesi: la manipolazione del mercato realizzata attraverso i *social bots*

Oltre agli HFT, esistono altre applicazioni dell'intelligenza artificiale ai mercati finanziari. L'IA viene utilizzata per esempio anche in ambienti esterni alle piattaforme di negoziazione, nell'ambito di settori che influenzano indirettamente il prezzo dei titoli. È evidente, infatti, l'enorme impatto sui mercati delle notizie diffuse attraverso *internet* e in particolare attraverso i *social media*. Questo dato viene talvolta sfruttato da strategie manipolative diverse rispetto a quelle precedentemente analizzate; tale manipolazione, detta

[64] J. CAVOLI, W. CHARLES, C. EVANS, E. CLARKE, K. GIAMPAOLO, C. MARINKOVIC, *Spoofing Under US and UK Law, cit.*
[65] *Ibidem.*

"informativa", consiste nella diffusione di notizie false o fuorvianti finalizzate ad influenzare l'andamento dei prezzi.[66]

Questo tipo di condotta viene talvolta realizzata tramite dei sistemi di IA chiamati *social bots*; si tratta di *software* che, automatizzando alcuni *account* della piattaforma, simulano comportamenti di utenti reali. I *bots* possono essere utilizzati per vari scopi leciti, ad esempio per finalità legate al *marketing*, ma talvolta vengono programmati per diffondere informazioni fuorvianti, al fine di modificare intenzionalmente i prezzi o di creare un'impressione di interesse per i prodotti finanziari.[67] Possono inoltre essere programmati con l'obbiettivo di ingannare, con le proprie interazioni, altri partecipanti al mercato, compresi gli algoritmi di lettura delle notizie dei rivali.[68]

Specificatamente, i *social bots* possono essere impiegati per il "*pump and dump"*, una particolare strategia manipolativa che consiste nel fare lievitare artificialmente il prezzo di un titolo, mediante dichiarazioni false, fuorvianti o esagerate, con l'obiettivo di vendere titoli ad un prezzo superiore di quello di acquisto.[69] Ovviamente in questi casi non si pongono particolari problematiche in relazione al dolo poiché si tratta sempre di una manipolazione *by design*.

3.4.1 L'utilizzo dell'intelligenza artificiale sulle piattaforme social per manipolare il mercato: il caso di Twitter

Un esempio del fenomeno descritto nel precedente paragrafo è stato analizzato da alcuni studiosi italiani nell'ambito di un lavoro relativo all'influenza del comportamento di *social bots*, presenti su Twitter, sull'andamento di alcuni titoli.[70]

Lo studio evidenzia la larga diffusione dei *bots* su Twitter e l'esistenza di *bots* "evoluti" che imitano in modo fedele il comportamento umano e generalmente agiscono in maniera coordinata e sincronizzata. I *bots* sono sistemi di IA che operano su piattaforme *social* e

---

[66] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia*, p. 378, Wolters Kluwer, Milano, 2020

[67] A. AZZUTTI, W. G. RIING, H. S. STIHEL, *Machine learning, Market Manipulation and Collusion on capital markets why the "Black Box" matters,* in *University of Pennsylvania Journal of International Law,* 2021.

[68] *Ibidem*.

[69] R. BORSARI, *Intelligenza artificiale e responsabilità penale: le prime considerazioni,* in *Media Laws*, 2019.

[70] S. CRESCI, F. LILLO, D. REGOLI, S, TARDELLI, M. TESCONI, *Cashtag Piggybacking: Uncovering Spam and Bot Activity In Stock Microblogs On Twitter*, aprile 2019.

gestiscono degli *account*s operando come persone fisiche. I *bots* sono spesso indistinguibili, per coloro che vi entrano in contatto, dagli utenti umani.

Il *paper* ha evidenziato che i *microblogs*[71] sono sempre più sfruttati per prevedere i prezzi e i volumi scambiati dei titoli nei mercati finanziari. Tuttavia, gran parte dei contenuti di tali *microblogs* è creata da *accounts bot*.

Lo studio, in modo innovativo, si è proposto di approfondire l'impatto degli *stock microblogs* di Twitter sull'andamento dei prezzi di alcuni titoli azionari dei cinque principali mercati finanziari statunitensi. La ricerca è fondata sulla comparazione tra picchi di *tweets* riguardanti determinati titoli e l'innalzamento di valore di tali titoli sui mercati. È stato infatti notato che, in corrispondenza al picco di *tweets* riguardanti un determinato titolo, si verificava un aumento del prezzo dello stesso titolo sui mercati azionari.

Nell'indagare le cause di questo fenomeno, gli autori del *paper* hanno ricostruito l'adozione di una pratica potenzialmente manipolativa: è stato verificato che i messaggi comparsi nei *microblogs* abbinavano il titolo oggetto di manipolazione a titoli particolarmente liquidi.

In particolare, l'indagine è stata svolta utilizzando i cosiddetti "*cashtags".* Twitter, infatti, segue la convenzione di *taggare* gli *stock microblogs* con un "*cashtag"*: un simbolo formato dal dollaro e dalla sigla del titolo (es. $AAPL). Cliccando su un tale simbolo sarà possibile visionare altri tweets con lo stesso riferimento azionario.[72] Alla luce della lista dei 6689 titoli commerciati sui principali mercati USA, sono stati considerati i *tweets* dove appariva anche solo un *cashtag* della lista del periodo da maggio a settembre 2017.

È stato rilevato che in corrispondenza agli squilibri nei prezzi dei titoli, si registrava un picco di *tweets* che accostavano *cashtags* di titoli molto liquidi (come Tesla o Apple) a titoli poco liquidi, scambiati in mercati non regolamentati. Si può dedurre che questo abbinamento abbia favorito la pubblicizzazione sulla piattaforma *social* dei titoli di basso valore, che hanno beneficiato della notorietà dei titoli ai quali erano stati accostati. Tale pratica, definita *cashtag piggybacking,* è stata attuata da gruppi coordinati di bots. I ricercatori, infatti, attraverso l'utilizzo di un sofisticato algoritmo che identifica i *bot*s, hanno

[71] I *microblogs* sono una forma di pubblicazione costante di piccoli contenuti in rete, sotto forma di brevi messaggi di testo, immagini, video, audio MP3, ma anche segnalibri, citazioni, appunti. Questi contenuti vengono pubblicati in un servizio di rete social, visibili a tutti o soltanto alle persone della propria comunità.
[72] Si veda https://help.twitter.com/it/resources/glossary#:~:text=cashtag,menzionano%20lo%20stesso%20simbolo%20azionario.

accertato che ben il 71% degli autori di *tweets* finanziari sospetti erano in realtà sistemi di IA.

A dimostrazione della fondatezza delle conclusioni, il *paper* evidenzia che pochi mesi dopo la pubblicazione dell'indagine, il 37 % di tali accounts è stato sospeso da Twitter.

Lo studio citato apre un'interessante prospettiva su un ulteriore impiego dei sistemi di IA in relazione a condotte manipolative del mercato. Questo fenomeno, tuttavia, pare porre minori problemi di accertamento a livello penalistico. È evidente, infatti, che la vasta scala dell'attività, la coordinazione e il controllo dei *social bots*, necessari per la realizzazione di tale pratica, presuppongono una precisa volontà manipolatoria da parte della persona fisica organizzatrice.

CAPITOLO IV
IL REATO DI MANIPOLAZIONE DEL MERCATO NELL'ORDINAMENTO ITALIANO: L'ARTICOLO 185 TUF

SOMMARIO: 4.1 L'analisi della norma – 4.1.1 La tradizione giuridica italiana e la normativa euro unitaria – 4.1.2 L'interesse tutelato – 4.1.3 I soggetti attivi – 4.1.4 Le condotte: la distinzione tra manipolazione informativa e operativa – 4.1.5 Altri artifici – 4.1.6 Le fonti utilizzabili per risolvere i problemi di indeterminatezza – 4.1.7 Il requisito della "*price sensitivity*" – 4.1.8 Il momento consumativo – 4.1.9 Il dolo – 4.1.10 Le prassi di mercato ammesse – 4.1.11 Il trattamento sanzionatorio – 4.1.12 La fattispecie amministrativa, l'articolo 187-*ter* – 4.2 L'applicabilità della norma italiana alla fattispecie realizzata attraverso sistemi di HFT: i possibili punti critici – 4.2.1 Il soggetto attivo – 4.2.2 La condotta – 4.2.3 La causalità – 4.2.4 Il dolo – a) L'oggetto del dolo – b) Il dolo dell'utilizzatore; tra *dolus generalis* e dolo eventuale – c) Il dolo del programmatore; il dolo di concorso – 4.3 Le criticità sottese all'elemento soggettivo e le soluzioni proposte – 4.3.1 *Strict liability* – 4.3.2 *Actio libera in causa* – 4.3.3 Responsabilità indiretta – 4.3.4 Interpretazione estensiva dell'art.8 del d.lgs. 231/2001

4.1 L'analisi della norma

Delineate le principali problematiche, affrontate soprattutto dalla dottrina e dalla giurisprudenza anglosassone, in relazione ad operazioni manipolatorie effettuate grazie a sistemi di HFT, il presente capitolo passerà ad un'analisi del problema dal punto di vista dell'ordinamento italiano. Si inizierà, quindi, da una panoramica relativa al reato di "manipolazione del mercato" previsto all'art 185 del d.lgs. n.58 del 1998 (Testo Unico in materia di intermediazione finanziaria).[1]

4.1.1 La tradizione giuridica italiana e la disciplina eurounitaria

Già il codice Zanardelli ed alcuni codici preunitari punivano il fenomeno manipolativo del mercato, denominato aggiotaggio.[2] Il Codice Rocco ha poi inserito l'art. 501, rubricato "*Rialzo e ribasso fraudolento di prezzi sul pubblico mercato o nelle borse di commercio"*, che prevedeva già una distinzione tra una condotta informativa (pubblicazione o diffusione

[1] D'ora in avanti TUF.

[2] A. GALANTI, *La manipolazione del mercato*, in *Diritto penale dell'impresa*, vol. 10, Cendon, Keyeditore, Milano 2015, p. 11.

di notizie false, esagerate o tendenziose) e una condotta operativa che si riferiva al compimento di "*altri artifici*".[3]

Sono state successivamente inserite altre ipotesi di aggiotaggio (come quello bancario o societario), poi unificate in un'unica fattispecie introdotta nell'ambito della riforma dei reati societari operata dal d.lgs. n. 61 del 2002. Si tratta dell'art. 2637 c.c., rubricato nuovamente "*aggiotaggio*".[4]

Nel 2003, in aggiunta al panorama normativo interno, viene introdotta un'ulteriore disciplina, di origine comunitaria. Viene infatti emanata una direttiva europea relativa agli abusi di mercato (MAD)[5] che induce il legislatore italiano a integrare l'ordinamento con una nuova fattispecie di manipolazione del mercato. La legge di conversione della MAD (l. n.62/2005) introduce, nel Titolo I-*bis* del TUF, l'art 185 ("*manipolazione del mercato*") e contemporaneamente, restringendo l'ambito di operatività dell'art 2637 c.c., distingue le due fattispecie dal punto di vista dell'oggetto materiale della condotta. Sebbene il nuovo art. 185 TUF ricalchi sostanzialmente la fattispecie prevista nel Codice civile, l'art 2637 c.c. rimane in vigore in relazione all'aggiotaggio bancario e per quanto riguarda le condotte manipolative effettuate su "*strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato di un paese appartenete all'UE.*"[6] Si desume quindi che il generico riferimento dell'art 185 TUF agli "strumenti finanziari" riguardi gli strumenti quotati o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato di un paese appartenete all'UE.[7]

Nel 2014 il panorama normativo sovranazionale è mutato con l'emanazione del Regolamento n. 596/2014 (Market Abuse Regulation o MAR) e della Direttiva 2014/57/UE (MAD II), le quali hanno indotto il legislatore italiano a modificare nuovamente la fattispecie in questione. L'art 185 TUF, infatti, è stato integrato in conseguenza dell'inserimento da parte delle fonti comunitarie di nuove piattaforme di negoziazione: gli *Organised Trading*

[3] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare,* Giuffrè Ed., Milano, 2010, p.188, A. GALANTI, *La manipolazione del mercato*, *cit.*, p.14.
[4] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia*, Wolters Kluwers, Milano, 2020, p.375.
[5] Direttiva 2003/6/ CE (MAD)
[6] F. SGUBBI, D. FONDAROLI, A.F. TRIPODI, *Diritto Penale del Mercato Finanziario*, CEDAM, Padova, 2013, p.72.
[7] A. GALANTI, *La manipolazione del mercato*, *cit.*, p.16.

Facility (OTF) e i *Multilateral Trading Facility* (MTF).[8] Il d.lgs. n.107/2018 ha quindi inserito nella norma in esame un comma 2-*bis* che prevede una fattispecie contravvenzionale in relazione alle medesime condotte previste dal primo comma se realizzate in relazione a strumenti finanziari negoziati su OTF o MTF, a derivati o a quote di emissione.[9] Tuttavia la scelta di prevedere una pena meno severa per tali condotte ha suscitato alcune perplessità in dottrina, poiché il disvalore della fattispecie è apparso comunque analogo rispetto ai fatti puniti più gravemente dal primo comma.[10]

Nel 2021 il legislatore italiano è stato costretto ad apportare alcune ulteriori modifiche alla normativa interna all'esito delle contestazioni sollevate dalla Commissione Europea.[11] La legge n.238/2021[12] ha equiparato le condotte realizzate su strumenti finanziari negoziati su mercati regolamentati e quelle realizzate su strumenti negoziati in altre *trading venues,* come OTF o MTF. In particolare, sono stati abrogati i commi 2-*bis* e 2-*ter*: di conseguenza si ritiene che il delitto di cui al primo comma si riferisca, con l'espressione "strumenti finanziari", a tutte le condotte che hanno per oggetto qualsiasi strumento finanziario, anche se negoziato su piattaforme diverse dai mercati regolamentati.[13]

---

[8] I MTF sono sistemi multilaterali di negoziazione diversi dai mercati regolamentati che, al pari di questi, consentono l'incontro al loro interno, in base a regole non discrezionali, di proposte dirette alla conclusione di contratti aventi per oggetto qualsiasi strumento finanziario. Gli OTF sono un'altra categoria di piattaforma in cui, a differenza dei mercati regolamentati e dei MTF, il gestore ha un potere discrezionale in ordine all'esecuzione degli ordini immessi nel sistema. Si veda A. PERRONE, *Il diritto del Mercato dei Capitali*, Giuffrè, Milano 2020, p. 296.

[9] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia*, *cit*., p.375

[10] M. GAMBARDELLA, *Condotte economiche e responsabilità penale*, Giappichelli, Torino, 2020, p.407.

[11] Si tratta della procedura di infrazione n. 2019/2130, sollevata dalla Commissione Europea contro l'Italia in relazione a vari aspetti:

i) l'ambito di applicazione dei reati e degli illeciti amministrativi (art. 182 del TUF);
ii) il regime sanzionatorio previsto per i reati che riguardano strumenti finanziari negoziati su sistemi multilaterali di negoziazione (MTF) e sistemi organizzati di negoziazione (OTF), nonché per la manipolazione degli indici di riferimento (art. 182, 184, comma 1, e 185 del TUF);
iii) la punibilità dei c.d. insider secondari (art. 184, comma 3, del TUF);
iv) la confisca penale limitata al solo profitto del reato (art. 187, comma 1, del TUF).

[12] Legge europea 2019-2020 (22G00004), *Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea*.

[13] Audizione della Consob presso la Quattordicesima Commissione Permanente (Politiche dell'Unione Europea) del Senato della Repubblica, in relazione al disegno di legge n. 2169 ("Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea" - Legge europea 2019-2020), si veda https://www.senato.it/application/xmanager/projects/leg18/attachments/documento_evento_procedura_commissione/files/000/354/301/CONSOB.pdf

4.1.2 L'interesse tutelato

Le fattispecie di manipolazione del mercato sono finalizzate, in linea di principio, a tutelare l'integrità e l'efficienza dei mercati, in modo tale da conservare la fiducia degli investitori nei valori mobiliari e negli strumenti derivati, quale fattore essenziale per la crescita e il benessere economico.[14] Tuttavia, a livello più immediato e diretto, si può affermare che il reato previsto all'art 185 TUF tuteli la corretta formazione dei prezzi degli strumenti finanziari quotati.[15] Infatti la fattispecie punisce le condotte informative e operative solo nel caso in cui queste siano concretamente idonee a provocare una "*sensibile alterazione del prezzo di strumenti finanziari*".

4.1.3 I soggetti attivi

La manipolazione del mercato è un reato comune, come suggerisce tra l'altro il termine "chiunque". A differenza di quanto avviene nella fattispecie gemella prevista dall'art 184 TUF (*Abuso di informazioni privilegiate*), il pronome non è infatti accompagnato da nessun tipo di condizione relativa al soggetto attivo.[16]

Pertanto, non è necessario che l'autore del reato possieda una particolare qualifica o svolga una specifica attività, ad esempio che ricopra un determinato ruolo all'interno di una società o che faccia parte dell'organico impiegato per il funzionamento di una piattaforma di negoziazione. Tali elementi rileveranno invece ai fini dell'aggravante prevista dal secondo comma dell'art 185 TUF che prevede, tra i fattori che possono essere considerati dal giudice ai fini dell'aumento della pena pecuniaria, anche "*le qualità personali del colpevole*". [17]

4.1.4 Le condotte: la distinzione tra manipolazione informativa e operativa

Il reato di manipolazione del mercato contempla diverse tipologie di condotte: in particolare la fattispecie punisce "*chiunque diffonda notizie false o ponga in essere*

[14] Direttiva 2014/57/UE, considerando n.1
[15] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia*, *cit.*, p. 376; A. GALANTI, *La manipolazione del mercato, cit.*, p. 41.
[16] F. SGUBBI, D. FONDAROLI, A.F. TRIPODI, *Diritto Penale del Mercato Finanziario, cit.,* p. 74.
[17] Si veda § 4.1.11

operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari".

Una visione classica, derivante dall'impostazione americana della disciplina, impone la bipartizione tra la manipolazione "informativa" (*information-based manipulation*) che prevede la "diffusione di notizie false", e la manipolazione "operativa" (*trade-based manipulation*) che prevede invece il "compimento di operazioni simulate o altri artifici".[18]

Riservando l'approfondimento del significato del termine "artifici" al seguente paragrafo, possiamo anticipare in questa sede che, secondo alcuni autori, le condotte descritte dall'art. 185 TUF sarebbero tre: due "nominate" (la diffusione di notizie false e il compimento di operazioni simulate) e una "innominata" (il compimento di altri artifici). Secondo questa impostazione, la condotta informativa e quella simulatoria costituirebbero in realtà un'elencazione esemplificativa rispetto al "*compimento di altri artifici*" che, ben lungi dall'essere una semplice formula di chiusura, costituirebbe il vero fulcro della fattispecie.[19] Si tratta di una tecnica legislativa frequentemente utilizzata che sembra ricalcare, ad esempio, la struttura del reato previsto dall'art. 434 c.p. che punisce chiunque commetta "*un fatto diretto a cagionare il crollo di una costruzione o di una parte di essa ovvero un altro disastro."*

La manipolazione informativa consiste nella diffusione di notizie false. Con diffusione si intende qualsiasi tipo di comunicazione, trasmessa con qualsiasi mezzo, diretta ad un numero indeterminato di persone.[20] La notizia diffusa deve essere falsa e quindi non conforme al vero, anche se in realtà l'art 5 della direttiva 214/57/UE (MAD II) fa riferimento alla trasmissione di notizie "*false o fuorvianti*". Pertanto, alla luce di tale disposizione parte della dottrina propone un'interpretazione estensiva del termine "false" nel senso di ricomprendere nel fatto tipico anche informazioni esagerate, tendenziose o comunque appunto fuorvianti rispetto ad un contesto di riferimento.[21] Altra parte della dottrina, rimanendo più aderente al testo della norma incriminatrice, esclude la possibilità di ampliare il novero di comportamenti punibili.[22] Appare opportuno evidenziare che, la diffusione di

[18] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia*, *cit*., p. 376
[19] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare, cit*., p.213.
[20] F. SGUBBI, D. FONDAROLI, A.F. TRIPODI, *Diritto Penale del Mercato Finanziario*, *cit*., p. 75.
[21] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia*, *cit*., p. 382,
[22] F. MUCCIARELLI, *Aggiotaggio*, in *Il nuovo diritto penale delle società*, a cura di A. Alessandri, Milano, 2002, p. 425.

informazioni esagerate, tendenziose o fuorvianti potrebbe in ogni caso rientrare nella nozione di "altri artifici".[23]

Ai fini del presente lavoro, la fattispecie che risulta maggiormente rilevante è la manipolazione operativa, poiché è quella che potrebbe più facilmente essere realizzata da sistemi di IA che operano *trading* ad alta frequenza. È su queste condotte, quindi, che si soffermerà l'analisi del reato.

In riferimento al compimento di operazioni simulate, occorre innanzitutto distinguere tra una simulazione relativa e una simulazione assoluta. Il primo caso si realizza quando il tipo di negozio finanziario compiuto in realtà ne cela un altro, realmente voluto dalle parti. Il secondo caso, maggiormente frequente in questi ambiti, prevede il compimento di operazioni che vengono compiute solo formalmente, ma che in realtà non producono alcun effetto pratico.[24]

Alcuni esempi di strategie di questo tipo consistono nel compimento di *improper matched orders*[25], dei cosiddetti *wash sales*[26] o del *painting the tape.*[27]

4.1.5 Altri artifici

La nozione di "artifici", seppur nota al penalista, presenta in questo contesto alcuni problemi di carattere definitorio. Sia che si voglia intenderla come una formula di chiusura, che come il fulcro della norma, contenente i caratteri tipici delle altre condotte,[28] tale espressione appare alquanto vaga e potenzialmente idonea a provocare dei problemi in relazione alla determinatezza della fattispecie penale.[29]

---

[23] *Ibidem*.
[24] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare, cit.*, p. 195.
[25] Si tratta di una strategia in cui due o più operatori si scambiano in contemporanea le medesime quantità di uno strumento finanziario, simulando un movimento del mercato, che in realtà non si riflette sugli assetti possessori iniziali, che rimangono invariati. Si veda F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare, cit.*, p.195.
[26] Si tratta di una strategia che prevede il compimento di operazioni di compravendita di strumenti finanziari, che non comporta una reale modifica della proprietà beneficiaria o del rischio di mercato. Si veda N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia*, *cit*., p. 383.
[27] Si tratta di una strategia secondo la quale le negoziazioni sono finalizzate a creare un'impressione di fluttuazioni del prezzo di uno strumento finanziario o dell'esistenza di un mercato attivo. Si veda *ibidem*.
[28] Si veda § 4.1.4.
[29] F. SGUBBI, D. FONDAROLI, A.F. TRIPODI, *Diritto Penale del Mercato Finanziario*, *cit*. p.81.

In primo luogo, secondo la dottrina maggioritaria non sarebbe necessario che gli strumenti giuridici rientranti nella nozione di artifici siano intrinsecamente illeciti.[30] Sarebbe invece la combinazione di condotte di per sé non vietate e di determinate circostanze spazio-temporali che integrerebbe la condotta decettiva tipica degli artifici.[31] A giustificazione di tale assunto, è possibile riportare le considerazioni contenute nella *Relazione di accompagnamento del codice Rocco* in relazione alla distinzione tra l'espressione "altri artifici" dell'art. 501 c.p. e quella "altri mezzi fraudolenti" contenuta invece nell'abrogato art 2628 c.c. In tale relazione si sottolineava infatti come la nozione di "artifici" avesse un contenuto più ampio rispetto a quella di "mezzi fraudolenti" che invece presupponeva l'intrinseca illiceità del mezzo utilizzato.[32]

Si ritiene quindi che l'attitudine distorsiva del mercato di tali condotte prescinda dal fatto che i mezzi utilizzati siano di per sé vietati o meno.

Una parte minoritaria della dottrina, invece, obbietta che la peculiarità degli artifici rispetto alle altre due condotte (informativa e simulatoria) non possa riguardare solo la capacità di influenzare l'andamento dei prezzi: altrimenti si andrebbe a confondere il giudizio sul comportamento complessivo dell'agente con quello sulla mera reazione del mercato rispetto alla condotta.[33]

La giurisprudenza, tuttavia, ha smentito quest'ultima impostazione. In un caso del 2002, ad esempio, sono stati definiti "artifici" ai fini dell'integrazione della fattispecie dell'allora aggiotaggio, i comportamenti che integrano la strategia del "*marking the close*". Si tratta di una modalità di alterazione del prezzo di determinati strumenti finanziari che si concretizza con l'inserimento di molti ordini solo alcuni istanti prima della chiusura della giornata di negoziazione. In questo modo tali ordini non possono essere assorbiti dal mercato e il prezzo dello strumento finanziario risulta alterato. Su questo punto il Tribunale di Milano ha affermato: «*L'inganno può essere realizzato attraverso condotte apparentemente lecite, ma che combinate tra loro, ovvero realizzate in presenza di determinate circostanze di tempo e di luogo intenzionalmente realizzino una distorsione del gioco della domanda e dell'offerta*

[30] A. GALANTI, *La manipolazione del mercato*, *cit*., p.75.
[31] F. MUCCIARELLI, *Altri artifici: una (controversa) modalità di realizzazione del delitto di manipolazione del mercato*, in *Studi in onore di Mario Romano*, Napoli, 2011, p. 2026
[32] F. SGUBBI, D. FONDAROLI, A.F. TRIPODI, *Diritto Penale del Mercato Finanziario*, *cit*. p.82.
[33] C. PEDRAZZI, *Turbativa dei mercati*, In *Dig. Disc. Pen*., XIV, 1999, p. 421 ss.

in modo tale che il pubblico degli investitori sia indotto in errore circa lo spontaneo e corretto processo di formazione dei prezzi»[34]

Un ulteriore aspetto rilevante, per quanto riguarda la definizione di "artifici", è il parallelismo con il reato di truffa previsto all'art. 640 c.p. Anche in questo settore, infatti, l'insidiosità dell'inganno varia sempre in rapporto alla situazione, all'ambiente e al momento in cui è stata tenuta.[35]

Tuttavia, se nel reato di truffa l'artificio si accompagna ad un elemento fattuale necessario alla consumazione del reato, ossia l'induzione in errore, il reato previsto dall'art 185 TUF non richiede questo passaggio, in quanto è sufficiente che gli artifici siano "*concretamente idonei a provocare una sensibile alterazione dei prezzi degli strumenti finanziari*". Occorre tenere presente però che l'alterazione dei prezzi verrebbe eventualmente prodotta dalla reazione dei partecipanti al mercato, i quali, fuorviati dal panorama operativo o informativo creato dal manipolatore, agirebbero di conseguenza. Si potrebbe quindi affermare che anche nella manipolazione del mercato è presente, in senso lato, un inganno. Semplicemente, invece che riferirsi ad un soggetto determinato, come avviene nella truffa, tale inganno si rivolge genericamente a tutti i partecipanti al mercato, in un contesto de-individualizzato, regolato da procedure di registrazione elettroniche.[36]

Ovviamente nell'art 185 TUF la soglia di consumazione viene anticipata rispetto alla truffa, perché non rileva l'effettivo verificarsi del danno né dell'induzione in errore. Nella truffa, invece, si considerano punibili solo le condotte che hanno effettivamente influenzato il convincimento di un altro soggetto, a prescindere dall'astratta idoneità ingannatoria degli artifici.[37]

La rilevanza collettiva degli interessi coinvolti nella manipolazione del mercato ha quindi indotto il legislatore all'utilizzo di una nozione più estensiva di artifici, rispetto a quella utilizzata nella fattispecie prevista dall'art 640 c.p. Infatti, le operazioni finanziarie devono adeguarsi a determinate procedure o a specifici *standard* di correttezza, imposti per

---

[34] Trib. Milano, 11 novembre 2002, in *Riv. Trim. dir. pen. ec*., 2003 confermata dalla Corte di Appello di Milano (App. Milano 17 marzo 2004, in *Foro ambr*., 2005) e dalla Cassazione (Cass. sez. V, 07 dicembre 2004, in *Banca borsa tit. cred*., 2006).

[35] G. LA CUTE, *Truffa*, in *Enc. dir. (XLV)*, Giuffrè, 1992.

[36] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare, cit.*, p.199

[37] Cass., sez. II, 27-7-1990. Si veda inoltre P. PISA, *Giurisprudenza Commentata di Diritto Penale, Volume Primo, Delitti contro la persona e contro il patrimonio*, Wolters Kluwer, Milano, 2018, p. 615.

il corretto funzionamento dei mercati.[38] In questo senso la maggiore attenzione nei mercati finanziari, rispetto ad altri settori giuridici, a valori come la trasparenza e la correttezza, secondo alcuni autori, può essere considerata come un fattore alla luce del quale poter dettagliare la nozione di artifici.[39] Pertanto, alcune condotte che, nelle relazioni patrimoniali tra privati, non sarebbero penalmente rilevanti, nel contesto dell'ordinamento finanziario potrebbero più facilmente assumere rilevanza penale in quanto lesive di principi di trasparenza ed efficienza.[40]

4.1.6 Le fonti utilizzabili per risolvere i problemi di indeterminatezza

Nonostante le considerazioni svolte nel precedente paragrafo, appare comunque evidente come la fattispecie di manipolazione del mercato possa entrare pericolosamente in tensione con il principio di determinatezza delle condotte; e ciò soprattutto in relazione alla nozione di "altri artifici".

Al di là di possibili dubbi in relazione al rispetto del principio di legalità in materia penale, in un contesto come quello dei mercati finanziari è particolarmente importante che gli operatori economici conoscano con certezza quali condotte potrebbero essere considerate manipolative e quali invece siano lecite.[41]

Per ovviare a questo problema, è possibile fare riferimento, a livello interpretativo, ad alcune fonti (sovranazionali e interne) che elencano operazioni o strategie che devono essere considerate manipolative. Senza alcuna pretesa di esaustività, questi elenchi hanno una duplice funzione: da una parte, quella di aiutare l'interprete a definire maggiormente la norma e ridurre la sfera di indeterminatezza, dall'altra, in un'ottica preventiva, quella di consentire agli operatori del mercato di conoscere quali condotte devono ritenersi sicuramente illecite.[42]

Una delle fonti che può essere utilizzata a questo fine è di carattere sovranazionale e si ha nel Regolamento n. 596/2014 (MAR) e in particolare nell'Allegato I.

---

[38] Ad esempio, l'art 21 c.1 lett. a) del TUF impone che "*nella prestazione dei servizi e delle attività di investimento e accessori i soggetti abilitati devono comportarsi con diligenza, correttezza e trasparenza, per servire al meglio l'interesse dei clienti e per l'integrità dei mercati*"

[39] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare, cit.*, p. 201

[40] *Ibidem.*

[41] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia*, Wolters Kluwers, Milano, 2020

[42] *Ibidem*.

L'art 12 del MAR, infatti, definisce, attraverso disposizioni generali, cosa si intende per manipolazione del mercato. Tale definizione non è tuttavia parallela a quella fornita dall'art 185 TUF, ma è fondata su indicazioni esemplificative. Tali previsioni generali sono poi specificate al secondo comma dell'art 12 attraverso un elenco di più concreti comportamenti manipolativi.

L'Allegato I fornisce un elenco di indicatori non tassativi e non vincolanti utili per la qualificazione della condotta come abusiva.

Tra questi vanno menzionati quelli previsti alle lettere c) ed e).

Il primo, che recita "c) *se operazioni avviate non portano a modificare la titolarità economica 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*", pare ricomprendere la strategia manipolativa denominata *improper matched orders.*[43]

Il secondo, che prevede quale specifico indicatore "e) *la misura in cui gli ordini di compravendita inoltrati o le operazioni avviate sono concentrati in un breve lasso di tempo nel corso della sessione di negoziazione e determinano una variazione del prezzo che successivamente si inverte*", pare riferibile alle strategie manipolative effettuate attraverso la contrattazione ad alta frequenza.

Un ulteriore documento utile a livello interpretativo è la Comunicazione n. DME/5078692 del 29/11/2005 della Consob, con cui l'agenzia ha riprodotto, sostanzialmente traducendoli, vari esempi di manipolazioni del mercato e di operazioni sospette indicate dal *Committee of European Securities Regulators* (CESR) nel documento "*Market Abuse Directive - Level 3 – first set of CESR guidance and information on the common operation of the Directive.*[44] Tali esempi, come si precisa nella comunicazione, hanno come scopo quello di fornire una guida per operatori e riguardano in realtà la fattispecie amministrativa di manipolazione del mercato, prevista dall'art 187-*ter* del TUF anche se *"possono ricondursi anche ad altre ipotesi ivi previste"*.[45] Tali indicazioni, fornite

[43] Si veda nota 25.

[44] Documento disponibile presso https://www.esma.europa.eu/document/market-abuse-directive-level-3-%E2%80%93-first-set-cesr-guidance-and-information-common-operation

[45] La Comunicazione n. DME/5078692 del 29-11-2005, nella sezione A, afferma infatti: "*Gli esempi indicati di seguito:*
a) hanno la mera finalità di fornire una guida agli operatori;
b) sono scritti in linguaggio non tecnico-giuridico;
c) costituiscono una elencazione non esaustiva e non limitano l'ambito di applicazione delle fattispecie cui sono riferiti;

dall'autorità di settore, possono essere utilizzate dall'interprete come elementi utili a qualificare una condotta come manipolativa o meno, senza ovviamente trascurare il puntuale accertamento degli ulteriori aspetti della fattispecie.

Un aspetto particolarmente interessante, in relazione al *focus* del presente lavoro, consiste nel fatto che una delle strategie elencate dalla Consob nella citata comunicazione è denominata come "*placing orders with no intention of executing them",*[46] condotta che sembra sostanzialmente definire la già menzionata pratica dello *spoofing*.[47] La crescente diffusione di tale pratica ha indotto l'Autorità a specificare ulteriormente la propria comunicazione. Con la Comunicazione n DME/10039224 del 30 aprile 2010 la Consob ha precisato che "*benché l'immissione e la successiva cancellazione di ordini non costituisca di per sé manipolazione di mercato, tale modalità operativa rappresenta comunque uno degli elementi o circostanze da prendere in considerazione al fine di valutare se un comportamento sia qualificabile come manipolativo.*"

Naturalmente le fonti menzionate, dal punto di vista penalistico, possono avere solo funzione interpretativa. Il Regolamento Europeo, infatti, seppur dotato efficacia diretta nel territorio dello Stato, non può inserire norme penali incriminatrici.[48] D'altra parte, ovviamente, nemmeno una comunicazione della Consob potrebbe definire sul piano formale fattispecie penali, senza violare il principio costituzionale di riserva di legge.

L'art. 185 TUF, seppur non presentandosi con il tipico rinvio caratteristico delle "norme penali in bianco",[49] risulta comunque in parte indeterminato in relazione alla individuazione delle specifiche modalità di realizzazione della condotta tipica. Pertanto, in una fattispecie così tecnica, un'integrazione basata su fonti emesse da autorità di settore

---

d) fanno riferimento a specifiche fattispecie di manipolazione del mercato previste dall'articolo 187-ter del Testo unico; tuttavia, esse possono ricondursi anche ad altre ipotesi ivi previste;
e) sono tradotti dall'inglese ma non intendono modificare quanto espresso dal CESR."

[46] La Comunicazione n. DME/5078692 del 29-11-2005 descrive il fenomeno in questo modo: "*Questo comportamento implica l'inserimento di ordini, specie nei mercati telematici, a prezzi più alti (bassi) di quelli delle proposte presenti dal lato degli acquisti (vendite). L'intenzione sottostante agli ordini non è quella di eseguirli ma di fornire indicazioni fuorvianti dell'esistenza di una domanda (offerta) sullo strumento finanziario a tali prezzi più elevati (bassi). (Una variante di questo comportamento consiste nell'inserimento di un ordine per quantitativi minimi in modo da muovere il prezzo delle migliori proposte in acquisto o in vendita sullo strumento finanziario con l'intenzione di non eseguirlo, ma rimanendo eventualmente disponibili all'esecuzione qualora non si riesca a ritirarlo in tempo.)"*

[47] Si rinvia al paragrafo 2.2.1 per un'analisi più dettagliata del fenomeno di *spoofing*.

[48] R. ADAM, A. TIZZANO, *Manuale di diritto dell'Unione Europea*, Giappichelli, Torino, 2017, p. 411 ss., G. MARINUCCI, E. DOLCINI, G. L. GATTA, *Manuale di Diritto Penale parte generale*, Giuffrè, Milano, 2022, p.52 ss.

[49] C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale*, *cit*., p.101.

risulta particolarmente utile. La regolamentazione fornita dall'agenzia, seppur sul piano amministrativo, fornisce una sicura base interpretativa anche a livello penale. La stessa Corte Costituzionale ha riconosciuto l'importante ruolo della "*mediazione interpretativa*" assicurata dalle agenzie preposte alla regolamentazione di determinati settori proprio in relazione alla loro particolare qualificazione nella definizione di aspetti tecnici.[50]

4.1.7 Il requisito della "*price sensitivity*"

Le condotte tipizzate dall'art 185 TUF non richiedono la verificazione di un evento lesivo, ma devono risultare "*concretamente idonee a provocare una sensibile alterazione dei prezzi degli strumenti finanziari*". Si tratta del cosiddetto requisito della "*price sensitivity"*.

Tale caratteristica induce l'interprete a qualificare la fattispecie come reato di pericolo, proprio perché non è necessario che si verifichi effettivamente un danno, inteso come "sensibile alterazione dei prezzi", ma è sufficiente che le condotte siano idonee a cagionarlo.[51]

In virtù dell'avverbio "*concretamente*", la norma sembra riconducibile alla categoria dei "reati di pericolo concreto".

Occorre quindi premettere una breve distinzione tra le nozioni di reato di pericolo concreto e astratto. Nei reati di pericolo concreto, infatti, il pericolo stesso è un elemento costitutivo della fattispecie che il giudice dovrà, quindi, accertare volta per volta. Con "pericolo si intende, in questo senso, la probabilità o la rilevante possibilità che l'evento dannoso si realizzi.[52] L'accertamento dovrà essere effettuato con un criterio di prognosi postuma: il giudice deve porsi al momento realizzazione del reato e chiedersi se allora apparisse probabile la verificazione dell'evento, tenendo conto di tutte le circostanze

[50] Si allude alla celeberrima sentenza della Corte Costituzionale n. 364/1988 che, seppur in relazione ad aspetti differenti da quelli in esame, in un inciso afferma: "*La completa, in tutte le sue forme, sicura interpretazione delle leggi penali ha, oggi, spesso bisogno di seconde, ulteriori mediazioni: quelle ad es. di tecnici, quanto più possibile qualificati, di organi dello Stato (soprattutto di quelli istituzionalmente destinati ad applicare le sanzioni per le violazioni delle norme, ecc.). Specifici, particolari doveri, nei destinatari delle leggi penali (di richiesta e controllo delle informazioni ricevute, ecc.) discendono da un sistema di norme "strumentali", la violazione delle quali già denota quanto meno una "trascuratezza" nei confronti dei diritti altrui, delle persone umane e, conclusivamente, dell'ordinamento tutto."*

[51] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia, cit.*, p. 386.

[52] C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale, cit.*, p. 296.

concrete e utilizzando come metro di giudizio leggi scientifiche di copertura e massime di esperienza.[53]

Nei reati di pericolo astratto, invece, il pericolo costituisce semplicemente la *ratio* della norma: il legislatore, sulla base di una valutazione astratta, ritiene necessario vietare una determinata condotta poiché potrebbe mettere in pericolo un bene giuridico meritevole di tutela. In questo caso il giudice dovrà limitarsi ad accertare che il fatto concreto sia conforme alla fattispecie astratta.[54] In questa tipologia di reati vi è una maggior distanza logico-temporale tra la condotta tipica e il danno rispetto a quella presente nei reati di pericolo in concreto.[55]

Come precedentemente affermato, gli interpreti evidenziano la natura di "reato di pericolo in concreto" dell'art. 185 TUF. In realtà, la fattispecie presenta alcune caratteristiche di astrattezza.

Un primo aspetto riguarda il rapporto tra l'evento e l'offesa del bene protetto. L'evento di alterazione dei prezzi, infatti, può definirsi giuridicamente "neutro" a meno che non venga preceduto da una condotta artificiosa e non comporti un'inefficiente collocazione dell'investimento mobiliare. In questo senso, il legislatore sembra anticipare ulteriormente la soglia di tutela, poiché, identificando l'offesa tipica nell'alterazione dei prezzi degli strumenti finanziari, presume che qualsiasi alterazione comporti necessariamente una cattiva allocazione dell'investimento.[56]

In secondo luogo, l'elemento dell'alterazione dei prezzi nella struttura della norma è solo indicativo ed anticipatore di un probabile pregiudizio; pertanto, si può affermare che il pericolo non rappresenta una conseguenza diretta e immediata della condotta.[57]

Un terzo aspetto riguarda l'elemento causale, in questo contesto definibile più precisamente come "causalità potenziale della condotta".[58]

---

[53] Si ritiene che, poiché il pericolo costituisce un elemento della fattispecie oggettiva, il giudizio debba essere "a base totale" e quindi debba prendere in considerazione tutte le circostanze concretamente presenti al momento del giudizio. Al contrario si procederà con un giudizio "a base parziale", prendendo quindi conto delle condizioni di fatto conoscibili dall'agente al momento della condotta, per quanto riguarda l'accertamento relativo all'elemento soggettivo. C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale, cit.*, p. 297

[54] *Ibidem*.

[55] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare,* Giuffrè Ed., Milano, 2010, p. 264.

[56] *Ibidem*.

[57] *Ibidem*.

[58] *Ibidem*.

Da questo punto di vista, appare opportuno prendere come spunto di riflessione una celebre sentenza del Tribunale di Torino del 2011, relativa al caso *Ifil*.[59] Tale pronuncia, utilizzando un percorso logico innovativo in relazione all'accertamento del pericolo nei reati di questo tipo, pone l'accento su un problema di incompatibilità del criterio di prognosi postuma con il giudizio sull'idoneità concreta all'alterazione dei prezzi. [60]

Il Tribunale, infatti, qualifica il reato di manipolazione del mercato come reato di pericolo in concreto in cui, però, il pericolo deve essere concepito quale evento; è pertanto necessario un accertamento in concreto, cronologicamente successivo rispetto a quello della condotta. Nella pronuncia, quindi, viene escluso un semplice giudizio di pericolosità *ex ante*, ma viene ritenuto necessario l'accertamento (*ex post*) dell'avvenuta lesione del bene giuridico, ovviamente nella dimensione del pericolo.[61] La soluzione prospettata consiste nell'attenta analisi della reazione del mercato alla condotta manipolativa. Se effettivamente si constatasse l'avvenuta alterazione dei prezzi degli strumenti finanziari, il pericolo sarebbe ovviamente dimostrato e sarebbe altresì dimostrata una piena e materiale lesione dell'interesse giuridico tutelato.

Se invece tale alterazione non si fosse verificata, sarebbero prospettabili due ipotesi. Se la mancata alterazione è dipesa da «*fattori esterni e indipendenti (..) che, intervenuti autonomamente, hanno vanificato gli effetti della condotta manipolativa*»,[62] si può sostenere sia stato comunque realizzato un pericolo concreto. Se, invece, l'alterazione dei prezzi non si è verificata pur in mancanza di qualsiasi altro elemento che possa aver annullato l'effetto della condotta sul mercato, significa che tale condotta non ha prodotto, non solo il danno, ma nemmeno il pericolo concreto; in questo caso, secondo la sentenza citata, occorre negare la sussistenza del reato.

Tale impostazione, tuttavia, è rimasta isolata anche a causa dell'intervento della Corte di Cassazione che ha annullato, con rinvio, la sentenza. La Corte, seguendo l'impostazione tradizionale, ha infatti qualificato la fattispecie pervista dall'art 185 TUF come reato di mera condotta, ritenendo ingiustificata, alla luce del dettato normativo, «*l'introduzione per mano*

---

[59] Trib. Torino, sez. I pen., 18 marzo 2011, pres. ed est. Casalbore, imp. Gabetti e a. (manipolazione del mercato), disponibile su https://archiviodpc.dirittopenaleuomo.org/d/640-tribunale-di-torino-sez-i-pen-21122010-dep-18032011-pres-ed-est-casalbore-imp-gabetti-e-a-manipolaz. Si tratta di un caso di manipolazione di mercato di tipo informativo che coinvolse la società Fiat.

[60] F. CONSULICH, *Manipolazione del mercato e disorientamenti dogmatici: tra eventi di pericolo e pericolo di eventi*, in Le Società 7/2011, p. 823 ss.

[61] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia, cit.*, p. 387

[62] Trib.Torino, *cit.*

dell'interprete di un ulteriore elemento costitutivo quale l'evento naturalistico», ribadendo ai fini dell'accertamento del requisito di *price sensitivity*, il criterio della prognosi postuma.[63]

Nonostante le numerose critiche giurisprudenziali e dottrinali, la pronuncia del Tribunale di Torino appare comunque degna di nota poiché, nello sforzo di concretizzare il giudizio di pericolo, rende manifesta la difficoltà di accertare il pericolo concreto nelle complesse dinamiche che caratterizzano i mercati finanziari.

Il giudizio di pericolo, infatti, oltre a richiedere conoscenza totale delle circostanze concrete che accompagnano la condotta, impone l'utilizzo, come metro di valutazione del pericolo, di leggi scientifiche e di massime di esperienza.

In un contesto complesso come quello dei mercati finanziari, influenzato da molteplici fattori anche imprevedibili, mancano delle leggi economiche che assicurino un sufficiente grado di certezza. Inoltre, le variabili che sarebbe necessario conoscere per verificare se una determinata condotta sia idonea ad alterare sensibilmente i prezzi di strumenti finanziari, sono così numerose che è pressoché impossibile averne anche solo la piena contezza.[64]

Per questi motivi, la scienza economica, per accertare empiricamente se una manipolazione del mercato si sia realizzata, non effettua una prognosi, ma una diagnosi, partendo dall'analisi dell'andamento concreto delle quotazioni nel mercato di riferimento.[65] Tali difficoltà vengono poste in luce dalla sentenza del Tribunale di Torino, anche se con un ragionamento basato su presupposti giuridici non condivisi né dalla Corte di Cassazione né dalla dottrina.

Tenendo conto delle diverse considerazioni svolte in relazione all'art 185 TUF, si rileva che molti autori, dovendo necessariamente escludere la qualificazione della fattispecie quale reato di pericolo puramente astratto in virtù dell'esplicito riferimento normativo alla concretezza, hanno qualificato il reato come di pericolo solo *tendenzialmente concreto*, ossia di pericolo generico.[66]

---

[63] Cass., sez. V, 20 giugno 2012, n. 40393 disponibile presso italigiure.giustizia.it

[64] F. CONSULICH, *Manipolazione del mercato e disorientamenti dogmatici: tra eventi di pericolo e pericolo di eventi, cit.*

[65] *Ibidem*.

[66] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare, cit*., p. 269; sullo stesso tema si veda anche S. SEMINARA, *Diritto penale commerciale*, I, *Il diritto penale del mercato mobiliare*, Torino, 2018, p. 98 il quale afferma «*il requisito della concretezza, se da un lato si presta ad escludere l'integrazione del reato quando sia dimostrabile l'assenza di un pericolo, dall'altro non si spinge fino ad esigere un'impossibile dimostrazione empirica della probabilità dell'alterazione nella situazione data*».

Appare a questo punto opportuna l'analisi delle tecniche concretamente utilizzate dalla giurisprudenza per effettuare il giudizio di pericolo sulla base del criterio della prognosi postuma e quindi per verificare l'idoneità delle condotte manipolative ad alterare concretamente i prezzi di strumenti finanziari.

Un parametro tradizionalmente utilizzato dalla giurisprudenza rinvia alla nozione di "investitore ragionevole".[67] Tale investitore è rappresentato da «*una persona di normale avvedutezza, tuttavia suscettibile di essere tratta in inganno*».[68]

Si tratta di un criterio generalmente utilizzato in relazione alla manipolazione informativa e si concretizza nel chiedersi se l'informazione falsa costituisca o meno un elemento che un investitore ragionevole potrebbe porre a fondamento di una propria decisione di investimento. Nel caso di risposta affermativa si presuppone che il mercato potrebbe reagire a tale informazione e che quindi la condotta risulti concretamente idonea ad alterare sensibilmente i prezzi degli strumenti finanziari.[69] Si potrebbe affermare che il medesimo ragionamento possa essere svolto anche per quanto riguarda la manipolazione operativa, semplicemente sostituendo all'informazione falsa la condotta artificiosa o simulatoria e chiedendosi quindi se le operazioni siano tali da costituire un elemento utilizzabile dall'investitore ragionevole per assumere una decisione di investimento.

Appare necessario evidenziare, tuttavia, che questo parametro risulta inadeguato. La dottrina americana già da quasi un decennio ha sottolineato la crisi del paradigma dell'"investitore ragionevole".[70] Utilizzare come criterio di giudizio la ragionevolezza dell'investitore implica, infatti, usare le informazioni disponibili secondo parametri di efficienza e razionalità economica e la loro automatica incorporazione nel prezzo di mercato degli strumenti finanziari. Già in passato alcuni autori hanno smentito tale assunto ritenendo che il mercato non fosse composto da agenti "razionali" ma da agenti "emotivi".[71] Oggi il parametro dell'investitore ragionevole appare addirittura anacronistico in relazione al fatto che i mercati risultano composti in gran parte non da operatori fisici, ma da operatori algoritmici che basano le loro decisioni esclusivamente su calcoli di tipo probabilistico e

[67] Si tratta di un criterio inizialmente utilizzato in relazione alla fattispecie di *insider trading* o "abuso di informazioni privilegiate" per valutare l'esistenza stessa dell'informazione privilegiata, definita dall' art 7 par.1 lett. a) del MAR anche sulla base del requisito della *price sensitivity* ("*la diffusione dell'informazione potrebbe avere un effetto significativo sui prezzi*")

[68] Cass. Sez. V, 20 luglio 2011, n. 28932, disponibile presso www.dirittobancario.it (sentenza *Parmalat*)

[69] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia*, *cit.*, p. 388.

[70] L. TOM C. W., *Reasonable Investor(s),* in *95 Boston University Law Review*, 2015.

[71] *Ibidem*.

pongono in atto strategie di investimento, che vengono loro insegnate dai programmatori o che apprendono autonomamente dagli altri operatori del mercato.[72]

Sembra quindi necessaria, a questo proposito, una revisione del criterio di accertamento del requisito di *price sensitivity*, poiché appare illogico ragionare in una prospettiva soggettiva, seppur fittizia, in un contesto in cui la maggior parte degli operatori sono in realtà algoritmi. [73]

4.1.8 Il momento consumativo

In relazione all'individuazione del momento consumativo e del *locus comissi delicti* del reato di manipolazione del mercato, ha avuto luogo un acceso dibatto giurisprudenziale e dottrinale, oggi parzialmente risolto.

Quella parte della giurisprudenza che ha considerato la fattispecie quale reato "ad evento di pericolo", ha affermato che il delitto in esame si consuma nel momento e nel luogo in cui si concretizza, quale conseguenza della condotta, la rilevante possibilità di verificazione della sensibile alterazione del prezzo.[74]

Successivamente la giurisprudenza ha cambiato orientamento a seguito della sentenza della Cassazione sul caso "*Parlamat*" (il quale, in realtà, riguardava una manipolazione informativa). La Suprema Corte ha infatti stabilito che «*l'illecito si consuma nel momento stesso in cui la notizia, foriera di compenso valutativo del titolo, viene comunicata o diffusa, e, cioè, esce dalla sfera del soggetto attivo*».[75]

Per quanto riguarda la manipolazione operativa, invece, la giurisprudenza è concorde nell'affermare che il reato si consuma nel luogo in cui il soggetto pone in essere l'artificio connotato dall'attributo della concreta idoneità ad influenzare sensibilmente il prezzo degli strumenti finanziari. Quindi, se si tratta di inserimento di ordini sul mercato, il luogo in cui avviene l'abbinamento automatico delle proposte di negoziazione in acquisto e vendita degli strumenti finanziari, ovvero il luogo ove si trovano i *provider* di Borsa Italiana.[76]

---

[72] Si veda § 2.1.2.

[73] H. ASHTON, *Definition of intent suitable for algorithms*, in *Artificial Intelligence and Law*, 2022.

[74] A. NISCO, *Manipolazione informativa del mercato e luogo di consumazione del reato*, in *Diritto Penale Contemporaneo*, 2014.

[75] Cass. Sez. V, 20 luglio 2011, n. 28932, disponibile presso www.dirittobancario.it (sentenza *Parmalat*)

[76] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia, cit*., p.395.

Alcuni autori, tuttavia, hanno proposto di estendere alla manipolazione di mercato un diverso ragionamento, compiuto dalla Corte di Cassazione nel 2009 in relazione alla fattispecie di *insider trading*.[77] In questa pronuncia la Corte ha negato la competenza territoriale del Tribunale di Milano, rifacendosi alla normativa extra-penale sulla dematerializzazione di strumenti finanziari negoziati sui mercati regolamentati. La consumazione del reato, infatti, non si realizzerebbe nel momento dell'abbinamento automatico degli ordini di segno opposto, ma solo con l'individuazione degli strumenti finanziari venduti, la quale avverrebbe nel luogo e «*nel momento in cui si opera la registrazione dell'operazione e dei titoli sul conto aperto dell'acquirente presso l'intermediario finanziario che ha svolto l'operazione*». Solo in questo momento vi sarebbe un effettivo passaggio di proprietà del titolo; precedentemente si verificherebbe una vendita a efficacia obbligatoria, irrilevante ai fini della consumazione del reato.[78]

L'estensione alla manipolazione del mercato di questo percorso logico è, tuttavia, stata esclusa dalla giurisprudenza successiva. La Corte d'Appello di Milano, ad esempio, ha sostenuto che «*l'annotazione dell'intermediario sul dossier titoli del cliente (…) assume una valenza meramente dichiarativa della conclusione dell'operazione già avvenuta con l'abbinamento, sul circuito telematico, dell'ordine di acquisto con l'ordine di vendita*.»[79]

Quindi si può affermare che, per quanto riguarda il reato di manipolazione del mercato di tipo operativo, l'orientamento giurisprudenziale prevalente al momento prevede la competenza del giudice del luogo dove sono collocati i *provider* della piattaforma di negoziazione. In concreto è quindi il Tribunale di Milano il giudice che, nella maggior parte dei casi, viene ritenuto competente, poiché i *provider* di Borsa Italiana hanno sede a Milano.

---

[77] L'art. 184 TUF (180 TUF all'epoca della sentenza, nella previgente formulazione) prevede una fattispecie di abuso di mercato denominata "*Abuso di informazioni privilegiate*". Tra le varie condotte previste, tale norma punisce chi "*essendo in possesso di informazioni privilegiate in ragione della partecipazione al capitale di una società, ovvero dell'esercizio di una funzione, anche pubblica, di una professione o di un ufficio, acquista, vende o compie altre operazioni, anche per interposta persona, su strumenti finanziari avvalendosi delle informazioni medesime;"*

[78] Cass. Sez. V, 23 febbraio 2009, n. 200 citata da F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare, cit.*, p. 341.

[79] App. Milano, sez. II pen., 12-22 marzo 2012, n. 1602 (caso SS Lazio s.p.a.), citata da F. SGUBBI, D. FONDAROLI, A.F. TRIPODI, *Diritto Penale del Mercato Finanziario*, *cit*., p.105.

4.1.9 Il dolo

Il reato di manipolazione del mercato, in quanto delitto, è punibile a titolo di dolo. Tuttavia, a differenza dell'art 501 c.p. che prevede il dolo specifico **"***di turbare il mercato interno dei valori o delle merci"*, il reato previsto dall'art. 185 TUF prevede il dolo generico.[80]

L'autore del reato deve quindi avere la coscienza e la volontà di diffondere notizie false o di porre in essere operazioni simulate o altri artifici e la consapevolezza della loro idoneità a determinare una sensibile alterazione del prezzo degli strumenti finanziari.[81]

Parte della dottrina ha manifestato alcune perplessità in relazione alla mancanza di una specifica finalità lesiva della condotta, evidenziando il rischio che, con l'utilizzo del dolo eventuale, si pervenga a sanzionare comportamenti più propriamente colposi.[82] Pertanto tali autori ritengono che il giudice dovrà accertare con particolare rigore l'elemento soggettivo, così da evitare inammissibili dilatazioni di responsabilità.[83]

La giurisprudenza sembra invece ammettere pacificamente l'imputabilità del reato di manipolazione del mercato anche a titolo di dolo eventuale. Il Tribunale di Milano, in una sentenza del 2002, ha ad esempio affermato che «*la struttura del reato in esame risulta costruita a titolo di dolo generico ed ammette pertanto la configurabilità del reato anche a titolo di dolo eventuale*»[84]

Appare opportuno ricordare che la contravvenzione prevista dal comma 2-*bis* dell'art. 185 TUF, ormai abrogata nel 2021, era invece punibile anche a titolo di colpa.[85]

---

[80] A. GALANTI, *La manipolazione del mercato, cit.*, p.105.
[81] *Ibidem.*
[82] S. SEMINARA, *Diritto penale commerciale*, I, *Il diritto penale del mercato mobiliare*, Torino, 2018, p. 102.
[83] *Ibidem*.
[84] Trib. Milano, 11 novembre 2002, in *Riv. trim. dir. pen, econ*., 2003, p.747. In altre sentenze lo stesso Tribunale di Milano si è dimostrato più restio a riconoscere il dolo eventuale, ritenendo necessario un accertamento più approfondito. Ad esempio, in una pronuncia del 2005 (Trib. Milano, 14 novembre 2005) il coimputato viene assolto perché non si ritiene provata la consapevolezza che l'operazione si inscrivesse in un più ampia strategia tesa a creare una alterazione del mercato. Infatti, la condanna dell'imputato ordinante l'operazione si fonda sulla dimostrazione che le singole operazioni disposte convergessero nell'indurre, fuori di qualunque motivazione economica, il mercato tutto a credere ad un *trend* rialzista. Sul tema F. GUARINELLO, *Gli abusi di mercato. La manipolazione di mercato: fattispecie penale e amministrativa*., in *Diritto bancario Tidona*, 2006, disponibile al seguente link https://www.tidona.com/gli-abusi-di-mercato-la-manipolazione-di-mercato-fattispecie-penale-ed-amministrativa/
[85] A. GALANTI, *La manipolazione del mercato, cit.*, p.106.

4.1.10 Le prassi di mercato ammesse

Il già menzionato d.lgs. 107/2018 ha introdotto il comma 1-*bis* dell'art 185 TUF che prevede la non punibilità di 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."*[86]

L'art 13 del MAR stabilisce quindi le condizioni e le procedure con le quali le autorità competenti di ogni stato membro possono, di concerto con l'ESMA, stabilire prassi di mercato ammesse.

La *ratio* di questo istituto è quella di mandare esenti da sanzione coloro che compiono operazioni speculative normalmente accettate, che condividono tuttavia tratti delle condotte manipolative.[87] Ad esempio, i *cross orders* sono ordini di segno opposto provenienti dallo stesso operatore e sono leciti purché effettuati nel rispetto delle regole del mercato, ma possono facilmente dar luogo alla pratica manipolativa degli *improper matched orders*.[88]

L'altro elemento previsto dalla norma al fine di escludere la configurabilità dell'illecito è di natura soggettiva e fa riferimento alla legittimità dei motivi in forza dei quali vengono effettuati i comportamenti conformi alle prassi di mercato. Come è evidente dalla dizione letterale della norma, al fine di escludere la responsabilità, occorre l'accertamento di entrambi i profili.[89]

In merito alla natura giuridica di tale clausola di esenzione della responsabilità, sono state suggerite diverse teorie.

L'ipotesi di qualificare la norma come mera causa di non punibilità appare in realtà da escludere poiché la legittimità dei motivi, insieme alla conformità della condotta a prassi di mercato ammesse, sembra far venire meno la stessa *ratio* della norma sanzionatoria, rendendo la condotta non meritevole di sanzione in quanto espressione di un comportamento pienamente legittimo.[90]

Parte della dottrina ha invece sostenuto che si potrebbe trattare di una causa di esclusione del fatto, ossia un elemento negativo della fattispecie, incidente sulla tipicità del

---

[86] Precedentemente le prassi di mercato ammesse erano espressamente previste solo in relazione all'illecito amministrativo (187-*ter*). A. GALANTI, *La manipolazione del mercato, cit.*, p.32.
[87] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia, cit.*, p. 390.
[88] Si veda nota numero 25.
[89] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia, cit.* p. 392.
[90] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare, cit.*, p. 226.

fatto.[91] Vi è infatti una fattispecie principale che delinea il fatto tipico e una fattispecie secondaria che individua alcune condotte escludendole dall'area di applicazione di quella principale.[92] Va tuttavia ricordato che una delle caratteristiche di una causa di esclusione della tipicità del fatto consiste nella sua estraneità all'oggetto di rappresentazione dell'agente. In questo caso invece è presente un elemento soggettivo poiché la condotta compiuta deve essere sorretta da motivi legittimi. Inoltre, la causa di esclusione della tipicità sottrae una specifica categoria di condotte dall'operatività della norma incriminatrice, ma non integra una fattispecie permissiva.[93]

Alcuni autori hanno quindi suggerito che quella in esame sarebbe una causa di giustificazione di origine "*prasseologico-consuetudinaria*". Infatti, è necessario che le prassi di mercato vengano identificate attraverso un riconoscimento formale da parte dell'autorità di settore. In questa prospettiva, i motivi legittimi previsti dal citato comma 1-*bis* costituirebbero l'elemento soggettivo della causa di giustificazione e potrebbero essere identificati in qualsiasi motivazione giuridica incompatibile con la finalità di manipolazione del mercato.[94]

4.1.11 Il trattamento sanzionatorio

Per quanto riguarda il trattamento sanzionatorio, la previsione della reclusione da uno a sei anni prevista dal primo comma dell'art.185 TUF è stata raddoppiata dall'art 39 comma 1 della l. n 262/2005 a tutela del risparmio. La sanzione pecuniaria, invece, già ampiamente fuori dai limiti codicistici, non pare suscettibile di raddoppio.[95]

Il secondo comma dell'art 185 TUF contiene una circostanza aggravante che prevede la possibilità del giudice di aumentare la multa fino al triplo o fino al maggior importo di dieci volte il prodotto o il profitto del reato "*quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo."*

---

[91] F. D'ALESSANDRO, *Tutela dei mercati finanziari e rispetto dei diritti umani fondamentali*, in *Dir. pen. e proc*., 2014.
[92] *Ibidem*.
[93] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare*, *cit*., p. 226.
[94] *Ibidem*.
[95] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia, cit.* p. 387

La condanna per il delitto di manipolazione del mercato prevede poi l'applicabilità delle pene accessorie elencate dall'art 186 TUF[96] per una durata non inferiore a sei mesi e non superiore a due anni, nonché la pubblicazione della sentenza su almeno due quotidiani, di cui uno economico, a diffusione nazionale.

L'art 187 TUF inoltre prevede, per quanto riguarda i delitti di manipolazione del mercato e di *insider trading*,[97] un'ipotesi di confisca speciale, obbligatoria, che ha per oggetto i beni che costituiscono il profitto conseguito dal reato. Tale confisca può avvenire anche per equivalente.

Occorre ricordare inoltre che i due reati di "abuso di mercato" sono inseriti tra le fattispecie che danno luogo alla responsabilità amministrativa dell'ente, prevista dal d.lgs 231/2001. L'art 25 del d.lgs. riguarda espressamente la manipolazione del mercato e prevede inoltre che, se la commissione del reato ha procurato un prodotto e un profitto di rilevante entità, la sanzione venga aumentata fino a dieci volte tale prodotto o profitto.

4.1.12 La fattispecie amministrativa, l'articolo 187-*ter*

A conclusione dell'analisi fornita del reato di manipolazione di mercato, appare opportuno trattare in breve anche la fattispecie sanzionata sul piano amministrativo.

L'art 187-*ter* effettua un rinvio espresso al MAR per quanto riguarda la definizione delle condotte sanzionate affermando che "*salvo le sanzioni penali quando il fatto costituisce reato, è punito con la sanzione amministrativa pecuniaria da ventimila euro a cinque milioni di euro chiunque viola il divieto di manipolazione del mercato di cui all'articolo 15 del regolamento (UE) n. 596/2014."*

La fattispecie amministrativa, pertanto, presenta caratteristiche differenti rispetto a quella penale, in particolar modo dal punto di vista dell'elemento soggettivo: l'art 12 del MAR, a cui fa riferimento l'art. 15 del MAR per la definizione della manipolazione, descrive

[96] L'interdizione dai pubblici uffici, l'interdizione da una professione o un'arte, l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese e l'incapacità temporanea di contrattare con la pubblica amministrazione.
[97] Art. 184 TUF.

condotte anche colpose.[98] Sembra quindi che le sanzioni previste dall'art 187-*ter* del TUF possano essere applicate anche nel caso di una condotta colposa. [99]

L'esistenza di un doppio binario sanzionatorio per gli abusi di mercato, che si concretizza nella compresenza di sanzioni amministrative e di quelle penali per il medesimo fatto storico, ha creato alcuni problemi in relazione alla violazione del principio del *ne bis in idem*.[100] In particolare, la questione è stata risolta con una parabola giurisprudenziale della Corte EDU che, dopo aver affermato un principio "processuale" e "forte" del *ne bis in idem*,[101] ha invece optato per un principio "sostanziale" e "debole" dello stesso. Nella sentenza *A e B c. Norvegia* del 2016, la Corte ha infatti affermato che non sussiste una violazione del principio del *ne bis in idem* quando sussista un nesso temporale e sostanziale tra i due procedimenti ("*sufficiently close connection in substance and time"*) e nel caso in cui il cumulo sanzionatorio derivante dalla convergenza procedimentale risulti complessivamente proporzionato rispetto al disvalore del fatto. Sarebbe così ammissibile, in linea generale, la duplicazione di procedimenti per uno stesso fatto, a condizione che il trattamento sanzionatorio complessivo risulti adeguato.

Sulla base di queste considerazioni anche la Corte di Giustizia dell'Unione Europea si è pronunciata sulla questione, individuando un proprio test di proporzionalità sanzionatoria. Infatti, il giudice nazionale che, trovandosi dinnanzi ad un doppio binario sanzionatorio,

---

[98] Art 12 MAR definisce come condotta manipolativa qualsiasi attività che "*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 prodotto oggetto d'asta sulla base di quote di emissioni; 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;"

[99] F. GUARINELLO, *Gli abusi di mercato. La manipolazione di mercato: fattispecie penale e amministrativa*., in *Diritto bancario Tidona*, 2006, disponibile al seguente link https://www.tidona.com/gli-abusi-di-mercato-la-manipolazione-di-mercato-fattispecie-penale-ed-amministrativa/

A. GALANTI, *La manipolazione del mercato, cit.,* p.106.

[100] Il medesimo problema si presenta anche in altri settori dell'ordinamento oltre a quello dei *market abuses*, come ad esempio in tema di reati tributari che si intersecano e cumulano con le corrispettive sanzioni amministrative. A. CONTRINO, E. DELLA VALLE, A. MARCHESELLI, E. MARELLO, G. MARINI, S.M. MESSINA, M. TRIVELLIN, *Fondamenti di diritto tributario*, Wolters Kluwer, Milano, 2020, p.509.

[101] Nella sentenza *Grande Stevens e altri c. Italia* del 2014, proprio in relazione ad una fattispecie di manipolazione di mercato, la Corte EDU ha affermato che le ingenti sanzioni amministrative previste per le fattispecie di abuso di mercato avessero uno scopo eminentemente repressivo e afflittivo e rappresentassero un istituto sostanzialmente penale. Pertanto, il fatto che i ricorrenti, già condannati in via definitiva nel procedimento amministrativo, fossero successivamente sottoposti a nuovo giudizio penale, avrebbe comportato una violazione del principio del *ne bis in idem*, inteso nel senso di vietare due processi per il medesimo fatto storico. Si veda N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia*, *cit*., p.341.

intervenga nel secondo procedimento, deve valutare se il cumulo di sanzioni che deriva dai due procedimenti sia proporzionato o meno. Nel caso sia proporzionato, allora il principio del *ne bis in idem* si intende rispettato. Se invece il carico sanzionatorio risulta eccessivo rispetto al disvalore del fatto, il giudice nazionale deve disapplicare le disposizioni che definiscono trattamento sanzionatorio poiché contrastanti con l'art 50 della Carta di Nizza. La disapplicazione sarà totale nel caso in cui la sanzione amministrativa ricopra intero disvalore del fatto, altrimenti il giudice disapplicherà solo parzialmente tali disposizioni, modulando la sanzione alla luce delle misure già applicate nel primo procedimento.[102]

Il legislatore italiano si è quindi conformato alla giurisprudenza della Corte di Giustizia modificando (con il d.lgs. n.107/2018) il meccanismo compensativo delle sanzioni previsto dall'articolo 187-*terdecies* e recependo il principio esposto.[103]

4.2 L'applicabilità della norma italiana alla fattispecie realizzata attraverso sistemi di HFT: i possibili punti critici

Sono già state discusse le ripercussioni penalistiche più rilevanti attinenti ai problemi di trasparenza precedentemente evidenziati derivanti dal modello *black-box*.[104] L'obbiettivo dei seguenti paragrafi sarà quello di analizzare tali aspetti calati nell'ordinamento italiano, prendendo in considerazione specificatamente il reato di manipolazione del mercato (185 TUF) e i sistemi di imputazione propri del diritto penale.

Nei casi in cui un sistema di HFT compia operazioni di *spoofing* o altre strategie particolarmente aggressive, ci si chiede, quindi, se le persone fisiche che utilizzano la macchina o che hanno contribuito alla sua programmazione possano essere ritenute responsabili del reato di manipolazione del mercato, oppure se non si corra il rischio di creare un pericoloso vuoto di tutela penalistica.

[102] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia*, *cit.* p. 397.
[103] *Ibidem*.
[104] Si veda §2.2.1 e §3.3

4.2.1 Il soggetto attivo

Dal punto di vista dell'autore del reato, si potrebbe in prima approssimazione affermare che a compiere effettivamente le condotte penalmente rilevanti sia il sistema di IA impiegato nell'HFT. In realtà, come precedentemente evidenziato,[105] seppur alcuni studiosi abbiano tentato di ipotizzare un sistema di imputazione penale diretto dei sistemi di intelligenza artificiale più avanzati,[106] almeno per il momento, la dottrina prevalente ritiene che nessun ordinamento penalistico possa essere in grado di sostenere l'imputazione dell'algoritmo in quanto tale.[107]

Nei casi di condotta manipolativa realizzata dalla macchina, alla luce degli attuali meccanismi di imputazione del diritto italiano si potrebbero prendere in considerazione sostanzialmente due soggetti: l'utilizzatore del sistema di IA e il *designer*, inteso come il soggetto programmatore-produttore.

L'utilizzatore è il soggetto che si serve dell'algoritmo per compiere l'attività di *high frequency trading*. Si tratta generalmente di grandi società, pertanto la macchina viene materialmente utilizzata da diversi dipendenti nell'ambito di compiti e mansioni ripartite all'interno della struttura aziendale. In questi casi si pone l'ordinario problema penalistico del frazionamento della responsabilità per reati compiuti nell'ambito di organizzazioni complesse.[108]

Anche per il soggetto produttore-programmatore sorge il medesimo problema relativo alla responsabilità penale del singolo nell'ambito di grandi enti; in questo caso tale aspetto può risultare persino accentuato dal fatto che il *software* venga progettato e realizzato in varie fasi, per segmenti, da soggetti diversi e talvolta anche da società differenti.[109]

Tali tematiche, tuttavia, sono state ampiamente affrontate e risolte dalla giurisprudenza in relazione a diverse tipologie di reati.[110] Si può ritenere quindi che la frammentazione della responsabilità penalistica e le problematiche connesse, costituiscano semplicemente un fattore aggiuntivo di complessità delle indagini eventualmente rilevanti a livello di

---

[105] Si veda §2.2.1 sec *a*

[106] G. HALLEVY, *Liability for Crimes Involving Artificial Intelligence Systems*, Berlino, 2015, 47 ss.

[107] A. CAPPELLINI, *Machina delinquere non potest,* in www.discrimen.it, 2019; R. BORSARI, *Intelligenza artificiale e responsabilità penale: le prime considerazioni,* in *Media Laws*, 2019; C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato,* in *Riv. it. dir. proc. pen*, vol.63, N°4, 2020.

[108] I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale,* in *Riv. it. dir. proc. pen*, fasc.1, marzo 2021, p.83.

[109] *Ibidem.*

[110] Ci si riferisce alla complessa materia dei reati caratterizzati dalla violazione di norme antinfortunistiche, ai reati ambientali e ai reati societari e fallimentari.

accertamento, ma che non influenzano gli aspetti sui quali si focalizza il presente lavoro. Pertanto, nei seguenti paragrafi ci si riferirà all'utilizzatore e al *designer* come ad agenti monosoggettivi, ponendo in essere una semplificazione indispensabile al fine di concentrarsi sulle complesse problematiche penalistiche che sorgono in relazione alla fattispecie in esame.

4.2.2 La condotta

Nell'impossibilità di attribuire una responsabilità penalistica direttamente ai sistemi di IA, occorre ragionare su un modello di imputazione incentrato sulla persona fisica.

È infatti l'utilizzatore del sistema di *trading* ad alta frequenza, identificabile come colui che aziona la macchina, a realizzare, anche se indirettamente, la condotta tipica.[111] In questa prospettiva, il sistema di IA potrebbe essere considerato come un mero strumento, seppur complesso, nelle mani della persona fisica che, rendendo operativo il sistema di HFT nella giornata di contrattazione, si serve della macchina per realizzare le condotte manipolative.[112] Si ritiene pertanto che sia l'utilizzatore della macchina a realizzare, seppur in via mediata, le operazioni manipolative che teoricamente sono poste in essere dal sistema di IA.

Come già visto al paragrafo 2.2.1, i sistemi di HFT talvolta mettono in atto strategie che possono avere importanti effetti distorsivi sul mercato e definibili come manipolative.[113] Occorre quindi capire se le operazioni effettuate dal sistema di IA possano rientrare nell'area di tipicità della norma italiana e quindi siano riconducibili alla definizione di "operazioni simulate" o agli "altri artifici" previsti dall'art. 185 TUF.

Si ricorda brevemente il funzionamento di alcune strategie operative dei sistemi di HFT che, più di altre, possono essere considerate abusive. Ad esempio, vi è un gruppo di tecniche (*Pinging*, *Spoofing*, *Smoking* e *Layering*) caratterizzato dalla medesima base di funzionamento. Attraverso l'immissione e la cancellazione ripetuta di *limit orders*,[114] l'HFT riesce a creare artificiosamente condizioni di mercato a lui favorevoli e a sfruttare la propria

[111] Si tratta ovviamente di una semplificazione in relazione a tutte le problematiche penalistiche che possono sorgere quando, come spesso avviene, colui che aziona la macchina non ne sia proprietario ma sia un dipendente ed esegua semplicemente direttive che provengono da un datore di lavoro.
[112] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato, cit*.
[113] Ci si riferisce in particolare alle strategie di *pinging, layering, spoofing* e *quote stuffing.*
[114] Ordini di acquistare o vendere ad un determinato prezzo "limite" o ad un prezzo più vantaggioso. Si veda §2.2.1

superiorità tecnologica per trarre profitti, a discapito degli altri partecipanti del mercato che vengono tratti in inganno da situazioni non rispondenti alla realtà.[115]

Ci potrebbe domandare se tale immissione e successiva cancellazione di ordini finalizzata alla creazione di una situazione di mercato fittizia possa essere considerata *"concretamente idonea a provocare una sensibile alterazione del prezzo di strumenti finanziari"*.[116]

A questo proposito, si ricordano le problematiche di accertamento precedentemente evidenziate in relazione a tale aspetto.[117] Nella difficoltà di provare la caratteristica dell'idoneità delle condotte a creare una sensibile alterazione di prezzi di strumenti finanziari attraverso una prognosi postuma, parte della dottrina e della giurisprudenza ha ritenuto che, nel momento in cui si riscontra che sia avvenuta l'effettiva alterazione dei prezzi, l'accertamento sull'idoneità sia quantomeno semplificato.[118]

Le strategie di *trading* di sistemi di IA comportano l'immissione e la cancellazione di ordini realizzata ad una velocità molto elevata; tale caratteristica talvolta comporta una quasi immediata reazione dei prezzi degli strumenti finanziari.[119] Viene quindi realizzato l'evento che, nella struttura della norma, costituisce il pericolo e la cui verificazione non è necessaria ai fini della consumazione del reato.[120] Tuttavia, questo aspetto potrebbe facilitare l'accertamento.

Si anticipa che tale accertamento potrebbe comunque comportare alcune problematiche in relazione ad una differente tematica. Anche nel caso di verificazione dell'evento dell'alterazione, infatti, potrebbe risultare molto complicato, se non impossibile ricostruire precisamente il decorso causale che ha portato all'alterazione del prezzo di uno strumento finanziario e verificare che proprio quelle operazioni abbiano provocato

---

115 Sul punto il sito www.investopedia.com al seguente link: http://www.investopedia.com/terms/l/limitorder.asp

116 Per quanto riguarda il compimento di operazioni simulate, queste vengono utilizzate per altre strategie manipolative (si veda §4.1.4), che però non sono particolarmente diffuse nel panorama della contrattazione ad alta frequenza.

117 Si veda §4.1.7.

118 Trib. Torino, sez. I pen., 18 marzo 2011, pres. ed est. Casalbore, imp. Gabetti e a. (manipolazione del mercato), disponibile presso https://archiviodpc.dirittopenaleuomo.org/d/640-tribunale-di-torino-sez-i-pen-21122010-dep-18032011-pres-ed-est-casalbore-imp-gabetti-e-a-manipolaz.
F. CONSULICH, *Manipolazione del mercato e disorientamenti dogmatici: tra eventi di pericolo e pericolo di eventi*, *cit*.

119 A. PUORRO, *High Frequency Trading: una panoramica,* in *Questioni di Economia e Finanza (Occasional Papers)*, CONSOB, 2013.

120 F. SGUBBI, D. FONDAROLI, A.F. TRIPODI, *Diritto Penale del Mercato Finanziario*, *cit*., p. 95.

l'aumento o la diminuzione del valore del titolo. Tale problematica è inoltre amplificata dall'alta concentrazione di operatori algoritmici sul mercato.[121]

Un ulteriore elemento della norma incriminatrice consiste nel fatto che l'alterazione debba essere *sensibile*. Le strategie utilizzate dai *traders* ad alta frequenza in generale sfruttano anche minime variazioni di prezzo di strumenti finanziari. Il profitto per la singola operazione spesso è minimo ma, tenuto conto della velocità e della mole di operazioni, tali tecniche diventano alquanto proficue.[122]

Anche le strategie più aggressive, come lo *spoofing*, spesso provocano solo una leggera reazione del prezzo dello strumento finanziario.

Alterazione dei valori dei titoli per effetto di operazioni di HFT hanno luogo anche in relazione ad episodi di *flash crash*. In questi casi l'impatto sul prezzo degli strumenti finanziari può essere molto significativo. Tuttavia, nonostante non sia ancora chiaro quale possa essere la precisa genesi eziologica di tali fenomeni, le varie teorie economiche concordano sul fatto che non siano provocati da un singolo blocco di operazioni, ma derivino dall'interazione reciproca tra i partecipanti al mercato.[123] Pertanto appare eccessivo richiedere che la potenziale alterazione del valore dei titoli derivante dalle condotte manipolative debba essere di dimensioni tali da essere qualificata come un *flash crash*.

Tornando invece alle strategie che si basano sull'immissione e cancellazione di ordini (come lo *spoofing*), ci si può chiedere se, in questi casi, l'alterazione del prezzo degli strumenti finanziari, seppur minima, sia tale da poter essere definita sensibile, ai sensi dell'art 185 TUF.

La sensibilità è sicuramente un elemento normativo caratterizzato da una certa indeterminatezza, essendo complesso individuare specifici parametri di valutazione.

Tale aspetto deve essere valutato rispetto all'andamento del titolo nel tempo e quindi alle normali fluttuazioni di prezzo degli strumenti finanziari, le quali generalmente sono determinate da una pluralità di fattori, anche "esterni", difficilmente isolabili gli uni dagli altri.[124] Il criterio della sensibilità introduce quindi una componente di tipo quantitativo all'interno del pericolo concreto della norma. Interviene su fatti già autonomamente

[121] Tale aspetto verrà analizzato più approfonditamente nel paragrafo successivo (§4.2.3)
[122] A. PUORRO, *High Frequency Trading: una panoramica, cit.*
[123] *Ibidem.* In relazione agli episodi di *flash crash* si vedano i paragrafi 2.3.1, 2.3.2
[124] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia, cit.*, p.390.

caratterizzati nel disvalore (condotte idonee ad alterare i prezzi di strumenti finanziari), elevando la soglia di punibilità.[125]

Dal punto di vista del significato letterale, si evidenziano diverse interpretazioni del termine "sensibile". La caratteristica della sensibilità, infatti, può indicare semplicemente il fatto che l'oggetto in questione sia "*conoscibile attraverso i sensi*", oppure che venga "*percepito con una certa evidenza, quindi in modo apprezzabile*".[126]

Analizzando la *ratio* della norma, sembra preferibile il secondo significato. Infatti, il criterio della sensibilità appare finalizzato ad escludere potenziali alterazioni che siano sostanzialmente inoffensive.[127]

Attraverso le strategie di *trading* precedentemente esposte vengono effettuate operazioni che sono concretamente idonee ad alterare il prezzo di strumenti finanziari, ma ci si chiede se l'alterazione sia appunto sensibile, poiché la variazione di prezzo del singolo strumento potrebbe anche essere minima.

Occorre domandarsi a questo punto se la valutazione debba essere effettuata sulla variazione del prezzo di un singolo strumento finanziario o in generale in relazione all'effetto distorsivo complessivo che potenzialmente potrebbe investire il mercato per effetto dell'operazione manipolativa.

Considerando il singolo strumento finanziario la risposta potrebbe essere negativa; tuttavia, tenendo presente la *ratio* della norma, l'operazione complessiva e l'entità dell'effetto distorsivo che può essere creato con un'operazione di questo tipo, si potrebbe concludere che, almeno dal punto di vista della condotta, la fattispecie descritta rientri nell'area di tipicità della norma.

Un ulteriore elemento che potrebbe confermare la natura manipolativa di alcune strategie realizzate dai *traders* ad alta frequenza consiste nell'esplicito riferimento del MAR ai *traders* algoritmici e in particolare agli HFTs. Il Regolamento Europeo sugli abusi di mercato si pone l'obbiettivo di ridefinire la manipolazione del mercato, alla luce della

---

[125] S. SEMINARA, *Diritto penale commerciale*, I, *Il diritto penale del mercato mobiliare*, Torino, 2018, p.1010.
[126] Vocabolario Treccani, voce "sensibile".
[127] A questo proposito appare opportuno ricordare un'obiezione precedentemente esposta in relazione alla natura di reato di pericolo della fattispecie. Il legislatore, infatti, presume che qualsiasi alterazione sensibile del prezzo di strumenti finanziari comporti necessariamente una cattiva allocazione dell'investimento. Questa crasi all'interno della norma incriminatrice potrebbe creare dei problemi scontrandosi con un principio di offensività nei casi in cui l'alterazione del valore dei titoli, seppur ingente, non provochi una cattiva allocazione dell'investimento, oppure quando un'anche minima variazione del prezzo realizzi un effetto distorsivo ingente. F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare, cit*., p. 264.

sempre maggior automatizzazione del commercio degli strumenti di mercato.[128] Vengono quindi forniti "*esempi di strategie abusive specifiche che possono essere effettuate con qualsiasi strumento disponibile di negoziazione, incluse le negoziazioni algoritmiche e quelle ad alta frequenza.*"[129]

Come precedentemente accennato,[130] il secondo comma dell'art 12 del MAR descrive alcune condotte che devono essere considerate manipolative. Tra queste ritroviamo alla lettera 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;*"[131]

La descrizione di tali condotte sembra riferirsi alle strategie di *quote stuffing, spoofing e layering*, modelli di *trading* strettamente legati alla negoziazione ad alta frequenza.

Come precedentemente chiarito,[132] tale riferimento effettuato dal Regolamento pur non potendo essere certo inteso quale norma incriminatrice, potrebbe però costituire un forte argomento interpretativo per sostenere che le strategie realizzate dai sistemi di HFT costituiscano vere e proprie condotte manipolative.

---

[128] Regolamento (UE) N. 596/2014 del Parlamento Europeo e del Consiglio del 16 aprile 2014 relativo agli abusi di mercato (regolamento sugli abusi di mercato - MAR), considerando n. 38
[129] *Ibidem.*
[130] Si veda §4.1.6
[131] MAR, art 12, n.2, lett. c)
[132] Si veda §4.1.6

Si potrebbe quindi concludere che l'utilizzatore, nell'azionare il sistema di HFT all'inizio della giornata di contrattazione, realizza, per mezzo dello strumento di IA, condotte che sono riconducibili alla nozione di artifici fornita dall'art. 185 TUF.

Assumendo che l'utilizzatore commetta effettivamente il reato,[133] potrebbe emergere la responsabilità penale del programmatore; il *designer*, infatti, potrebbe quindi rispondere per concorso con l'utilizzatore ai sensi dell'art 110 c.p.

Gli elementi necessari che devono essere provati per fondare questo tipo di responsabilità sono il contributo concorsuale e un particolare elemento soggettivo.[134]

Affidando la trattazione approfondita dell'elemento soggettivo al paragrafo espressamente dedicato al dolo, si può analizzare brevemente l'aspetto attinente al contributo concorsuale del programmatore rispetto alla condotta dell'utilizzatore.

Nei fatti, il soggetto precedentemente definito come produttore-programmatore realizza un sistema di IA attraverso il quale l'autore del reato potrà compiere le condotte manipolative. Se si tratta di intelligenze artificiali più evolute, come sistemi di *reinforcement learning* o *deep learning*,[135] la realizzazione dell'algoritmo di IA si estrinseca in una prima fase di mera programmazione e una fase successiva di "addestramento".[136] Generalmente il programma viene poi venduto all'utilizzatore. Attraverso questo insieme di comportamenti il *designer* realizza un contributo materiale alla condotta dell'autore del reato poiché mette a disposizione lo strumento di realizzazione dello stesso.

In altri casi, il programma potrebbe essere progettato e realizzato dallo stesso utilizzatore: in questa circostanza, ovviamente, non si realizza un concorso di persone per la mancanza della pluralità di soggetti coinvolti.

Potrebbe inoltre verificarsi l'ipotesi in cui una fase di programmazione o addestramento venga affidata al soggetto utilizzatore, che modifica il sistema di IA adattandolo alle proprie specifiche esigenze. In presenza di tale fattispecie, occorrerebbe effettuare un accertamento molto complesso a livello tecnico, individuando se il prodotto, nel momento della vendita, fosse già in grado di realizzare le condotte manipolative (o di

[133] In questo momento si intende volutamente tralasciare le criticità che sorgono in relazione ad altri elementi della fattispecie che saranno invece affrontate nei seguenti paragrafi.
[134] C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale*, *cit.*, p. 553
[135] Si veda §1.1.1
[136] B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automazione artificiale,* in *Diritto dell'Informazione e dell'informatica* (II), fasc.2, 2021, p. 317.

apprendere dal mercato come realizzarle) o se, invece, tale capacità derivi delle modifiche successive che sono state effettuate dall'utilizzatore. Dalla risposta a questo quesito dipenderà la sussistenza del contributo concorsuale e quindi la responsabilità del programmatore.

4.2.4 La causalità

Si è già visto come la mancanza di trasparenza dei sistemi di *black box* possa dare luogo a problemi legati alla ricostruzione del percorso causale che ha portato alla realizzazione dell'evento.[137]

La dottrina americana ha evidenziato che, quando il danno è riconducibile ad un cosiddetto "fattore robotico" (ossia una decisione presa dal sistema di IA estranea all'originario disegno del programmatore), la persona fisica non può essere ritenuta penalmente responsabile perché l'evento ricade al di fuori dell'area di rischio prevedibile.[138] Alcuni autori italiani hanno riconosciuto in questo ragionamento la tematica del fattore causale sopravvenuto interruttivo del nesso causale, secondo quanto previsto dall'art 41, comma 2 c.p.[139] In tal senso, il comportamento autonomo e imprevedibile del sistema si sarebbe infatti interposto tra la condotta della persona fisica e l'evento penalmente rilevante cagionando un rischio qualitativamente diverso da quello *ab origine* concepito.[140]

La medesima dottrina ha tuttavia criticato tale impostazione della dottrina statunitense, ritenendo che, nell'ambito del diritto italiano, l'art. 41 comma 2 c.p. non possa trovare applicazione in questo caso. Chi programma il sistema di IA sa, infatti, di costruire un sistema il cui comportamento sarà in parte imprevedibile, ma sa anche che i suoi effetti si estrinsecheranno all'interno di un'area di rischio comunque conosciuta. Pertanto, il comportamento della macchina non costituisce un fattore terzo eccezionale rispetto alla condotta dell'agente.[141]

Per quanto riguarda specificatamente i reati di manipolazione del mercato realizzati con sistemi di HFT, un aspetto necessario da evidenziare è che l'art 185 TUF non è un reato

---

[137] Y. BATHAEE, *The Artificial Intelligence Black Box and the failure of intent and causation,* in *Harvard Journal of Law & Technology* Volume 31, Number 2 Spring, 2018.
[138] *Ibidem*.
[139] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato, cit*.
[140] *Ibidem.*
[141] *Ibidem*.

di evento, ma di condotta. Apparentemente, le problematiche legate alla causalità non sembrano interessare il reato in esame, poiché manca un evento a cui riferirle.

Tuttavia, si ritiene che alcuni aspetti relativi in senso lato al decorso causale possano comunque interessare il presente lavoro. Nell'ambito di reati di manipolazione del mercato compiuti attraverso l'utilizzo di sistemi di IA, infatti, alcune tematiche relative alla causalità potrebbero emergere da due differenti punti di vista.

Un primo aspetto, in realtà, prescinde dalla natura algoritmica dell'operatore di mercato e costituisce una tematica generale relativa alla fattispecie di reato. Si tratta di un problema di "causalità potenziale" legata all'accertamento del pericolo ossia della concreta idoneità della condotta a "*provocare una sensibile alterazione dei prezzi di strumenti finanziari*".[142] Per accertare tale idoneità, occorre quindi valutare il possibile impatto che l'operazione potrebbe avere sul mercato.

Il giudizio di pericolo richiesto dall'art 185 TUF già in passato appariva particolarmente complesso se calato in un contesto dinamico come quello dei mercati finanziari, influenzato da molteplici fattori. Mancano, infatti, in questo settore leggi economiche che assicurino un sufficiente grado di certezza.[143]

In epoca più recente, tale accertamento è reso ancora più difficile dall'elevata presenza all'interno dei mercati di operatori algoritmici ad alta frequenza.[144] Il fatto che i sistemi di HFT operino ad altissima velocità e che prendano decisioni operative autonome rende ancora più incerto e imprevedibile l'andamento dei mercati e quindi meno utilizzabili le leggi economiche o le massime di esperienza necessarie per effettuare un giudizio di pericolo.

D'altra parte, talvolta, proprio grazie all'alta velocità, l'evento dell'alterazione, di per sé non necessario per la consumazione del reato, viene subito realizzato. Si è precedentemente osservato che nella difficoltà di effettuare una vera e propria prognosi postuma relativa all'idoneità delle condotte di alterare i prezzi dei titoli, spesso ci si affida all'analisi della concreta reazione del mercato alle operazioni. Pertanto, se l'alterazione dei prezzi è stata prodotta, tale giudizio potrebbe essere più semplice, poiché il pericolo si è

---

[142] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare, cit.* p.264.

[143] F. CONSULICH, *Manipolazione del mercato e disorientamenti dogmatici: tra eventi di pericolo e pericolo di eventi, cit.*

[144] O. KAYA, *High-frequency trading, reaching the limits*, Research Briefing Global financial markets, Deutsche Bank Research, Francoforte, 2016.

effettivamente realizzato.[145] In realtà, questa strada non risulterebbe risolutiva poiché potrebbe comunque sorgere il dubbio che l'alterazione dei prezzi non derivi effettivamente dalle operazioni prodotte dal sistema di HFT, ma da altri fattori del mercato. Tra l'altro non vi sarebbe comunque modo di verificare con certezza questo particolare tipo di percorso causale data la mancanza di linearità delle dinamiche di mercato.[146]

Un secondo aspetto legato, in senso lato, a dinamiche di tipo causale è relativo specificatamente a casi in cui le operazioni manipolative siano realizzate da sistemi di AI sufficientemente complessi.

In questi casi, pur mancando l'evento naturalistico, si può osservare che la condotta descritta inizia con l'azionamento della macchina, ma viene effettivamente realizzata dal sistema di IA nel momento in cui vengono immesse nel mercato operazioni definibili come manipolative.[147] Ci si potrebbe quindi riferire ad una sorta di causalità "interna" alla condotta stessa, influenzata, in questo caso, dalle problematiche legate alla *black box*. Quando lo strumento utilizzato per compiere il reato è un sistema di IA, la fattispecie sembra influenzata dalle stesse problematiche legate alla causalità che vengono generalmente alla luce solo nei reati di evento. Semplicemente, invece che prendere in considerazione il caso in cui il decorso causale si concluda con un evento, si potrebbe considerare che il momento finale del percorso eziologico, iniziato con l'azionamento della macchina, coincida con il compimento delle operazioni manipolative.

Sotto questo particolare profilo emergono le due problematiche sopra evidenziate relative ai sistemi di IA che presentano le caratteristiche di *black boxes*.

La teoria relativa al fattore "robotico" interruttivo del nesso causale sembra non trovare riscontro all'interno del nostro ordinamento, almeno secondo la parte dottrina che si è pronunciata sul tema.[148]

---

[145] F. CONSULICH, *Manipolazione del mercato e disorientamenti dogmatici: tra eventi di pericolo e pericolo di eventi, cit.*

[146] Si veda §4.1.7

[147] Tale problema non si pone quando gli strumenti utilizzati per commettere reati non sono sistemi di IA con caratteristiche di *black boxes*. Ad esempio, in caso di diffamazione online, l'autore del reato si limita ad inviare il messaggio, compiendo in realtà la sola condotta fisica di premere il tasto "invio". Nessuno però si potrebbe porre dei problemi relativi alla causalità, poiché è evidente che la pubblicazione del messaggio diffamatorio è automatica e indissolubilmente legata all'azione "fisica" dell'autore.
Quando si tratta di sistemi di IA l'automatismo non è più così scontato dato che il sistema di IA è in grado di prendere decisioni in maniera autonoma e non è possibile ricostruire *ex post* il percorso logico compiuto dalla macchina.

[148] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato, cit.*

L'aspetto più discusso riguarda, invece, l'impossibilità di ricostruire il decorso causale che ha portato il sistema di IA al compimento delle operazioni. A questo proposito occorre tuttavia effettuare una distinzione tra il soggetto che aziona la macchina e chi invece l'ha programmata.

Per l'utilizzatore il problema non sembra essere particolarmente rilevante: egli fornendo l'avvio al sistema di IA, al di là degli imperscrutabili meccanismi interni, sicuramente provoca, a livello causale, il compimento delle operazioni. A tal proposito potrebbe al massimo essere evidenziato un problema relativo all'elemento soggettivo, in relazione alla rappresentazione del decorso causale.[149]

Dal punto di vista della responsabilità del programmatore occorre valutare se il contributo materiale fornito nell'ambito del concorso possa costituire una condizione necessaria rispetto al compimento delle operazioni manipolative da parte del sistema di IA.

Per valutare il contributo del concorrente, infatti, secondo parte della dottrina sarebbe necessario utilizzare un criterio di causalità condizionalistica rispetto al fatto di reato.[150]

Anche da questo punto di vista, in realtà, non sembrano sorgere particolari problemi. Infatti, la realizzazione materiale dello strumento attraverso il quale viene compiuto il reato ovviamente è indispensabile al fine della realizzazione dello stesso. Non risulta rilevante a tal fine il fatto che i meccanismi interni al sistema di IA non siano conoscibili.

L'unico aspetto che potrebbe interrompere il nesso causale del contributo del programmatore è un'eventuale riprogrammazione da parte di soggetti terzi del sistema di IA.

Al di là di queste considerazioni, alcuni autori, per sopperire all'inevitabile *gap* conoscitivo caratteristico dei sistemi di *black box*, hanno proposto l'installazione di "scatole nere", in questo contesto intese come meccanismi capaci di registrare i passaggi interni al funzionamento del sistema di IA e finalizzate alla ricostruzione *ex post* della dinamica causale.[151] Una strategia di questo tipo è stata ipotizzata anche dalla già citata proposta di Regolamento Europeo in materia di intelligenza artificiale.[152] Per i sistemi ad alto rischio,

[149] Si veda il paragrafo seguente.
[150] C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale*, *cit*., p. 557., F. MANTOVANI, Cedam, Padova, 2020, p.561.
[151] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato, cit.*
[152] *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione*, 2021, eur-lex.europa.eu

infatti, il Regolamento richiede l'installazione di meccanismi che consentano la registrazione automatica degli eventi (*log*) durante il funzionamento.[153]

4.2.4 Il dolo

La problematica principale in relazione al compimento di reati attraverso l'intelligenza artificiale è quella relativa all'elemento soggettivo.

I sistemi di IA più avanzati sono dotati di un'ampia autonomia decisionale, accompagnata però da una scarsa trasparenza in relazione al loro funzionamento. Tali programmi sono in grado di elaborare soluzioni nuove e inaspettate al problema loro assegnato attraverso quello che è stato definito "*comportamento emergente"*.[154] Inoltre, per effetto della *black box* non è possibile ricostruire il procedimento decisionale del sistema e quindi comprendere quali informazioni hanno condotto l'algoritmo al compimento di determinate operazioni.[155] Come precedentemente osservato,[156] queste due caratteristiche creano sicuramente alcune problematiche in relazione all'elemento soggettivo e in particolare al dolo della persona fisica che utilizza la macchina. L'imprevedibilità del comportamento del sistema di IA potrebbe infatti rendere impossibile, per la persona fisica che aziona la macchina, la rappresentazione delle conseguenze del proprio agire.[157]

Inoltre, nel contesto dei mercati finanziari il problema sembra acuirsi poiché l'alta presenza di agenti artificiali, anche non dichiarati, genera una condizione di incertezza diffusa che rende impossibile stimare delle previsioni ragionevoli in relazione al comportamento degli operatori del mercato e all'andamento dei titoli.[158]

Tenendo in considerazione queste osservazioni generali, il presente paragrafo si pone l'obbiettivo di analizzare le specifiche problematiche relative al dolo in relazione alla fattispecie incriminatrice italiana della manipolazione del mercato, nel caso in cui il reato venga compiuto attraverso sistemi di HFT.

---

[153] Si veda §1.1.2

[154] B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automazione artificiale, cit*.

[155] I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale, cit*.

[156] Si vedano §1.1.1 e §3.3

[157] Y. BATHAEE*, The Artificial Intelligence Black Box and the failure of intent and causation,* in *Harvard Journal of Law & Technology* Volume 31, Number 2 Spring, 2018.

[158] F. CONSULICH, *Flash Offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti*, in *Riv. it. dir. e proc. pen*., n.3- 2022.

a) L'oggetto del dolo

Secondo la dottrina e la giurisprudenza consolidata il dolo è costituito da due elementi: volontà e rappresentazione. L'art 43 comma 1 c.p.[159] sancisce che l'oggetto di tale volontà e rappresentazione consiste nell'evento dannoso o pericoloso, risultato dell'azione od omissione. Tale definizione è da tempo ritenuta incompleta; la dottrina infatti sostiene che la rappresentazione e la volizione del dolo debbano riferirsi all'intero fatto tipico e non al solo evento naturalistico, poiché altrimenti si andrebbe ad escludere dall'area di applicazione del dolo tutti i reati di sola condotta.[160] Una simile conclusione trova, tra l'altro, un riscontro normativo nell'art 47 c.p., il quale, stabilendo che il dolo è escluso dall'errore sul "*fatto che costituisce reato*", conferma l'assunto che volontà e rappresentazione debbano avere per oggetto il fatto tipico.[161]

Tale fatto tipico deve inoltre essere inteso come astratto: non è necessario che il dolo si concretizzi nella volontà e nella rappresentazione del "fatto storico", poiché è sufficiente che investa soltanto gli elementi rilevanti per l'integrazione della fattispecie legale.[162]

Tutti gli elementi della fattispecie tipica sono ricompresi nell'oggetto del dolo, anche se a questo proposito occorre effettuare una distinzione.

Oggetto di rappresentazione devono essere tutti gli elementi descrittivi e normativi del fatto: sia le qualifiche naturalistiche che quelle giuridiche. Nei reati di evento anche il decorso causale deve essere oggetto di rappresentazione. Tuttavia, è sufficiente che l'agente si prefiguri lo svolgimento del reato nei tratti essenziali rilevanti ai fini della valutazione penalistica: la rappresentazione della derivazione causale dell'evento non viene meno per un qualche decorso causale anomalo.[163]

Per quanto riguarda la volontà, abbandonata la cosiddetta "teoria della rappresentazione" (secondo la quale l'oggetto di volizione poteva essere solo la condotta,

---

[159] Art 43 comma 1 c.p. recita "*Il delitto: è doloso, o secondo l'intenzione, quando l'evento dannoso o pericoloso, che è il risultato dell'azione od omissione e da cui la legge fa dipendere l'esistenza del delitto, è dall'agente preveduto e voluto come conseguenza della propria azione od omissione*;"

[160] S. PROSDOCIMI, *Reato Doloso*, in *Digesto*, Wolters Kluwer, 1996, disponibile presso One Legale. A titolo di completezza si citano precedenti teorie dottrinali ormai superate che prevedevano che il riferimento dell'art 43 c.p. all'evento non riguardasse l'evento naturalistico, ma l'evento in senso giuridico, concepito come lesione o messa in pericolo del bene protetto.

[161] *Ibidem*.

[162] F. MANTOVANI, *Diritto Penale, cit*., p. 338.

[163] G. FIANDACA, E. MUSCO, *Diritto penale parte generale*, Zanichelli, Bologna, 2019, p. 376; C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale, cit*., p. 361

poiché ciascuno può volere solo i propri movimenti corporei), oggi la dottrina concorda che oggetto della volizione debbano essere tutti gli elementi della fattispecie tipica. Fanno eccezione solo i presupposti della condotta e le qualifiche personali che appunto non possono essere volute dall'agente ma solo conosciute.[164]

Un aspetto lungamente dibattito è relativo alla necessità che l'oggetto del dolo ricomprenda la coscienza dell'offesa. A questo proposito, anche se non sono mancati sostenitori di una tesi affermativa, oggi la maggior parte della dottrina ritiene che la consapevolezza dell'illiceità del comportamento esuli dall'oggetto del dolo.[165] Una delle motivazioni più frequenti a questo proposito consiste nel fatto che non sempre all'illiceità penale è presupposta una violazione dei valori fondamentali. Ad esempio, è escluso nei "reati di pura creazione legislativa", dove spesso è molto difficile cogliere il carattere antisociale del fatto.[166]

Svolte queste doverose premesse, occorre concentrarsi sull'oggetto del dolo nella norma incriminatrice in esame nel presente lavoro. In particolare, per quanto riguarda la manipolazione operativa del mercato, il dolo generico richiesto dall'art 185 TUF si manifesta nella volontà di porre in essere operazioni simulate o altri artifici e nella rappresentazione della concreta idoneità di questi a provocare una sensibile alterazione del prezzo degli strumenti finanziari.[167]

Come già sottolineato, il legislatore ha strutturato il reato di manipolazione del mercato come un reato di pericolo, anticipando quindi la tutela ed escludendo l'insieme delle conseguenze della condotta dagli elementi del fatto tipico. Probabilmente uno dei motivi di tale scelta è legato al fatto che, nel contesto del mercato finanziario, l'operatore non è in grado di prevedere i fattori che potrebbero essere innescati dalla propria condotta. Secondo la formulazione della norma incriminatrice, non è necessaria quindi una rappresentazione delle conseguenze dannose del proprio comportamento.[168]

Oggetto di rappresentazione deve essere, invece, la concreta idoneità delle condotte ad alterare i valori dei titoli. Rispetto a questo elemento, l'agente potrebbe facilmente essere animato da dolo eventuale. Egli, infatti, a causa della complessità del mercato e

---

[164] C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale, cit.*, p. 362
[165] *Ibidem*.
[166] G. FIANDACA, E. MUSCO, *Diritto penale parte generale*, *cit*., p. 379.
[167] N. MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia*, *cit*.., p. 394.
[168] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare*, *cit*., p.283.

dell'interazione con gli altri operatori, solo in rari casi può avere la certezza che il proprio comportamento manipolativo sia concretamente idoneo all'alterazione dei prezzi.[169]

L'applicazione del dolo eventuale ad una caratteristica della condotta non è un fenomeno estraneo al nostro ordinamento. Si pensi, ad esempio, al delitto di ricettazione previsto dall'art 648 c.p. In questo caso la giurisprudenza ammette un'imputazione a titolo di dolo eventuale in relazione alla "*provenienza delittuosa della cosa*". La Corte di Cassazione ha infatti sostenuto che sia configurabile questa ipotesi nel caso in cui l'agente sia animato da un atteggiamento psicologico che, pur non attingendo il livello della certezza, si colloca ad un gradino immediatamente più alto del mero sospetto, configurandosi in termini di rappresentazione di acquistare, ricevere o occultare denaro o cose di provenienza delittuosa.[170]

Infine, appare opportuno sottolineare che l'art 185 TUF si riferisce in generale all'alterazione "*di strumenti finanziari*": sembra che non si debba trattare di strumenti finanziari determinati o precedentemente individuati. L'agente dovrà quindi solamente essere consapevole dell'idoneità delle proprie condotte ad alterare il prezzo di un qualsiasi strumento finanziario.

b) Il dolo dell'utilizzatore; tra dolus generalis e dolo eventuale

Sono già state descritte alcune fattispecie, ricondotte al concetto di "*abuse by design*", nelle quali viene provato un preciso intento manipolativo dell'utilizzatore che ha impartito determinate istruzioni al programmatore al fine realizzare il reato in questione.[171]

L'ipotesi che si intende esaminare in questo paragrafo è tuttavia differente: si tratta del caso in cui il sistema di IA, originariamente non programmato con lo specifico obbiettivo di

---

[169] *Ibidem.*

[170] Cass., sez. un., 30 marzo 2010, n.12433, in *Dir. pen. proc*., 2010, in merito alla configurabilità del dolo eventuale nel delitto di ricettazione.
Si veda inoltre Cass., sez. II, 22 maggio 2017, n. 25439: "*In tema di ricettazione, ricorre il dolo nella forma eventuale quando l'agente ha consapevolmente accettato il rischio che la cosa acquistata o ricevuta fosse di illecita provenienza, non limitandosi ad una semplice mancanza di diligenza nel verificare la provenienza della cosa, che invece connota l'ipotesi contravvenzionale dell'acquisto di cose di sospetta provenienza. (Nella fattispecie, relativa all'esposizione al pubblico, da parte dell'imputato, di merce contraffatta adagiata in terra su un lenzuolo, la Corte ha ritenuto immune da censure la sentenza impugnata, secondo cui le modalità di presentazione degli oggetti consentivano di escludere che il medesimo ignorasse la loro illecita provenienza, quantomeno a titolo di dolo eventuale)*."

[171] Si veda il caso Coscia, descritto al §3.2.2

effettuare operazioni manipolative, attraverso meccanismi di *machine learning*, apprenda autonomamente strategie abusive che permettano di massimizzare i profitti.

A questo proposito vengono alla luce le problematiche sopra esposte in relazione alla crisi dell'elemento soggettivo di fronte a fattispecie di reato materialmente compiute da sistemi *black box*. Le istruzioni fornite alla macchina, infatti, hanno natura generale ed indicano all'algoritmo quale comportamento finanziario seguire, non il tipo di operazione o di artificio da compiere, il momento in cui realizzarlo e le concrete modalità.[172]

Il soggetto che aziona la macchina, quindi, non può avere una piena rappresentazione, nello specifico, delle operazioni che in concreto verranno compiute dell'algoritmo. Pertanto, secondo la dottrina maggioritaria, la persona fisica difetta del dolo del fatto, a meno che non si ritenga sufficiente una sorta di *dolus generalis*.[173]

Questa particolare categoria di dolo è stata in realtà creata in relazione a reati di evento: si tratta della situazione in cui l'agente si rappresenta e vuole l'evento naturalistico, ma in termini astratti e generici, senza che l'atteggiamento psicologico sia specificamente rivolto a tutti gli elementi del fatto storico.[174] La giurisprudenza tende a negare la configurabilità di una tale dilatazione dell'elemento soggettivo.[175]

La categoria del *dolus generalis* è stata utilizzata dalla giurisprudenza soprattutto in relazione a particolari casi di omicidio in cui, a seguito di atti lesivi sorretti dalla volontà omicida che non raggiungono lo scopo, l'autore del reato ha cagionato effettivamente la morte della persona in virtù di un successivo comportamento realizzato nell'erroneo convincimento di aver precedentemente provocato la morte della vittima.[176] La giurisprudenza in questi casi ha ritenuto che non potesse essere ipotizzato un dolo dell'agente in relazione al fatto di reato poiché l'atto che ha effettivamente cagionato la morte della vittima sarebbe sorretto invece da colpa. In questi casi, quindi, è stato configurato il tentato omicidio in concorso con l'omicidio colposo.

---

[172] F. CONSULICH, *Il Nastro Di Möbius. Intelligenza Artificiale e imputazione penale nelle nuove forme di abuso del mercato*, Banca Borsa e Titolo di Credito - n. 2, 2018

[173] *Ibidem*.

[174] C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale*, *cit*., p. 362.

[175] Cass., sez. I, 18 marzo 2003, n. 1697, Iovino e altri, richiamata da Cass., sez. I, 17 novembre 2015, n. 15774, disponibili presso italigiure.giustizia.it

[176] Si tratta generalmente di casi in cui l'autore del reato ferisce la vittima causandone l'incoscienza e, credendola già deceduta, cerca di sbarazzarsi del cadavere. La morte in questi casi però sopravviene per effetto della seconda condotta.

Parte della dottrina non concorda con questa ricostruzione e ritiene invece che tali condotte si presentino come sufficientemente unitarie e sorrette da dolo, caratterizzate semplicemente da un'*aberratio* nell'*iter* causale che produce l'evento.[177]

Appare opportuno osservare, inoltre, che la giurisprudenza in questi casi non esclude completamente la configurabilità del dolo. In alcune circostanze potrebbe essere comunque ravvisato il dolo eventuale o il dolo alternativo in relazione all'ultimo atto della condotta. Una pronuncia della Corte di Cassazione del 2003, infatti, ha affermato che nel caso in cui "*venga accertata dal giudice di merito l'inesistenza dell'errore sullo stato vitale del soggetto passivo e l'agente abbia agito nel mero dubbio circa la già avvenuta produzione dell'evento, la morte sarà attribuita a titolo di dolo diretto, nella forma di dolo alternativo*".[178] In altre situazioni in caso di dubbio potrebbe essere più facilmente ipotizzato un dolo eventuale.[179]

Ritornando al campo di analisi del presente lavoro, si potrebbe evidenziare come la fattispecie descritta presenti alcuni punti di contatto con quella relativa alla realizzazione di una manipolazione del mercato attraverso sistemi di IA. In entrambi i casi, infatti, l'autore compie una condotta frazionata in cui l'ultimo atto (che in una fattispecie realizza l'evento naturalistico di omicidio e nell'altra realizza le operazioni manipolative) non è sorretto da un vero e proprio dolo da parte dell'agente.[180]

La giurisprudenza ha sostenuto, nel caso sopra citato, che l'esistenza di un dubbio in relazione alla già avvenuta produzione dell'evento morte permette l'imputazione a titolo di dolo eventuale. Ci si potrebbe pertanto chiedere se sia possibile applicare il dolo eventuale anche al caso in cui l'utilizzatore del sistema di HFT azioni la macchina con la consapevolezza che questa potrebbe compiere operazioni manipolative.

---

[177] P. PISA, *Giurisprudenza commentata di diritto penale, Volume Primo, delitti contro la persona e il patrimonio*, *cit*., p.23.

[178] Cass., sez. I, 18 marzo 2003, n. 1697, Iovino e altri, disponibile presso italigiure.giustizia.it, citata in P. PISA, *Giurisprudenza commentata di diritto penale, Volume Primo, delitti contro la persona e il patrimonio*, *cit.*, p.23.
A questo proposito si aggiunge che se fosse invece configurato un dolo eventuale questo potrebbe comunque sopravvivere alla formula "*Thyssen Krupp*" poiché, dato l'originario dolo di omicidio, appare evidente che l'autore del reato avrebbe agito anche se avesse avuto la certezza di provocare la morte.

[179] P. PISA, *Giurisprudenza commentata di diritto penale, Volume Primo, delitti contro la persona e il patrimonio, cit.,* p.23.

[180] Ovviamente le due fattispecie non sono sovrapponibili. Al di là del fatto che in un caso si tratta di un reato di evento e nell'altro la fattispecie incriminatrice prevede solo una condotta, in relazione all'omicidio, l'autore aveva un dolo originariamente rivolto alla morte della vittima, mentre l'utilizzatore che aziona il sistema di IA potrebbe difettare di un originario intento manipolativo.

A questo proposito, appare opportuno premettere che, se è vero che l'utilizzatore del sistema di HFT non è in grado di prevedere con esattezza *quale* operazione manipolativa verrà compiuta, sicuramente è a conoscenza della capacità della macchina di apprendere comportamenti abusivi e di realizzarli.

In base all'analisi effettuata, appare evidente che la consapevolezza che i sistemi di IA sufficientemente avanzati, utilizzati per la contrattazione ad alta frequenza, siano in grado apprendere e realizzare strategie manipolative, sia ampiamente diffusa nel settore. Molti studi hanno infatti evidenziato che, se si permette ai sistemi di intelligenza artificiale di basare il proprio apprendimento sui dati ricavati direttamente dal mercato,[181] gli algoritmi non solo potrebbero autonomamente imparare e mettere in atto operazioni manipolative, ma è statisticamente molto probabile che lo faranno.[182]

È sicuramente vero che l'utilizzatore non può rappresentarsi quale operazione sarà compiuta dalla macchina, in quale momento, o quale effetto distorsivo tale operazione è concretamente idonea a provocare. Appare però ugualmente evidente che, nel momento in cui aziona la macchina, l'utilizzatore si rappresenta comunque la possibilità del compimento di operazioni manipolative da parte del sistema di HFT. In un contesto così tecnico non appaiono plausibili, infatti, le obiezioni basate sulla mancanza di conoscenza delle potenzialità manipolative dei sistemi di HFT.

Occorre osservare tuttavia che, anche se si volesse accettare la configurabilità di un dolo eventuale in cui la rappresentazione non investa una specifica strategia manipolativa ma semplicemente il compimento di operazioni non predeterminate concretamente idonee ad alterare i prezzi di strumenti finanziari, occorrerebbe rispettare i criteri di accertamento enunciati dalla celebre sentenza "*ThyssenKrupp*".[183]

Tale sentenza, delineando il confine tra dolo eventuale e colpa cosciente, ha indicato i canoni probatori alla stregua dei quali il giudice deve valutare la sussistenza di questa categoria di elemento soggettivo.[184] Tra questi criteri, è presente la cosiddetta "formula di Frank" che prevede che, ai fini della configurazione del dolo eventuale, sia necessario fornire

[181] Il sistema di HFT che apprende dati direttamente dal mercato riesce infatti ad elaborare strategie di *trading* anche sulla base delle reazioni che hanno avuto gli altri partecipanti al mercato rispetto a precedenti operazioni.
[182] Si veda, ad esempio, il lavoro precedentemente descritto nel paragrafo 3.2.3. (T. MIZUTA, *Does an Artificial Intelligence Perform Market Manipulation with its own Discretion? – A Genetic Algorithm Learns in An Artificial Market Simulation*, SPARX Asset Management Co. Ltd., Tokyo, 2020.)
[183] Cass., sez. un., 24 aprile 2014, n.38343.
[184] C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale*, *cit*, p. 374.

la prova che l'autore del reato avrebbe agito ugualmente anche se avesse avuto la certezza della verificazione dell'evento.[185]

Occorrerebbe quindi provare che l'utilizzatore avrebbe azionato la macchina anche se avesse avuto la certezza che il sistema di IA avrebbe messo in atto un'operazione manipolativa.

Nonostante tale prova appaia molto difficile da fornire, si deve evidenziare che la diffusa consapevolezza della capacità manipolativa dei sistemi di HFT e le competenze professionali dell'agente costituiscano elementi idonei a dimostrare il superamento della "formula di Frank". Inoltre, altri canoni probatori citati dalla sentenza "*ThyssenKrupp*" sono la probabilità della verificazione dell'evento e le conseguenze negative anche per l'autore nel caso di sua verificazione.[186] A tal proposito si potrebbe argomentare che, secondo gli studi citati, la probabilità che un sistema di HFT, apprendendo dal mercato, impari e metta in atto una strategia manipolativa è prossima alla certezza.[187] Inoltre, il compimento del fatto di reato non comporterebbe particolari conseguenze negative per l'autore poiché da un lato questa tipologia di reati è molto difficile scoprire e dall'altro è invece molto proficua a livello economico.[188]

Tutte queste considerazioni in relazione all'applicabilità del dolo eventuale alla fattispecie oggetti di analisi trovano un ostacolo nella struttura dell'art. 185 TUF e in particolare nell'oggetto del dolo previsto dalla norma.

È stato precedentemente sostenuto che il reato di manipolazione del mercato possa reggere un'imputazione a titolo di dolo eventuale. Si è infatti ricordato che anche i reati di condotta possono essere interessati da questa categoria di elemento soggettivo.[189] Inoltre, la stessa giurisprudenza ha chiarito come il dolo generico previsto dal reato di manipolazione del mercato permetta l'applicazione del dolo eventuale.[190]

---

[185] In questo caso di parla di evento poiché la fattispecie è relativa a reati di omicidio, ma la formula è valida anche in relazione a reati di condotta. Semplicemente alla verificazione dell'evento si sostituirà in generale la commissione del reato.

[186] C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale, cit.,* p. 374.

[187] T. MIZUTA, *Does an Artificial Intelligence Perform Market Manipulation With Its Own Discretion? – A Genetic Algorithm Learns in An Artificial Market Simulation*, *cit.*

[188] In questo senso si veda A. AZZUTTI, W. G. RIING, H. S. STIHEL, *Machine learning, Market Manipulation and Collusion on capital markets why the "Black Box" matters*, in *University of Pennsylvania Journal of International Law,* 2021.

[189] Si veda il paragrafo precedente in relazione al reato di ricettazione.

[190] Trib. Milano, 11 novembre 2002, in *Riv. trim. dir. pen, econ*., 2003, *cit.*

Tuttavia, la giurisprudenza citata riferiva il dolo eventuale a un particolare elemento del reato, ossia la concreta idoneità delle condotte ad alterare sensibilmente il prezzo di strumenti finanziari.[191] In questo senso il soggetto che, pur nutrendo un dubbio sulla natura manipolativa di determinate operazioni, le compia ugualmente potrà essere ritenuto penalmente responsabile del reato a titolo di dolo eventuale.[192] In tal caso, però, le specifiche operazioni in questione sono conosciute e volute dall'agente.

La fattispecie in esame risulta invece differente: l'utilizzatore non può prevedere quali operazioni potranno essere messe in atto dalla macchina, sa solamente che tra la grande mole di operazioni che verranno realizzate dal sistema IA alcune potrebbero essere "*concretamente idonee ad alterare sensibilmente i prezzi di strumenti finanziari"*. In questo esempio, il dolo eventuale quindi non si riferirebbe appunto alla caratteristica della condotta ma alla possibilità di compimento della condotta stessa.

Pertanto, in relazione alle specifiche operazioni compiute dal sistema di HFT non si ravvisa né una rappresentazione né una volizione dell'agente, nemmeno nella forma del dolo eventuale.

Ai fini della configurabilità del dolo eventuale, sarebbe invece necessario che l'utilizzatore, rappresentandosi la possibilità che il sistema di IA compia una serie di operazioni manipolative determinate nei loro tratti essenziali, agisca ugualmente. Ovviamente non è questo il caso poiché, come più volte affermato, la persona fisica non può prevedere il concreto comportamento dell'agente artificiale.

Poiché quindi si ritiene necessario che il dolo dell'utilizzatore si estrinsechi nella rappresentazione e nella volontà della singola operazione (intesa da parte della dottrina come l'immissione di un ordine di acquisto o di vendita di uno specifico strumento finanziario),[193] la configurabilità dell'elemento soggettivo troverà un ostacolo nell'imprevedibilità del comportamento del sistema di IA.[194]

Quella del dolo eventuale appare quindi una strada eccessivamente lontana dal principio di colpevolezza previsto dalla Costituzione e che, tra l'altro, andrebbe

---

[191] Anche per quanto riguarda il reato di ricettazione la sentenza sopra citata (Cass., sez. II, 22 maggio 2017, n. 25439) in realtà sostiene l'ammissibilità del dolo eventuale in relazione ad un elemento del reato ossia la provenienza delittuosa della cosa.

[192] F. CONSULICH, *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare, cit*., p. 283.

[193] F. CONSULICH, *Il Nastro Di Möbius. Intelligenza Artificiale e imputazione penale nelle nuove forme di abuso del mercato*, *cit*

[194] Y. BATHAEE*, The Artificila Intelligence Black Box and the failure of intent and causation, cit.*

sostanzialmente ad impedire lo sviluppo di un fenomeno economico che, seppur discusso, appare comunque dotato di aspetti positivi.[195]

c) Il dolo del programmatore; il dolo di concorso

Come precedentemente affermato si potrebbe ipotizzare una responsabilità del programmatore del sistema di HFT per concorso con l'utilizzatore. Il programmatore fornisce infatti lo strumento di realizzazione del reato.

Dottrina e giurisprudenza consolidata ritengono che i requisiti strutturali del concorso di persone siano, oltre alla realizzazione di una fattispecie di reato e l'esistenza di una pluralità di agenti, il contributo concorsuale e l'elemento soggettivo.[196]

Gli aspetti relativi al contributo concorsuale del programmatore sono già stati approfonditi in precedenza.[197]

L'elemento soggettivo nel concorso di persona invece si estrinseca in due aspetti: la consapevolezza e la volontà di concorrere con altri nella commissione di un reato e la rappresentazione e la volontà in relazione al fatto di reato.[198]

Per quanto riguarda il primo aspetto non è necessario un previo accordo tra i concorrenti: è sufficiente, infatti, la coscienza unilaterale del contributo all'altrui condotta; non è peraltro necessario che l'autore della condotta tipica sia a conoscenza del contributo del concorrente.[199] In altre parole il concorso non presuppone un previo concerto né un particolare elemento soggettivo in capo all'autore materiale del reato. Il dolo di concorso è quindi indispensabile soltanto per il concorrente.

In relazione a questo secondo elemento, tuttavia, la giurisprudenza ritiene sufficiente che il concorrente si rappresenti il fatto nei suoi elementi costitutivi, non necessariamente in tutte le concrete modalità.[200] Ad esempio chi fornisce un'arma sapendo, anche nella forma

---

[195] I principali vantaggi riscontrati che sono stati ricondotti alla presenza dell'Hft nel mercato sono: i. l'aumento della liquidità a disposizione dei partecipanti al mercato; ii. la diminuzione del *bid-ask spread* medio; iii. la diminuzione dei costi di transazione; iv. l'aumento dell'efficienza informativa dei prezzi; v. l'aumento dei collegamenti *intermarket*. In merito si veda A. PUORRO, *High Frequency Trading: una panoramica, cit.*

[196] C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale*, *cit*., p. 553, G. FIANDACA, E. MUSCO, *Diritto penale parte generale*, *cit*., p. 522.

[197] Si veda §4.2.2.

[198] S. PROSDOCIMI, *Reato Doloso*, in *Digesto*, Wolters Kluwer, 1996, disponibile presso One Legale.

[199] A. TABOGA, *Dolo nel concorso di persone, commento a sentenza Cass, sez I, 1° agosto 2008, n. 32433,* in *Giurisprudenza italiana,* marzo 2009.

[200] *Ibidem*.

di dolo eventuale, che verrà utilizzata per un omicidio concorre nell'omicidio stesso. È irrilevante che non conosca il tempo, il luogo, le modalità concrete del delitto.

Sulla base di queste premesse, ci si potrebbe chiedere se il soggetto che programma un sistema di IA finalizzato all'attività di HFT e lo vende ad un soggetto utilizzatore possa essere ritenuto responsabile del reato previsto dall'art 185 TUF sulla base della funzione incriminatrice dell'art 110 c.p.

Per configurare la responsabilità concorsuale, dal punto di vista dell'elemento soggettivo, sarebbero necessari due elementi.

In primo luogo, il programmatore dovrebbe avere la consapevolezza di cooperare con l'autore del reato. Fornire la prova di questo elemento potrebbe essere più o meno complesso a seconda della specifica fattispecie concreta. Ovviamente sarà arduo negare il dolo di concorso in casi in cui l'utilizzatore abbia commissionato la realizzazione di un sistema di HFT con caratteristiche tali da poter apprendere dal mercato strategie abusive.

In secondo luogo, il programmatore dovrebbe volere, o almeno rappresentarsi, la commissione del reato. In questo caso l'elemento soggettivo del *designer* pone meno problemi rispetto a quello dell'utilizzatore.

È vero, infatti, che a causa dell'opacità dei modelli *black box*, il programmatore non ha la possibilità di prevedere il comportamento del sistema di IA,[201] ma ai fini della configurabilità concorso, come già è stato accennato, non è necessario che il concorrente si rappresenti le concrete modalità di esecuzione del reato.[202] Il *designer* sa di non poter prevedere il comportamento della macchina, ma sa anche che il sistema di IA molto probabilmente apprenderà dal mercato strategie manipolative e le metterà in atto per massimizzare i profitti.

A sostegno di questa tesi merita di essere citata una recente pronuncia relativa all'elemento soggettivo del concorrente in relazione al reato di strage. La Corte di Cassazione ha infatti ritenuto che "*Ai fini del concorso nel delitto di strage, è sufficiente un contributo limitato alla sola fase preparatoria e di organizzazione logistica del reato materialmente commesso da altri concorrenti, non occorrendo la conoscenza dell'identità di chi agirà, delle modalità esecutive della condotta e dell'identità della vittima, purché vi*

[201] Y. BATHAEE, *The Artificila Intelligence Black Box and the failure of intent and causation,* in *Harvard Journal of Law & Technology* Vol. 31, No. 2, 2018

[202] A. TABOGA, *Dolo nel concorso di persone, commento a sentenza Cass, sez I, 1° agosto 2008, n. 32433*, *cit*.

sia la consapevolezza dell'idoneità della propria azione a mettere in pericolo una pluralità di persone e del suo collegamento ad una più ampia progettazione delittuosa".[203]

Tale sentenza appare particolarmente interessante ai fini del presente lavoro poiché il delitto di strage, al pari di quello di manipolazione del mercato, è un reato di pericolo.

Si può quindi sostenere che, ai fini del concorso, non è necessario che il *designer* si rappresenti o voglia la singola operazione concreta, basta che sappia che l'utilizzatore attiverà la macchina mettendola quindi in condizione di effettuare operazioni manipolative.

Ovviamente ogni considerazione relativa alla responsabilità concorsuale del programmatore è legata alla sussistenza della responsabilità dell'utilizzatore.

Se infatti, come appare dai ragionamenti svolti nel precedente paragrafo, chi aziona la macchina difetta del dolo necessario a configurare il reato previsto dall'art 185 TUF, non realizza alcuna fattispecie di reato rispetto alla quale il programmatore potrebbe concorrere.

4.3 Le criticità sottese all'elemento soggettivo e le soluzioni proposte.

Nei precedenti paragrafi si è visto come le strategie realizzate da sistemi di HFT potrebbero rientrare nell'area di applicazione delle condotte manipolative previste dall'art. 185 TUF.

È stato tuttavia rilevato che in capo alle persone fisiche, teoricamente punibili per la commissione del fatto di reato, in realtà potrebbe difettare l'elemento soggettivo. Lo strumento utilizzato per la commissione del reato è infatti dotato di un'autonomia decisionale tale da escludere la possibilità di controllare e prevedere nel dettaglio il comportamento della macchina. Pertanto, si è sostenuto che, nell'impossibilità di ritenere sufficiente un "*dolo generale*" riferibile solamente ad eventuali e indefinite operazioni manipolative, l'utilizzatore potrà verosimilmente considerarsi privo dell'elemento soggettivo previsto dalla norma incriminatrice. In questo modo verrebbe meno anche l'ipotizzata responsabilità per concorso del soggetto programmatore.

Sul piano dell'offensività, tuttavia, non si può dubitare che alcune strategie messe in atto dai sistemi di HFT siano dotate di un'elevata idoneità lesiva del bene giuridico tutelato dalla norma. Si potrebbe anzi sostenere che, data l'alta velocità, la mole di operazioni

[203] Cass., sez. V, 5 maggio 2021, n. 40274, disponibile presso italgiure.giustizia.it. La sentenza riguarda la fattispecie relativa alla celebre strage di via D'Amelio.

realizzate e i possibili effetti distorsivi creati (si pensi ad esempio ai *flash crash*), una strategia manipolativa messa in atto da un operatore ad alta frequenza potrebbe creare squilibri di mercato perfino più rilevanti rispetto ad un comportamento realizzato da una persona fisica.[204]

Si tratta quindi di un fenomeno sicuramente offensivo, che tuttavia potrebbe non trovare un'adeguata risposta nella repressione penale a causa della complessità tecnologica senza precedenti dello strumento utilizzato.[205]

Si riscontra anche in questa specifica fattispecie la problematica, presentata in chiave generale nel primo capitolo, del *responsibility gap*.

Per colmare tale vuoto di tutela penalistica, sono state ipotizzate diverse soluzioni che hanno tentato di adattare, in modo più o meno forzato, gli istituti del diritto penale ai fini di risolvere tale problematica tecnologica senza precedenti.

4.3.1 *Strict liability*

Una prima soluzione, prospettata soprattutto dalla dottrina americana, è fondata su un meccanismo di imputazione basato sulla *strict liability*, assimilabile alla "responsabilità oggettiva" italiana.[206]

Questo tipo di responsabilità prevede che un soggetto possa, a determinate condizioni, rispondere di un fatto a prescindere dallo stato soggettivo che ne ha caratterizzato il compimento. In questo senso, si troverebbe una soluzione al *responsibility gap* che emerge in conseguenza all'elevata autonomia decisionale della macchina: la mancanza del dolo dell'agente umano non sarebbe rilevante.

Nel diritto americano la *strict liability* è un istituto che trova applicazione non soltanto nel diritto civile ma anche in alcuni limitati campi del diritto penale. Tra i differenti stati soggettivi che caratterizzano la cosiddetta *mens rea,* troviamo infatti anche la responsabilità oggettiva e quindi la mancanza di qualsiasi elemento soggettivo.[207] Tuttavia, nonostante tale

---

[204] A. AZZUTTI, W. G. RIING, H. S. STIHEL, *Machine learning, Market Manipulation and Collusion on capital markets why the "Black Box" matters*, *cit*.

[205] Tale problematica è trattata a livello generale in relazione all'utilizzo di sistemi di intelligenza artificiale nella commissione di fatti di reato da C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato, cit*., B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automazione artificiale, cit*.

[206] Y. BATHAEE, *The Artificial Intelligence Black Box and the failure of intent and causation, cit*.

[207] Ad esempio, negli Stati Uniti, il possesso di sostanze stupefacenti comporta una responsabilità penale a prescindere dalla consapevolezza dell'imputato di essere in possesso di tali sostanze. Si veda https://www.law.cornell.edu/wex/strict_liability

modello di imputazione in ambienti angloamericani sia ancora conosciuto e applicato, risulta comunque riservato a reati minori e appare destinato a progressivi ridimensionamenti.[208]

In ogni caso l'applicazione di una responsabilità di natura oggettiva nel nostro ordinamento risulta sicuramente inattuabile. La stessa Corte Costituzionale, infatti, attraverso la celebre pronuncia del 1988,[209] ha attribuito una rilevanza costituzionale al principio di colpevolezza, ancorandolo all'art 27 Cost. La concezione del fatto di reato come "proprio e colpevole" esclude quindi la compatibilità con la Costituzione di qualsiasi imputazione caratterizzata dalla mancanza dell'elemento soggettivo.[210]

Si è proceduto in questa direzione all'adattamento legislativo e giurisprudenziale di alcuni istituti (come l'evento preterintenzionale, alcune forme di *aberratio* o la responsabilità del concorrente per un reato diverso da quello voluto) che, elaborati in epoca pre-costituzionale, non rispecchiavano appieno il principio di colpevolezza in quanto basati sul brocardo "*qui in re illicita versatur, etiam tenetur pro casu*".[211]

É invece nell'ambito della responsabilità civile che i meccanismi di imputazione fondati sulla responsabilità oggettiva trovano una propria ragionevolezza. Tale istituto nasce proprio con l'avvento della società industriale ai fini ricomprendere in un'area risarcibile i danni cagionati da attività pericolose, di per sé non riconducibili ad un comportamento doloso o colposo.[212] In questo senso la responsabilità assume anche una funzione preventiva del danno, poiché il soggetto che viene individuato come responsabile avrà interesse ad evitarlo.

Proprio per questo motivo, tuttavia, alcuni autori escludono l'efficacia della responsabilità oggettiva, anche nell'ambito della responsabilità civile, nel caso in cui il danno venga cagionato da sistemi di IA sufficientemente avanzati. Infatti, secondo questa impostazione una responsabilità oggettiva avrebbe senso solo se il soggetto responsabile potesse prevedere in anticipo gli effetti dannosi del programma e agire preventivamente per evitarli. Tuttavia, come si è più volte affermato, il comportamento dei sistemi HFT è normalmente imprevedibile sia per l'utilizzatore che per il programmatore.[213]

---

[208] F. CONSULICH, *Flash Offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti*, *cit.*
[209] Corte Cost. n. 364/1988
[210] C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale*, *cit.*, p. 348.
[211] *Ibidem,* p. 425.
[212] V. ROPPO, *Diritto Privato*, Giappichelli, Torino, 2018, p.591.
[213] Y. BATHAEE, *The Artificial Intelligence Black Box and the failure of intent and causation, cit*.

4.3.2 *Actio libera in causa*

Alcuni autori hanno ipotizzato un'altra soluzione basata sul principio dell*'actio libera in causa*, secondo il quale risponderà ugualmente del reato commesso l'autore che si è volontariamente posto in uno stato di non imputabilità.[214]

Soprattutto in ambienti dottrinali angloamericani tale principio è elaborato in una concezione molto più ampia e si applica non solo a colui che si trovava al momento del fatto in uno stato di incapacità di intendere e di volere, ma anche a chi si è precostituito qualsiasi tipo di *defence*.[215]

In un certo senso, infatti, anche il caso in cui un soggetto si avvalga di un sistema di HFT dotato di un certo grado di autonomia e capacità di apprendimento per commettere un reato pone un problema di rimproverabilità *anticipata* dell'agente. L'elemento soggettivo che caratterizza il comportamento dell'agente non è più collocato temporalmente nel momento del fatto, ma in un momento precedente, ossia quando avviene l'attivazione della macchina e quindi all'inizio di un percorso offensivo che potrà svilupparsi in modo autonomo.[216]

Pertanto, si riscontra un'analogia rispetto al principio dell*'actio libera in causa*, soprattutto se questo viene inteso in senso ampio, come negli ambienti angloamericani. Anche in quel caso, il rimprovero può essere mosso in un momento precedente alla commissione del fatto di reato e non rileva l'impossibilità di individuare la colpevolezza durante la realizzazione della condotta tipica.[217]

L'ordinamento italiano, invece, ha formalizzato il principio dell*'actio libera in causa* attraverso articoli più specifici e caratterizzati da un campo applicativo maggiormente limitato. L'art 87 c.p. infatti esclude l'applicabilità della prima parte dell'art 85 c.p. (che sancisce la necessaria imputabilità dell'autore al momento del fatto) a "*chi si è messo in uno*

---

[214] F. CONSULICH, *Il Nastro Di Möbius. Intelligenza Artificiale e imputazione penale nelle nuove forme di abuso del mercato*, *cit.*, M. PALMISANO, *L'abuso di mercato nell'era delle nuove tecnologie. Trading algoritmico e principio di personalità dell'illecito penale*, in *Diritto Penale Contemporaneo*, n.2-2019.

[215] Ad esempio, la mancanza di *mens rea,* oppure le *excuses* o anche le *justification.* Per approfondimenti sulle tipologie di *defences* si veda www.law.cornell.edu

[216] F. CONSULICH, *Il Nastro Di Möbius. Intelligenza Artificiale e imputazione penale nelle nuove forme di abuso del mercato, cit.*

[217] *Ibidem.*

stato di incapacità di intendere e di volere al fine di commettere un reato o prepararsi una scusa".[218]

La dottrina italiana, inoltre ritiene che l'applicabilità di tale meccanismo di imputazione sia subordinata ad una perfetta corrispondenza tra il reato commesso e quello programmato: si esige quindi un nesso psichico e non una mera derivazione causale.[219]

Si ritiene pertanto che l'applicazione dell'istituto alle condotte di manipolazione del mercato realizzate attraverso sistemi di HFT trovi due fondamentali ostacoli.

Da una parte si prospetta un invalicabile limite normativo. Infatti, mentre nel panorama angloamericano l*'actio libera in causa* costituisce un principio generale di ascrizione di un fatto ad un soggetto che nel momento in cui agisce è assistito da qualsiasi tipo di *defence*, nell'ordinamento italiano l'art 87 c.p. vede la sua area di applicazione limitata al contesto della capacità di intendere e di volere. La forzata espansione del meccanismo di imputazione descritto costituirebbe senza dubbio un'analogia *in malam partem*.[220]

Un secondo limite sarebbe invece di natura soggettiva. Infatti, dato che l*'actio libera in causa*, come descritta dalla dottrina italiana, necessita di una perfetta identità tra il reato commesso (nello stato di incapacità) e quello programmato, verrebbe nuovamente alla luce la problematica relativa al dolo dell'utilizzatore di un sistema di intelligenza artificiale autonomo.[221]

In altre parole, anche seguendo la logica dell*'actio libera* in causa l'agente dovrebbe comunque rappresentarsi (al momento dell'azionamento della macchina) la concreta operazione manipolativa.

Pertanto, la soluzione analizzata, per lo meno nell'ordinamento italiano, non risulta affatto risolutiva.

---

[218] Lo stesso principio è individuabile anche nell'art. 92 c.p. e nell'art 93 c.p. in relazione rispettivamente allo stato di ubriachezza volontaria e allo stato di assunzione di sostanze stupefacenti. Non sembra invece riconducibile allo schema dell*'actio libera in causa* l'ubriachezza colposa (sempre disciplinata dall'art 92 c.p.) poiché in questo caso non vi è un iniziale volontà di commettere il reato. In merito si veda R. VENDITTI, *Actio libera in causa (I,1958)*, in *Enc. Dir.*, Giuffrè.

[219] G. FIANDACA, E. MUSCO, *Diritto penale parte generale*, cit., p. 359.

[220] F. CONSULICH, *Il Nastro Di Möbius. Intelligenza Artificiale e imputazione penale nelle nuove forme di abuso del mercato, cit*.

[221] *Ibidem.*

4.3.3 Responsabilità indiretta

Un ulteriore tentativo di colmare il *responsibility gap* derivante dall'utilizzo di sistemi IA nel compimento di abusi di mercato consiste nell'utilizzare un modello di responsabilità vicaria, sulla base del paradigma del *respondeat superior*.[222]

Tale principio è stato elaborato dalla dottrina e dalla giurisprudenza americana in relazione all'*agency law*, ossia al settore del diritto che si occupa dei rapporti di agenzia. Questo tipo di responsabilità vicariale prevede che un soggetto principale, il quale si serve di un altro soggetto per il compimento dei propri affari o per lo svolgimento del suo lavoro, risponda degli illeciti commessi da quest'ultimo.[223]

Parte della dottrina americana ha quindi suggerito l'applicazione di questo modello di imputazione ai reati di abuso di mercato commessi da sistemi di HFT. Secondo questa teoria, il sistema di IA costituirebbe una forma nuova e inedita di agente. Infatti, quando il sistema di IA prende decisioni e opera in modo autonomo è indistinguibile da un essere umano che trova nuove soluzioni per raggiungere l'obbiettivo fissato dal superiore. Inoltre, anche l'agente umano, proprio come l'agente artificiale, può comportarsi in modo imprevedibile.[224]

Ovviamente tale modello di imputazione nel nostro ordinamento causerebbe inevitabili frizioni con il principio di colpevolezza, risultando di conseguenza contrario alla Carta Costituzionale.[225]

Nell'ordinamento penale italiano, sono comunque presenti alcuni istituti che sembrano utilizzare un modello di responsabilità in senso lato vicariale, riconducibile alla figura dell'"autore mediato".[226] Con questo termine, elaborato dalla dottrina tedesca, ci si riferisce a colui che per il compimento di un reato si serve della condotta di un'altra persona, non imputabile o non punibile.[227] Il Codice Penale italiano prevede diverse figure riconducibili a questo schema. Si pensi ad esempio all'art. 86 c.p. punisce la determinazione in altri dello

---

[222] F. CONSULICH, *Flash Offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti, cit.*
[223] Y. BATHAEE, *The Artificial Intelligence Black Box and the failure of intent and causation, cit.*
[224] *Ibidem*.
[225] Si tratta delle medesime problematiche analizzate in precedenza in relazione alla responsabilità oggettiva. Si veda §4.3.1.
[226] C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale*, *cit.*, p.553.
[227] M. SINISCALCO, *Autore Mediato (dir. pen) (IV)*, in *Enc. Dir.,* 1959

stato d'incapacità allo scopo di far commettere un reato,[228] oppure all'art 111 c.p. che punisce chi ha determinato a commettere un reato una persona non imputabile o non punibile.[229]

Tuttavia, ritenere che l'azionamento del sistema di HFT da parte dell'utilizzatore possa costituire uno schema simile a quello descritto negli articoli menzionati implica un'analogia logicamente scorretta. L'agente artificiale, infatti, almeno per il momento, non è dotato di una soggettività giuridica propria e non può essere assimilato ad un soggetto non imputabile.[230] Pertanto non può concorrere con la persona fisica, nemmeno attraverso le peculiari modalità previste dalle due fattispecie descritte.[231]

Potrebbe invece trovare un'applicazione più lineare un altro tipo di responsabilità vicariale, ossia la responsabilità della persona giuridica in relazione ad un fatto di reato compiuto nel suo interesse o vantaggio. In questo caso, infatti, tra l'ente e l'agente algoritmico si pone una persona fisica che si avvale di quest'ultimo.[232]

4.3.4 Interpretazione estensiva dell'art. 8 del d.lgs. 231/2001

Una diversa soluzione prospettata dalla dottrina è stata quella di applicare un altro tipo di responsabilità vicariale, ossia la responsabilità dell'ente.[233]

Il legislatore italiano ha infatti disciplinato con il d.lgs. 231/2001 un modello di responsabilità della persona giuridica per fatto di reato. Si tratta di una responsabilità formalmente amministrativa[234] che nasce in conseguenza alla commissione di determinati

---

[228] L'art. 86 c.p. recita*: "Se taluno mette altri nello stato di incapacità di intendere o di volere, al fine di fargli commettere un reato, del reato commesso dalla persona resa incapace risponde chi ha cagionato lo stato d'incapacità."*

[229] L'art. 111 c.p. (Determinazione al reato di persona non imputabile o non punibile) recita: "*Chi ha determinato a commettere un reato una persona non imputabile, ovvero non punibile a cagione di una condizione o qualità personale, risponde del reato da questa commesso; e la pena è aumentata."*

[230] F. CONSULICH, *Flash Offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti, cit.*

[231] *Ibidem.*

[232] *Ibidem.*

[233] F. CONSULICH, *Il Nastro Di Möbius. Intelligenza Artificiale e imputazione penale nelle nuove forme di abuso del mercato*, *cit.*

[234] Molti autori hanno sostenuto che la responsabilità da reato degli enti abbia in realtà una natura sostanzialmente penale. Vi sono infatti numerosi elementi a favore di questa tesi. Innanzitutto, tale responsabilità sorge in conseguenza alla commissione di un illecito di natura penale, quindi sembra ragionevole che la responsabilità che ne consegue sia di natura penalistica. In secondo luogo, l'autorità competente a svolgere le indagini preliminari ed esercitare l'azione penale è il pubblico ministero e la contestazione dell'illecito avviene ai sensi dell'art. 59 del d.lgs.231/2001 in uno degli atti indicati dall'art 405 comma 1 c.p.p. Inoltre, il procedimento avviene, seppur con regole, speciali, all'interno del procedimento penale relativo al reato presupposto, terminando con una sentenza del giudice penale. È stato argomentato che la natura sostanzialmente penalistica della responsabilità dell'ente derivi anche dalla particolare afflittività delle sanzioni previste che, oltre ad incidere direttamente sul patrimonio dell'ente, possono interessare anche la sua libertà

tipi di reati; tra questi sono presenti anche i delitti di manipolazione del mercato e abuso di informazioni privilegiate, disciplinati dal TUF.[235]

Come noto, la responsabilità dell'ente sorge solo in presenza di determinate condizioni: occorre che il reato venga compiuto da una persona fisica appartenente all'ente (soggetti in posizione apicale o sottoposti) e nel suo interesse o vantaggio.[236]

La dottrina e la più recente giurisprudenza sostengono inoltre che per fondare la responsabilità dell'ente occorra anche un elemento ulteriore, ossia la "colpa di organizzazione".[237] In questo senso la persona giuridica è sanzionabile solo quando non abbia adottato ed efficacemente attuato modelli organizzativi idonei a prevenire la commissione del reato; si esige quindi che il comportamento criminoso posto in essere dalla persona fisica costituisca attuazione della politica aziendale o comunque derivi da una colpa di organizzazione.[238]

Anche se subordinata alla commissione di un reato da parte di una persona fisica, la responsabilità dell'ente si prospetta come autonoma. L'art. 8 del d.lgs. 231/2001 infatti prevede alcune situazioni rispetto alle quali tale responsabilità permane nonostante il processo penale della persona fisica non possa avere corso. In particolare, quando "*l'autore del reato non è stato identificato o non è imputabile"* oppure quando "*il reato si estingue per una causa diversa dall'amnistia."*

Sulla base di questo articolo, parte della dottrina ha elaborato un principio secondo il quale, ai fini della responsabilità dell'ente, non sarebbe necessario che il reato presupposto risulti completo di tutti gli elementi costitutivi, quindi anche dell'elemento soggettivo dell'agente, essendo invece sufficiente la realizzazione di un *fatto di reato*.[239] Tale assunto potrebbe fornire una soluzione al vuoto di tutela penalistica legato alla fattispecie in esame. Se infatti la persona fisica che utilizza il sistema di HFT per commettere il reato di manipolazione del mercato risultasse esente da responsabilità a causa della mancanza del

---

d'azione nel caso di sanzioni interdittive. Su questo tema si veda G. DE SIMONE, *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) d'imputazione*, in *Diritto Penale Contemporaneo*, 2012.

[235] Art. 25-*sexies* dlgs. 231/2001. In merito si veda inoltre A. GALANTI, *La manipolazione del mercato*, *cit*., p.133.

[236] Art 5 dlgs. 231/2001.

[237] MAZZACUVA, E. AMATI, *Diritto Penale dell'Economia, cit*, p. 39.
In relazione alla giurisprudenza questo indirizzo appare ormai consolidato: si veda, tra le altre, la recente pronuncia: Cass., Sez. IV, 11 gennaio 2023, n. 570, disponibile presso www.sistemapenale.it

[238] *Ibidem.*

[239] F. CONSULICH, *Il Nastro Di Möbius. Intelligenza Artificiale e imputazione penale nelle nuove forme di abuso del mercato, cit.*

dolo, il disvalore del fatto potrebbe essere comunque riversato sulla persona giuridica attraverso tale meccanismo imputativo.[240]

Occorre quindi soffermarsi sugli argomenti che hanno indotto alcuni autori ad affermare una tale estensione del principio di autonomia.

L'articolo 8, oltre all'ipotesi meno problematica di estinzione del reato, cita altri due casi in cui la responsabilità dell'ente sopravvive a quella della persona fisica.

Il primo riguarda l'ipotesi in cui l'autore del reato non venga identificato. In questa situazione, provata ovviamente l'appartenenza all'ente della persona fisica, è possibile che venga almeno identificato l'ufficio o comunque il livello gerarchico di organizzazione all'interno del quale l'autore del reato era inserito. Nel primo caso l'art. 8 sembra operare in modo abbastanza lineare poiché, pur non conoscendo l'identità di chi ha commesso il fatto, si sa se egli ricoprisse una posizione apicale o subordinata; pertanto, si applicherà il rispettivo regime probatorio previsto dagli art. 6 o 7 del d.lgs. 231/2001. Se invece non si conoscesse nemmeno la collocazione all'interno dell'organizzazione aziendale del soggetto si potrebbe sostenere che l'art. 8 non possa operare poiché non sarebbe in alcun modo identificabile il regime di responsabilità a cui dovrebbe essere sottoposto l'ente.[241] Una parte della dottrina, ha ritenuto invece che, nei casi di autore non identificato, l'art. 8 assuma un vero e proprio ruolo fondante della responsabilità dell'ente, autonoma rispetto a quella della persona fisica. In tale senso la stessa mancata individuazione del responsabile umano costituisce una manifestazione dell'organizzazione antidoverosa della persona giuridica e quindi di una colpa di organizzazione che si pone su un piano diverso e indipendente dal dolo o dalla colpa che nutrono l'imputazione della persona fisica. [242]

Appare particolarmente interessante, ai fini del presente lavoro, il secondo caso previsto dall'art. 8 del d.lgs. 231/2001: la non imputabilità della persona fisica.

Sulla base di una rigorosa interpretazione letterale, si dovrebbe concludere che la mancanza di imputabilità debba essere intesa come "incapacità di intendere e di volere" sulla base dell'art 85 c.p. Tuttavia, parte della dottrina sostiene che in contesti come quello dei reati economici, o di altri reati complessi nell'ambito di organizzazioni, appare alquanto

[240] *Ibidem*

[241] C. PECORELLA, *Principi generali e criteri di attribuzione della responsabilità*, *in La responsabilità amministrativa degli enti*, Milano, 2002, p. 81.

[242] F. CONSULICH, *Il principio di autonomia della responsabilità dell'ente, prospettive di riforma dell'art 8*, *cit.*

improbabile l'ipotesi in cui un soggetto realizzi il fatto, ad esempio, in uno stato di alterazione psicofisica. Tali autori hanno quindi sostenuto che il legislatore, non intendendo disciplinare un caso così residuale, abbia invece utilizzato il termine "imputabilità" in senso lato, con il significato di "colpevolezza".[243]

D'altra parte, il fatto che lo stesso art. 8 preveda il caso della mancata identificazione dell'autore del reato, secondo parte della dottrina potrebbe affrancare la tesi per cui la quale non sarebbe necessaria la prova della colpevolezza della persona fisica. Se infatti l'autore è ignoto, appare estremamente difficile riuscire a provare l'elemento soggettivo, in particolare il dolo.[244]

Un ulteriore argomento a sostegno di questa tesi si basa su una particolare concezione dell'intero sistema di responsabilità dell'ente. Alcuni autori hanno infatti riconosciuto nel modello di responsabilità previsto per l'ente un meccanismo estensivo della punibilità simile a quello previsto dall'art 110 c.p. in ambito di concorso tra persone fisiche. In questo senso si potrebbe interpretare il sistema come una sorta di fattispecie a concorso necessario in cui si impone una partecipazione dell'ente e un suo contributo alla realizzazione del fatto di reato che si estrinseca nella citata "colpa di organizzazione", che avrebbe per lo meno una funzione agevolatrice.[245] L'art. 8 del d.lgs. 231/2001 sembrerebbe quindi replicare alcuni meccanismi normativi previsti nell'ambito dell'ordinario concorso di persone dagli art. 111 e 112 c.p.. Anche in questi casi, infatti, è necessaria l'integrazione di un reato, inteso come in un fatto materiale tipico e illecito, ma non la colpevolezza dell'autore e quindi l'antigiuridicità del fatto.

Sulla base di queste considerazioni parte della dottrina ha quindi sostenuto che, ai fini della configurabilità della responsabilità dell'ente, nell'ambito dell'imprescindibile accertamento del reato della persona fisica, tale elemento deve essere inteso come "obbiettiva realizzazione di una condotta illecita", e quindi come la commissione di un "fatto antigiuridico", mentre non è necessaria la verificazione della dimensione psicologica dell'agente.[246]

---

[243] *Ibidem.*

[244] *Ibidem.*

[245] C.E. PALIERO, *La responsabilità penale della persona giuridica nell'ordinamento italiano: profili sistematici*, in *Societas puniri potest - La responsabilità da reato degli enti collettivi* (atti del convegno organizzato dalla Facoltà di giurisprudenza e dal Dipartimento di diritto comparato e penale dell'Università di Firenze, 15-16 marzo 2002), Cedam, Padova, 2003, p. 17.

[246] F. CONSULICH, *Il principio di autonomia della responsabilità dell'ente, prospettive di riforma dell'art 8, cit.*

Appare in ogni caso doveroso evidenziare che un'altra parte della dottrina esclude tale interpretazione dell'art. 8.[247] Secondo questo orientamento, infatti, il principio di autonomia della responsabilità dell'ente consentirebbe di prescindere dall'identificazione dell'autore fisico, ma non dalla commissione del fatto di reato completo in tutti i suoi elementi oggettivi e soggettivi. Occorrerebbe pertanto distinguere tra mancata identificazione del soggetto responsabile e assenza di un fatto tipico di reato, in particolare se doloso. Altrimenti, si potrebbe incorrere nel pericolo di ascrivere la responsabilità per un reato doloso ad un soggetto (la persona giuridica), pur nell'impossibilità di individuare in qualsiasi soggetto fisico l'elemento del dolo quale coefficiente psichico reale.[248]

Al di là del citato dibattito dottrinale, un'interpretazione estensiva dell'art 8 e un'applicazione in senso lato del principio di autonomia della responsabilità della persona fisica sembra, *de iure condito*, la soluzione più convincente in relazione alla problematica al centro del presente lavoro.

Nell'ambito del reato di manipolazione del mercato, infatti, sanzionare l'organizzazione all'interno della quale viene commesso il reato, appare certamente una soluzione efficace.

Il ricorso all'8 del d.lgs. 231/2001 permetterebbe di comminare sanzioni effettive, in situazioni in cui, altrimenti, si potrebbe creare un vuoto di tutela penalistica.[249]

In questi termini, l'interpretazione precedentemente esposta, se accolta, potrebbe fornire una soluzione per i casi in cui, a causa della complessità del reato, dello strumento utilizzato, o di altre circostanze non sia possibile attribuire una responsabilità penalistica alla persona fisica che ha realizzato una fattispecie criminosa nell'ambito dell'organizzazione di una persona giuridica.[250]

---

[247] G. DE VERO, *La responsabilità penale delle persone giuridiche, IV, Trattato di diritto penale. Parte generale*, Giuffré Milano, p. 204, N.M. MASULLO, *Colpa penale e precazione nel segno della complessità*, Edizioni Scientifiche Italiane, Napoli, 2012, p.234.

[248] M. PALMISANO, *L'abuso di mercato nell'era delle nuove tecnologie. Trading algoritmico e principio di personalità dell'illecito penale*, *cit*.

[249] F. CONSULICH, *Il principio di autonomia della responsabilità dell'ente, prospettive di riforma dell'art 8, cit.*

[250] Oltre ai reati commessi attraverso sistemi di IA, si pensi ad esempio ai reati ambientali nei quali spesso alla frammentazione della condotta in un ampio lasso tempo si unisce un aspetto multifattoriale relativo all'evento dannoso. *Ibidem.*

Pertanto, alcuni autori sostengono che l'art 8 potrebbe assumere "*una funzione preventiva d'avanguardia proprio nei contesti più avveniristici del reato economico, consentendo l'intervento penalistico rispetto alle ipotesi di irresponsabilità organizzata*".[251]

[251] F. CONSULICH, *Il Nastro Di Möbius. Intelligenza Artificiale e imputazione penale nelle nuove forme di abuso del mercato*, *cit*.

CAPITOLO V
LE PROSPETTIVE DE IURE CONDENDO

SOMMARIO: 5.1 – I possibili interventi del legislatore italiano – 5.2 Un approccio precauzionale: sanzioni penali o amministrative a tutela di Mifid II e (eventualmente) della Proposta di Regolamento sull'IA – 5.3 Un altro volto dell'Intelligenza Artificiale: sistemi di IA utilizzati per rintracciare gli abusi di mercato – 5.4 Conclusioni

5.1 I possibili interventi del legislatore italiano

Si è precedentemente visto come l'applicazione dei nuovi e più avanzati sistemi di IA possa mettere in crisi i tradizionali precetti del diritto penale. In particolare, l'utilizzo di sistemi di HFT per la realizzazione di operazioni manipolative potrebbe comportare un vuoto di tutela penalistica, almeno per quanto riguarda la persona fisica.

Per ovviare a tale problema, in un'ottica *de iure condendo*, si potrebbero immaginare diverse soluzioni adottabili dal legislatore italiano sia nell'ambito della manipolazione del mercato, sia, più in generale, in tutte le aree di applicazione dell'intelligenza artificiale che presentino problemi analoghi.

Una prima opzione potrebbe essere quella di inserire una fattispecie colposa di evento in relazione al bene tutelato dall'attuale art. 185 TUF. Si è visto, infatti, come l'aspetto che sostanzialmente esclude la responsabilità penale della persona fisica sia la mancanza del dolo in relazione al compimento delle operazioni: la volontà e la rappresentazione dell'agente, per effetto del comportamento autonomo della macchina potrebbero solo arrestarsi ad una soglia di *dolus generalis*, come noto, insufficiente nel nostro ordinamento.[1]

Ci si potrebbe peraltro chiedere se le problematiche legate alla *black box* algoritmica possano mettere in crisi anche un ipotetico meccanismo di imputazione colposo.

Occorre premettere che la colpa nel diritto penale può essere definita come la causazione di un fatto vietato dalla legge penale attraverso la violazione di regola cautelari, codificate o meno.[2] L'evento che si causa colposamente non è voluto, e può, solo

[1] F. CONSULICH, *Il Nastro Di Möbius. Intelligenza Artificiale e imputazione penale nelle nuove forme di abuso del mercato*, Banca Borsa e Titolo di Credito, n. 2, 2018, p. 195.
[2] C. PIERGALLINI, *Colpa (diritto penale)*, Annali X, Enciclopedia del diritto, 2017.

eventualmente, essere previsto dall'agente.[3] Inoltre per fondare un rimprovero colposo occorrerà provare la prevedibilità e l'evitabilità dell'evento cagionato.[4]

Pertanto, nel caso dell'utilizzazione di un sistema di IA, si potrebbe ipotizzare una responsabilità colposa della persona fisica per la creazione o per l'utilizzazione della macchina, nel caso in cui "*lo specifico evento storico appartenga alla classe di eventi dannosi che potevano essere ipotizzati al momento della creazione del sistema intelligente*".[5]

In relazione allo specifico campo di analisi del presente lavoro, si potrebbe aggiungere che se l'alterazione del mercato venisse causata da un sistema di HFT non adeguatamente testato, o non conforme ai requisiti previsti da Mifid II in relazione all'accesso al mercato oppure non sufficientemente monitorato, allora potrebbe prospettarsi una colpa specifica per violazione di norme cautelari.

Emerge in ogni caso un importante aspetto: l'impossibilità di prevedere *ex ante* le specifiche operazioni che il sistema di HFT effettuerà (fattore che rende inapplicabile il reato doloso) non rileva ai fini della responsabilità colposa, poiché in questo caso è sufficiente che il fatto di reato sia riconducibile ad un *genus* di eventi considerati *ex ante* dalla norma cautelare violata.[6]

Parte della dottrina, tuttavia, ritiene che in virtù dei principi di proporzionalità e offensività caratteristici del diritto penale, gli interessi potenzialmente lesi dai reati di natura economica (e in particolare dagli abusi di mercato[7]) non siano meritevoli di tutela laddove lesi da un'aggressione colposa.[8] Secondo questa visione, il reato colposo sarebbe più confacente ai casi in cui le conseguenze lesive del fatto riguardino interessi personalistici; la lesione di interessi patrimoniali, per quanto collettivi, non appare infatti sufficiente a giustificare una responsabilità per colpa.

---

[3] Art 43 c.p.

[4] C.F. GROSSO, M. PELISSERO, D. PERTINI, P. PISA, *Manuale di Diritto Penale Parte Generale*, Giuffrè, Milano 2020, p. 386.

[5] Tale prospettiva è ipotizzata, in relazione al fenomeno generale dei sistemi di IA utilizzati nella commissione di reati, da F. CONSULICH, *Flash Offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti*, in *Riv. it. dir. e proc. pen*., n.3, 2022, p.1015.

[6] L. ROMANÒ*, La responsabilità penale al tempo di chatgpt: prospettive de iure condendo in tema di gestione del rischio da intelligenza artificiale generativa*, in *Sistema Penale*, 2023.

[7] Le pene previste dagli articoli 184 e 185 TUF, appaiono molto severe in relazione alle fattispecie previste, specialmente a seguito del raddoppio selle sanzioni sancito dall'art 39 comma 1 della l. n. 262/2005.

[8] F. CONSULICH, *Flash Offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti, cit.*

Una diversa soluzione potrebbe consistere nell'inserimento di fattispecie di pericolo che puniscano la mancata realizzazione di una rete protettiva in relazione all'utilizzo del sistema di IA. Si tratterebbe quindi di reati colposi di mera condotta imperniati sull'omessa predisposizione o sulla rimozione di adeguate cautele idonee a contenere le scelte devianti della macchina.[9]

L'ordinamento penalistico italiano conosce già questo tipo di reati. Ne costituisce un esempio l'art 437 c.p.[10] in relazione alla sicurezza sul lavoro. Si tratta di un reato di condotta, aggravato dall'evento, che punisce la rimozione o l'omissione (in questo caso dolosa) di cautele contro gli infortuni sul lavoro.

In relazione alle manipolazioni del mercato realizzate attraverso sistemi di IA, si potrebbe immaginare una norma costruita in modo simile. In questo caso, la disposizione in questione potrebbe punire chi omette di inserire opportuni "blocchi" per evitare che il sistema, una volta operativo nel mercato, apprenda e realizzi autonomamente strategie manipolative.[11]

In questo modo verrebbero meno le problematiche legate alla *black box* e all'elemento soggettivo poiché il rimprovero che potrebbe essere mosso all'agente si collocherebbe, a livello logico e temporale, in un momento separato dall'operatività della macchina e non sarebbe affatto influenzato dalle dinamiche decisionali autonome del sistema di IA.

Un ulteriore esempio di una norma strutturata in questo modo è l'art. 615-*quater*, il quale punisce chi "*al fine di procurare a se' o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce*

---

[9] *Ibidem*.

[10] L'art. 437 c.p. (Rimozione od omissione dolosa di cautele contro gli infortuni sul lavoro) recita: *"Chiunque omette di collocare impianti, apparecchi o segnali destinati a prevenire disastri o infortuni sul lavoro, ovvero li rimuove o li danneggia, è punito con la reclusione da sei mesi a cinque anni.*
Se dal fatto deriva un disastro o un infortunio, la pena è della reclusione da tre a dieci anni."

[11] Si è precedentemente osservato (§3.2.3) come alcuni studi empirici abbiano dimostrato che se il sistema di apprendimento della macchina è basato sul *backtesting* (e non sull'elaborazione di dati che ricava in tempo reale dal mercato), l'HFT non ha la possibilità di imparare e realizzare autonomamente strategie manipolative. T. MIZUTA, *Does an Artificial Intelligence Perform Market Manipulation with Its Own Discretion? – A Genetic Algorithm Learns in An Artificial Market Simulation*, SPARX Asset Management Co. Ltd., Tokyo, 2020.

indicazioni o istruzioni idonee al predetto scopo".[12] Anche in questo caso si tratta di un reato di pericolo, con funzione anticipatrice della tutela, il quale punisce diverse condotte preliminari alla commissione di un reato più grave.

La struttura dell'art 615-*quater* potrebbe essere utilmente impiegata nella predisposizione di fattispecie di manipolazione del mercato effettuate attraverso l'HFT. In questi casi le problematiche penalistiche legate alla *black box* potrebbero essere risolte mediante l'anticipazione della soglia di punibilità alla sola "detenzione, produzione o diffusione" di sistemi di HFT potenzialmente in grado di effettuare operazioni manipolative.

5.2 Un approccio precauzionale: sanzioni penali o amministrative a tutela di Mifid II ed (eventualmente) della Proposta di Regolamento sull'IA

Il fenomeno dell'HFT è stato interessato da un'attenta regolamentazione contenuta nella direttiva 2014/65/UE (Mifid II).

Come è stato precedentemente esposto,[13] Mifid II, oltre a disciplinare gli aspetti relativi all'accesso al mercato degli operatori algoritmici, inserisce anche una normativa concernente un'attività di monitoraggio degli algoritmi. In particolare, tale direttiva pone a carico delle imprese di investimento l'obbligo di disporre controlli idonei a prevenire il malfunzionamento dei sistemi ed evitare che possano essere utilizzati per finalità contrarie al MAR.[14] Inoltre, è imposto alle sedi di negoziazione di adottare procedure idonee a testare i sistemi di IA e verificare che essi non possano turbare lo svolgimento delle contrattazioni o alterare il regolare funzionamento del mercato.[15] Le sedi di negoziazione hanno l'obbligo registrare l'attività e conservare i dati per cinque anni.[16]

Le misure descritte agiscono quindi in un'ottica preventiva, in quanto finalizzate a limitare il più possibile l'inevitabile rischio derivante dall'utilizzo massivo di sistemi di HFT nei mercati.

---

[12] Art. 615-*quater*. *(Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici)*
[13] Si veda § 2.4
[14] Art 17 Direttiva 2014/65/UE (Mifid II).
[15] Art 48 Direttiva 2014/65/UE (Mifid II).
[16] Divisione Mercati, Ufficio Vigilanza Infrastrutture di Mercato, CONSOB, *Mappatura delle sedi di negoziazione in Italia dopo l'entrata in vigore di MiFID II/MiFIR*, ottobre 2018.

Segue una logica simile, per quanto riguarda in generale i sistemi di IA, la citata proposta di Regolamento Europeo sull'Intelligenza Artificiale.[17] La disciplina dettata dal Regolamento per i "sistemi ad alto rischio" prevede infatti una serie di obblighi che il produttore dei sistemi di IA deve rispettare, sia nella fase di programmazione che di addestramento e convalida.[18] Inoltre, tali sistemi devono essere progettati in modo tale da poter essere "*efficacemente supervisionati da persone fisiche durante il periodo in cui il sistema è in uso*".[19] È infine previsto, oltre ad un dettagliato sistema di certificazioni, anche un obbligo di monitoraggio successivo all'immissione sul mercato.

In realtà, il Regolamento IA non prevede all'interno della categoria dei sistemi IA "ad alto rischio" quelli utilizzati per operare sui mercati finanziari. Probabilmente la già dettagliata disciplina contenuta in Mifid II e nel MAR è stata ritenuta sufficiente. Occorre tuttavia evidenziare che queste fonti, già ritenute da alcuni autori di per sé inadeguate a contrastare fenomeni abusivi realizzati con sistemi di HFT,[20] non forniscono alcuna indicazione o *standard* relativo alla fase di programmazione dei sistemi. Si potrebbe quindi ipotizzare, in un'ottica *de iure condendo*, l'inserimento dei sistemi IA utilizzati per il *trading* ad alta frequenza all'interno della categoria dei "sistemi ad alto rischio" del Regolamento.

Sulla base delle considerazioni svolte, si potrebbe affermare che il panorama normativo descritto in Mifid II (ed eventualmente nella proposta di Regolamento Europeo sull'IA) ricalchi un modello di disciplina tipico di settori complessi caratterizzati da un certo grado di rischio. Vi sono infatti dettagliate norme riguardanti procedure, obblighi, certificazioni che sono finalizzate a ridurre il più possibile l'area del "rischio consentito".[21]

A tal proposito può essere opportuno evidenziare che in altri settori, come quello relativo alla sicurezza sul lavoro o alla tutela ambientale[22], il legislatore italiano è intervenuto con sanzioni amministrative o penali (generalmente di natura contravvenzionale) a tutela del

[17] Si veda § 1.1.2

[18] Art. 9 *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione*, 2021, eur-lex.europa.eu

[19] Art 14 *ibidem*.

[20] T. ČUK, A. VAN WAEYENBERGE, *European Legal Framework for Algorithmic and High Frequency Trading (Mifid 2 and MAR), A Global Approach to Managing the Risks of the Modern Trading Paradigm,* in Cambridge University Press, Cambridge, 2018.

[21] In relazione alla tematica del rischio consentito, già affrontata all'interno del presente lavoro al paragrafo 1.1.2 lett. a), si veda F. CONSULICH, *Rischio Consentito,* in *Enc. dir*, Giuffrè, 2021, p.1102 ss.

[22] Si pensi ad esempio al d.lgs. 81/2008 (Testo Unico in materia di sicurezza e salute nei luoghi di lavoro) o al d.lgs. 152/2006 (Testo Unico in materia ambientale). Entrambi sono strutturati su una comune tecnica legislativa che prevede un dettagliato impianto di obblighi, procedure e prescrizioni seguito poi da disposizioni di carattere sanzionatorio (sia sul piano amministrativo che penale) per la violazione di tali norme.

rispetto delle suddette norme di carattere precauzionale. Si è infatti deciso di anticipare la tutela alla semplice violazione di quelle disposizioni finalizzate ad evitare la verificazione di eventi dannosi.[23]

Lo stesso articolo 187-*ter*.1 del TUF utilizza la medesima tecnica, prevedendo sanzioni amministrative per la violazione di determinate disposizioni contenute nel MAR, le quali non riguardano però la contrattazione algoritmica ma obblighi o divieti propedeutici ad impedire, a monte, la commissione di abusi di mercato.[24]

Si potrebbe quindi immaginare di adottare questa consolidata tecnica legislativa anche in relazione al fenomeno oggetto del presente lavoro, inserendo sanzioni penali o amministrative a tutela di quelle disposizioni di Mifid II (ed eventualmente anche del Regolamento Europeo sull'IA) propedeutiche alla riduzione del rischio connesso all'utilizzo di sistemi di IA per la contrattazione ad alta frequenza.

Tale strategia avrebbe l'indubbio vantaggio di evitare i problemi relativi al *responsibility gap* derivanti dall'imprevedibilità algoritmica tipica dei modelli *black box*. Infatti, la sanzione penale in questi casi interverrebbe in un momento precedente in cui, non solo la persona fisica non ha ancora effettivamente utilizzato la macchina, ma addirittura il sistema di IA potrebbe non essere ancora stato completato e reso operativo.

Nelle situazioni in cui, per circostanze riconducibili alle peculiarità del caso concreto, le risultanze probatorie siano tali da rendere indiscutibile la prova del dolo dell'utilizzatore, potrebbe ugualmente essere applicato l'art 185 TUF.[25] Tuttavia, nel caso in cui non venga raggiunta tale prova, il settore in esame potrebbe comunque beneficiare di una tutela penalistica (o punitivo- amministrativa) fondata su un eventuale mancato adempimento, a monte, di una serie di prescrizioni finalizzate ad evitare il rischio di verificazione dell'evento dannoso.

5.3 Un altro volto dell'intelligenza artificiale: sistemi di IA utilizzati per rintracciare gli abusi di mercato

[23] I. SCORDAMAGLIA, *Il diritto penale della sicurezza sul lavoro tra principi di prevenzione e precauzione*, in *Diritto Penale Contemporaneo*, 2012.
[24] Gli articoli del MAR interessati sono: l'art. 16 (Prevenzione e individuazione di abusi di mercato), l'art. 17 (Comunicazione al pubblico di informazioni privilegiate) e l'art. 18 (Elenchi delle persone aventi accesso a informazioni privilegiate)
[25] Si pendi ad esempio al precedentemente citato caso "Coscia".

Si è visto come l'incredibile evoluzione tecnologica abbia portato alla creazione di sistemi di IA dotati di un grado di autonomia tale da mettere in crisi i tradizionali paradigmi del diritto penale.[26] Inoltre, nell'ambito finanziario, l'estrema velocità e autonomia degli operatori algoritmici ad alta frequenza, costituiti appunto da sistemi di IA, hanno reso l'andamento dei mercati sempre più imprevedibile.[27]

Risulta opportuno, tuttavia, considerare che la creazione di sistemi di intelligenza artificiale costituisce un avanzamento tecnologico senza precedenti e che, nella società contemporanea, strumenti di questo tipo sono estremamente utili, se non indispensabili, per analizzare le grandi quantità di dati prodotti e registrati nei più svariati settori.

Per quanto riguarda i mercati finanziari, da tempo ci si avvale di algoritmi per classificare e analizzare i dati. Negli ultimi anni, tuttavia, le autorità di regolamentazione, le banche e le Borse di tutto il mondo hanno investito in maniera cospicua nello sviluppo di sistemi sempre più avanzati di sorveglianza e controllo dei mercati.

Ad esempio, già dal 2017 l'*Autoritè des Marchés Financiers* (AMF) francese ha reso operativa una piattaforma di supervisione del mercato, denominata ICY, che tramite la tecnologia di IA permette all'Autorità di elaborare in modo rapido ed efficiente grandi volumi di dati strutturati e non.[28]

I gestori delle piattaforme di negoziazione e le autorità nazionali di regolamentazione si sono infatti rese conto che l'unico modo per gestire la supervisione di un mercato veloce e informatizzato è servirsi di sistemi di IA che, da una parte, siano in grado di analizzare velocemente grandi quantità di dati e, dall'altra riescano a fornire stime e previsioni precise in relazione ai comportamenti attesi.

Un ulteriore esempio di applicazione della tecnologia dell'IA alla sorveglianza dei mercati è costituito dal progetto portato avanti dalla società Digital Reasoning, *leader* emergente nel campo dell'utilizzo dell'IA per l'analisi delle comunicazioni umane.[29]

---

[26] Si veda § 4.2.3 e § 4.2.4.

[27] O. KAYA, *High-frequency trading, reaching the limits*, Research Briefing Global financial markets, Deutsche Bank Research, Francoforte, 2016.

[28] *Artificial intelligence and Big Data are now a reality for the AMF*, disponible al seguente link https://www.amf-france.org/en/news-publications/news/artificial-intelligence-and-big-data-are-now-reality-amf

ICY, la nouvelle plateforme de surveillance de l'AMF, est opérationnelle, disponible al seguente link https://www.amf-france.org/fr/actualites-publications/actualites/icy-la-nouvelle-plateforme-de-surveillance-de-lamf-est-operationnelle

[29] R. HILL, *How artificial intelligence can stop market manipulation*, 2018, disponible al seguente link https://www.fia.org/marketvoice/articles/how-artificial-intelligence-can-stop-market-manipulation

Tale progetto, beneficiario di un grande investimento a cui hanno partecipato colossi del settore come Barclays, Goldman Sachs e Nasdaq, prevede la creazione di un sistema finalizzato all'elaborazione dei dati testuali. La società, già nota nel settore della sorveglianza militare, ha sviluppato una forma di intelligenza artificiale che interpreta in modo molto accurato il linguaggio umano.

Si tratta dell'"elaborazione del linguaggio naturale" (NLP): un sistema che combina la linguistica computazionale con modelli di *machine learning* e *deep learning*. Tale tecnologia, infatti, tiene conto del contesto del linguaggio e, apprendendo da precedenti esperienze, è in grado di comprendere un testo cogliendo le sfumature relative alle intenzioni e agli stati d'animo dell'autore.[30]

L'applicazione di tali sistemi alla sorveglianza dei mercati finanziari consentirebbe di individuare, analizzando i messaggi di testo, quelli che possono nascondere intenti potenzialmente manipolativi. In questo modo si potrebbero allertare le autorità al fine di prevenire la commissione dell'abuso di mercato.[31]

Anche l'Italia si sta muovendo in questa direzione. Consob, in collaborazione con la Scuola Normale Superiore di Pisa, ha recentemente portato a termine un progetto che prevede l'utilizzo di sistemi di IA come supporto alle attività di indagine relative agli abusi di mercato.[32]

Tale progetto si concentra in realtà sulla fattispecie di *insider trading*:[33] l'obbiettivo dell'analisi è quello di riuscire a valutare l'eventuale continuità o discontinuità della condotta dell'agente, in termini assoluti e relativi. Sono stati elaborati due modelli, basati su una tecnologia di IA di tipo *unsupervised machine learning,*[34] che potrebbero essere utilizzati per le analisi preliminari finalizzate all'individuazione di soggetti potenzialmente sospetti di *insider trading*.

---

[30] https://www.sas.com/it_it/insights/analytics/what-is-natural-language-processing-nlp.html

[31] R. HILL, *How artificial intelligence can stop market manipulation,* 2018, *cit.*

[32] P. MAZZARISI, A. RAVAGNANI, P. DERIU, F. LILLO, F. MEDDA, A. RUSSO, *A machine learning approach to support decision in insider trading detection*, Quaderni FinTec, Consob - Scuola Normale Superiore di Pisa, 2022.

[33] Si tratta di una delle condotte incriminate nel delitto di *Abuso di informazioni privilegiate* (185 TUF) : *"chiunque, essendo 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: 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; (...)*"

[34] Si veda § 1.1.1

Il primo modello viene utilizzato per identificare quei gruppi di investitori la cui attività di *trading,* in prossimità di un evento *price sensitive,* risulta non solo svolta in direzione premiante, ma anche caratterizzata da discontinuità operativa sia rispetto alla precedente storia di *trading* sia rispetto all'operatività tipica del gruppo di appartenenza. Tale sistema, basato su un metodo di *clustering analysis*, in primo luogo elabora un modello di *trading* per ciascun investitore sulla base di selezionati parametri quantitativi. Successivamente vengono individuati gruppi omogenei di investitori in relazione ad uno specifico orizzonte temporale. Infine, attraverso l'analisi dell'evoluzione della posizione assunta da ciascun investitore, il sistema distingue i cosiddetti "investitori discontinui", ossia coloro che, in prossimità di un evento *price sensitive*, hanno disatteso il comportamento previsto.[35]

Il secondo modello è finalizzato ad individuare i piccoli gruppi di investitori che agiscono in modo sincronizzato in prossimità di un evento *price sensitive*. Il *software* in questo caso costruisce una rete di investitori accomunati da un'attività sincrona per poi individuare gruppi omogenei di soggetti con attività simile che hanno operato ottenendo un profitto a seguito di un evento *price sensitive*.[36]

Si è potuto notare quindi come una svolta tecnologica epocale, come quella che stiamo vivendo in relazione all'evoluzione e lo sviluppo dell'intelligenza artificiale, possa creare numerosi problemi, ma anche costituirne, almeno in parte, la soluzione. Nel contesto dei mercati finanziari, parallelamente alla diffusione di sistemi di HFT, si stanno sviluppando modelli di sorveglianza basati su avanzati sistemi di IA. Tuttavia, si può evidenziare che perdura ancora un sensibile disallineamento tra le potenzialità lesive dei sistemi di contrattazione algoritmica ad alta frequenza e le capacità delle tecnologie di sorveglianza dei mercati. Queste ultime, per quanto avanzate, sono spesso ancora in fase di sviluppo e non sono ancora specializzate nel rintracciare quelle particolari tecniche manipolative poste in essere dagli HFT.

5.4 Conclusioni

[35] P. MAZZARISI, A. RAVAGNANI, P. DERIU, F. LILLO, F. MEDDA, A. RUSSO, *A machine learning approach to support decision in insider trading detection*, *cit*.
[36] *Ibidem*.

L'incessante succedersi di evoluzioni tecnologiche interessa la nostra società da decenni; tuttavia l'intelligenza artificiale costituisce un'invenzione che, probabilmente più di altre, rivoluzionerà numerosi aspetti della vita umana. Numerosi settori economici stanno già affrontando importanti cambiamenti in questa direzione; si inizia addirittura a parlare di "quarta rivoluzione industriale".[37]

Tale tecnologia, coinvolgendo così ampiamente la dimensione sociale, comporta inevitabilmente anche risvolti inerenti alla sfera penalistica.[38]

Il diritto penale si è trovato impreparato ad affrontare le problematiche legate all'intelligenza artificiale: i principi e i meccanismi tradizionali non si sono mai confrontati con casi in cui la macchina, lungi dal costituire strumento esecutivo del reato, integri la "mente" della fattispecie criminosa.[39]

L'ambito dei mercati finanziari è quello nel quale per la prima volta il diritto penale inizia a confrontarsi con le problematiche legate al *responsibility gap* derivante dai modelli *black boxes*.[40] Si tratta di un settore già di per sé complesso nel quale emergono ulteriori problematiche, come l'imprevedibilità dei mercati e la loro extraterritorialità; tutti elementi di ulteriore criticità che devono conciliarsi con i sistemi di diritto penale nazionale.

Nei paragrafi precedenti è stata esposta una panoramica delle soluzioni proposte dalla dottrina alla luce degli attuali strumenti giuridici disponibili[41] e, successivamente, sono stati ipotizzati eventuali interventi *de iure condendo* strumentali a far fronte alle lacune di tutela penalistica sottese al fenomeno della manipolazione di mercato, quando realizzata attraverso sistemi di HFT.[42]

Secondo parte della dottrina, tuttavia, tali proposte sarebbero in grado di offrire una soluzione solo provvisoria. Molti autori, infatti, sono concordi nel ritenere che le novità apportate dai sistemi di IA siano tali da obbligare ad un generale ripensamento delle

---

[37] M. GABBRIELLI, *Dalla logica al deep learning: una breve riflessione sull'intelligenza artificiale*, in *XXVI lezioni di diritto dell'intelligenza artificiale* a cura di U. Ruffolo, Torino, Giappichelli, 2020, p. 21.

[38] U. RUFFOLO, *XVI lezione: machina delinquere potest*, in *XXVI lezioni di diritto dell'intelligenza artificiale* a cura di U. Ruffolo, Torino, Giappichelli ed., 2020, p. 295; C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato,* in *Riv. it. dir. proc. pen*, vol.63, N°4, 2020; A. CAPPELLINI, *Machina delinquere non potest,* in www.discrimen.it, 2019.

[39] U. RUFFOLO, *XVI lezione: machina delinquere potest, cit.*

[40] F. CONSULICH, *Flash Offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti, cit.*

[41] Si veda § 4.3.1, § 4.3.2, § 4.3.3, § 4.3.4.

[42] Si veda § 5.1 e § 5.2

tradizionali categorie del diritto oppure all'introduzione di un nuovo "diritto dell'intelligenza artificiale".[43]

Parte della dottrina si è pertanto interrogata sulla possibilità di prevedere, a livello penalistico, schemi di attribuzione della responsabilità basati sulla causazione oggettiva del danno e focalizzati su nozioni come la "colpa di programmazione" o di "automazione", che coinvolgano l'impresa produttrice del sistema di IA.[44] Si tratterebbe di un settore del diritto penale a sé stante, ovviamente in tensione con i principi costituzionalmente imposti dalla responsabilità personale e colpevole.

Per tali motivi, altri autori hanno invece ritenuto che la strategia per garantire un'adeguata tutela in relazione a fatti illeciti compiuti da agenti di IA debba essere articolata in altri settori del diritto. Una delle soluzioni proposte, in chiave preventiva, è stata, ad esempio, quella di prevedere un sistema di autorizzazioni amministrative in relazione alla produzione e al commercio dei sistemi di IA.[45]

Una delle strade di sviluppo più promettenti del diritto dell'intelligenza artificiale attiene alla responsabilità civile per danni. La stessa Unione Europea sembra muoversi in questa direzione.[46]

Già nel 2017 la Risoluzione del Parlamento Europeo recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica suggeriva "*l'istituzione di uno status giuridico specifico per i robot nel lungo termine, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi.*"[47]

---

[43] N. MAZZACUVA, *Alcune riflessioni su intelligenza artificiale e diritto penale sostanziale*, in *XXVI lezioni di diritto dell'intelligenza artificiale* a cura di U. Ruffolo, Torino, Giappichelli, 2020, p. 287; U. RUFFOLO, *XVI lezione: machina delinquere potest*, *cit*.; B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automazione artificiale,* in *Diritto dell'Informazione e dell'informatica* (II), fasc.2, 2021, p. 317; C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato, cit.,* A. CAPPELLINI, *Machina delinquere non potest, cit.*

[44] N. MAZZACUVA, *Alcune riflessioni su intelligenza artificiale e diritto penale sostanziale, cit.*, p. 290.

[45] I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale,* in *Riv. it. dir. proc. pen*, fasc.1, marzo 2021, p.83.

[46] P. MORO, *Alle frontiere della soggettività: indizi di responsabilità delle macchine intelligenti*, in *XXVI lezioni di diritto dell'intelligenza artificiale* a cura di U. Ruffolo, Torino, Giappichelli ed., 2020, p.55.

[47] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, *Gazzetta ufficiale dell'Unione europea*, 18 luglio 2018, C 252/239

Nel settembre 2022 è stata poi approvata dalla Commissione Europea una proposta di Direttiva sulla responsabilità per danni causata dall'intelligenza artificiale.[48] Tale direttiva è parte di un approccio europeo coordinato che ricomprende anche la già citata proposta di Regolamento sull'IA. A differenza del Regolamento, che si concentra principalmente sul monitoraggio e la prevenzione dei danni, la Direttiva è finalizzata all'armonizzazione del regime di responsabilità applicabile nei casi in cui agenti autonomi causino danni.[49]

Una diversa impostazione si fonda su una sorta di "educazione" della macchina alle regole giuridiche. Parte della dottrina ha proposto una cosiddetta *legal protection by design*, la quale comporterebbe "*una traduzione di principi giuridici, in specie per la tutela dei diritti fondamentali, dal linguaggio naturale a quello computazionale attraverso la formazione di requisiti tecnici e formulazioni di default.*"[50] Si tratterebbe quindi di sfruttare i meccanismi di *machine learning* per inserire, attraverso la penalizzazione dell'errore, una dimensione etico-giuridica all'interno dei complessi meccanismi decisionali del sistema.[51]

Infine, vi è anche chi ha suggerito che tutte quelle prospettate sarebbero soluzioni temporanee, nell'attesa del momento in cui la tecnologia dell'intelligenza artificiale raggiunga un grado di avanzamento tale da poter essere in grado di "autodeterminarsi" e comprendere il disvalore sociale dei comportamenti.[52] Questo scenario, cin apparenza quasi

---

[48] 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), disponibile presso eur-lex.europa.eu.
La proposta di Direttiva ha come obbiettivo quello di favorire gli investimenti nel mercato interno ed evitare barriere di ingresso nel settore dell'intelligenza artificiale. Pertanto, la Direttiva mira, in generale, all'alleggerimento dell'onere della prova del danneggiato attraverso due principali strumenti: presunzione relativa e divulgazione di informazioni**.**
La presunzione è finalizzata a semplificare per i danneggiati la prova del nesso causale tra la colpa del convenuto e l'*output* (o la mancata produzione di un *output*) prodotto dal sistema di IA che ha provocato il danno.
Sono previsti regimi differenziati in relazione ai sistemi definiti "ad alto rischio" e per i sistemi utilizzati nel corso di un'attività personale non professionale
Inoltre, per i sistemi di IA ad alto rischio**,** la Direttiva attribuisce agli organi giurisdizionali nazionali il potere di ordinare la divulgazione di elementi di prova da parte del fornitore o altro soggetto tenuto ai medesimi obblighi del fornitore, nel caso in cui questi abbiano negato di dar corso alla medesima richiesta presentata dal danneggiato.

[49] https://www.agendadigitale.eu/cultura-digitale/danni-causati-dallintelligenza-artificiale-chi-paga-cosa-prevede-la-proposta-di-direttiva-ue/

[50] B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automazione artificiale, cit.*

[51] U. RUFFOLO, *XVI lezione: machina delinquere potest, cit.*

[52] A. CAPPELLINI, *Machina delinquere non potest, cit.*; I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale, cit.;* U. RUFFOLO, *XVI lezione: machina delinquere potest, cit.*

fantascientifico, potrebbe, secondo tali autori, permettere l'introduzione di un vero e proprio meccanismo di responsabilità diretta dei sistemi di IA.[53]

[53] Si allude alle teorie, ampiamente criticate, di Gabriel Hallevy vertenti su meccanismi di imputazione penale della macchina. Si rinvia a tal proposito al paragrafo §1.2.2.

BIBLIOGRAFIA

ADAM R., TIZZANO A., *Manuale di diritto dell'Unione Europea*, Giappichelli, Torino, 2017.

ANGELS J., HARRIS L., SPATT C., *Equity Trading in the 21st Century*, in *Marshall School of Business Working Paper*, Los Angeles, 2010.

ARULKUMARAN K., DEISENROTH M. P., BRUNDAGE M., BHARATH A. A., *A Brief Survey of Deep Reinforcement Learning*, in *IEEE Signal Processing Magazine*, 2017.

ASHTON H., *Definition of intent suitable for algorithms*, in *Artificial Intelligence and Law*, 2022.

Audizione della Consob presso la Quattordicesima Commissione Permanente (Politiche dell'Unione Europea) del Senato della Repubblica, in relazione al disegno di legge n. 2169 ("Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea" - Legge europea 2019-2020)

AZZUTTI A., RIING W. G., STIHEL 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.

BATHAEE Y.*, The Artificial Intelligence Black Box and the failure of intent and causation,* in *Harvard Journal of Law & Technology,* Volume 31, Number 2 Spring, 2018.

BORSARI R., *Intelligenza artificiale e responsabilità penale: le prime considerazioni,* in *Media Laws*, 2019.

BOUVERET A., GUILLAUMIE C., ROQUEIRO C. A., WINKLER C., NAUHAUS S., *High-frequency trading activity in EU equity markets*, Economic Report*,* ESMA, 2014.

CONTRINO A., DELLA VALLE E., MARCHESELLI A., MARELLO E., MARINI G., MESSINA S.M., TRIVELLIN M., *Fondamenti di diritto tributario*, Wolters Kluwer, Milano, 2020.

CAPPELLINI A., *Machina delinquere non potest,* in www.discrimen.it, 2019.

CAVOLI J., CHARLES W., EVANS C., CLARKE E., GIAMPAOLO K., MARINKOVIC C., *Spoofing Under US and UK Law,* Milbank, 2021, disponibile presso https://www.milbank.com/en/news/spoofing-under-us-and-uk-law.html?utm_source=mondaq&utm_medium=syndication&utm_content=inarticlelink&utm_campaign=article

CAVOLI J., GIAMPAOLO K., CLARKE E., Milbank LLP, *A Practice Guide on the Law of Spoofing in the Derivatives and Securities Markets*, Wolter Kluwer Legal and regulatory U.S. Whitepaper, 2021

Consob, Comunicazione n. DME/5078692 del 29/11/2005

Consob, Comunicazione n DME/10039224 del 30/04/2010

CONSULICH F., *Flash Offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti*, in *Riv. it. dir. e proc. pen*., n.3, 2022.

CONSULICH F., *Il Nastro Di Möbius. Intelligenza Artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca Borsa e Titolo di Credito*, n. 2, 2018.

CONSULICH F., *La Giustizia e il Mercato, miti e realtà di una tutela penale dell'investimento mobiliare,* Giuffrè, Milano, 2010.

CONSULICH F., *Manipolazione del mercato e disorientamenti dogmatici: tra eventi di pericolo e pericolo di eventi*, in *Le Società*, n.7, 2011, p. 823 ss.

CONSULICH F., *Rischio Consentito,* in *Enc. dir*, p.1102 ss, Giuffrè, 2021.

CONSULICH F., *Il principio di autonomia della responsabilità dell'ente, prospettive di riforma dell'art 8*, in *Rivista231,* n. 4, 2018.

CRESCI S., LILLO F., REGOLI D., TARDELLI S., TESCONI M., *Cashtag Piggybacking: Uncovering Spam and Bot Activity In Stock Microblogs On Twitter*, 2019.

ČUK T., VAN WAEYENBERGE A., *European Legal Framework for Algorithmic and High Frequency Trading (Mifid 2 and MAR), A Global Approach to Managing the Risks of the Modern Trading Paradigm,* in *Cambridge University Press*, Cambridge**,** 2018.

D'ALESSANDRO F., *Tutela dei mercati finanziari e rispetto dei diritti umani fondamentali*, in *Dir. pen. e proc*., 2014.

DE SIMONE G., *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) d'imputazione*, in *Diritto Penale Contemporaneo*, 2012.

DE VERO G., *La responsabilità penale delle persone giuridiche, IV Trattato di diritto penale. Parte generale*, Giuffré Milano, 2008.

Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2019-2020.

Divisione Mercati, Ufficio Vigilanza Infrastrutture di Mercato, CONSOB, *Mappatura delle sedi di negoziazione in Italia dopo l'entrata in vigore di MiFID II/MiFIR*, ottobre 2018.

FABOZZI F.J., FOCARDI S., JONAS C., *Investment Management after the Global Financial Crisis*, The Research Foundation of CFA Institute, 2010.

FIANDACA G., MUSCO E., *Diritto penale parte generale*, Zanichelli, Bologna, 2019.

FISHER J., CLIFFORD A., DINSHAW F., WERLE N., *Criminal forms of high frequency trading on the financial markets*, in *Law and Financial Markets Review*, Vol. 9, No. 2, London School of Economics, London, 2015.

GABBRIELLI M., *Dalla logica al deep learning: una breve riflessione sull'intelligenza artificiale*, in *XXVI lezioni di diritto dell'intelligenza artificiale* a cura di U. Ruffolo, Torino, Giappichelli, 2020, p. 21.

GALANTI A., *La manipolazione del mercato*, in *Diritto penale dell'impresa*, vol. 10, Cendon, Keyeditore, Milano 2015.

GAMBARDELLA M., *Condotte Economiche e Responsabilità Penale,* Giappichelli, Torino, 2020.

GROSSO C.F., PELISSERO M., PERTINI D., PISA P., *Manuale di Diritto Penale Parte Generale*, Giuffrè, Milano 2020.

GUARINELLO F., *Gli abusi di mercato. La manipolazione di mercato: fattispecie penale e amministrativa*., in *Diritto bancario Tidona*, 2006, disponibile al seguente link https://www.tidona.com/gli-abusi-di-mercato-la-manipolazione-di-mercato-fattispecie-penale-ed-amministrativa/

HALLEVY G., *Liability for Crimes Involving Artificial Intelligence Systems*, Berlino, 2015.

HILL R., *How artificial intelligence can stop market manipulation*, 2018, disponible al seguente link https://www.fia.org/marketvoice/articles/how-artificial-intelligence-can-stop-market-manipulation
https://www.sas.com/it_it/insights/analytics/what-is-natural-language-processing-nlp.html

KAYA O., *High-frequency trading, reaching the limits*, Research Briefing Global financial markets, Deutsche Bank Research, Francoforte, 2016.

LA CUTE G., *Truffa*, in *Enc. dir*, *(XLV)*, Giuffrè, 1992.

LILLO F., MARMI S., *Il calcolo della velocità,* in *Il Sole 24 Ore,* 19 maggio 2011.

LONGO M., *Un flash crash travolge i listini, ma pesano più Fed e Cina*, in *Il Sole 24 Ore*, 3 maggio 2022.

MANTOVANI F., *Diritto Penale*, Cedam, Padova, 2020.

MARINUCCI G., DOLCINI E., GATTA G. L., *Manuale di Diritto Penale parte generale*, Giuffrè, Milano, 2022.

MARTIELLO G., *Il "ravvedimento comunitario" del legislatore nazionale in tema di repressione degli abusi di mercato: prime note di commento all'art. 26 della legge n. 238/2021*, in *Leg. Pen*., 2022.

MARRO E., *Quanto c'entra la finanza ombra con il crollo delle borse?*, ilsole24ore.com, 2016.

MASULLO N.M., *Colpa penale e precazione nel segno della complessità*, Edizioni Scientifiche Italiane, Napoli, 2012.

MAZZACUVA N., AMATI E., *Diritto Penale dell'Economia*, Wolters Kluwer, Milano, 2020.

MAZZACUVA N., *Alcune riflessioni su intelligenza artificiale e diritto penale sostanziale*, in *XXVI lezioni di diritto dell'intelligenza artificiale* a cura di U. Ruffolo, Torino, Giappichelli, 2020.

MAZZARISI P., RAVAGNANI A., DERIU P., LILLO F., MEDDA F., RUSSO A., *A machine learning approach to support decision in insider trading detection*, Quaderni FinTec, Consob - Scuola Normale Superiore di Pisa, 2022.

MINELLI C., *La responsabilità "penale" tra persona fisica e corporation alla luce della Proposta di Regolamento sull'Intelligenza Artificiale*, in *Diritto penale Contemporaneo*, n.2, 2022.

MIZUTA T., *Does an Artificial Intelligence Perform Market Manipulation with Its Own Discretion? – A Genetic Algorithm Learns in An Artificial Market Simulation*, SPARX Asset Management Co. Ltd., Tokyo, 2020.

MORO P., *Alle frontiere della soggettività: indizi di responsabilità delle macchine intelligenti*, in *XXVI lezioni di diritto dell'intelligenza artificiale* a cura di U. Ruffolo, Torino, Giappichelli ed., 2020.

MUCCIARELLI F., *Aggiotaggio*, in *Il nuovo diritto penale delle società*, a cura di A. Alessandri, Milano, 2002.

MUCCIARELLI F., *Altri artifici: una (controversa) modalità di realizzazione del delitto di manipolazione del mercato*, in *Studi in onore di Mario Romano*, Napoli, 2011.

NICHOLSON W., *Medical Malpractice and Black-Box Medicine,* in *Big Data, Health Law, and Bioethics* in Cambridge University Press, U of Michigan Public Law Research Paper No. 536, 2017.

NISCO A., *Manipolazione informativa del mercato e luogo di consumazione del reato*, in *Diritto Penale Contemporaneo*, 2014.

PALIERO C.E., *La responsabilità penale della persona giuridica nell'ordinamento italiano: profili sistematici*, in *Societas puniri potest - La responsabilità da reato degli enti collettivi* (atti del convegno organizzato dalla Facoltà di giurisprudenza e dal Dipartimento di diritto comparato e penale dell'Università di Firenze, 15-16 marzo 2002), Cedam, Padova, 2003.

PALMISANO M., *L'abuso di mercato nell'era delle nuove tecnologie. Trading algoritmico e principio di personalità dell'illecito penale*, in *Diritto Penale Contemporaneo*, n.2, 2019.

PANATTONI B., *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automazione artificiale,* in *Diritto dell'Informazione e dell'informatica* (II), fasc.2, 2021, p. 317.

PECORELLA C., *Principi generali e criteri di attribuzione della responsabilità*, *in La responsabilità amministrativa degli enti*, Milano, 2002.

PEDRAZZI C., *Turbativa dei mercati*, In *Dig. Disc. Pen*., XIV, 1999.

PERRONE A., *Il diritto del Mercato dei Capitali*, Giuffrè, Milano 2020.

PICARDO E., *4 Big Risks of Algorithmic High-Frequency Trading*, investopedia.com, 2022.

PIERGALLINI C., *Colpa (diritto penale)*, Annali X, *Enc. Dir.*, 2017.

PIERGALLINI C., *Intelligenza artificiale: da "mezzo" ad "autore" del reato,* in *Riv. it. dir. proc. pen*, vol.63, N°4, 2020.

PISA P., *Giurisprudenza Commentata di Diritto Penale, Volume I, Delitti contro la persona e contro il patrimonio*, Wolters Kluwer, Milano, 2018.

Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione, 2021, eur-lex.europa.eu.

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), disponibile presso eur-lex.europa.eu

PROSDOCIMI S., *Reato Doloso*, in *Digesto*, Wolters Kluwer, 1996, disponibile presso One Legale.

PUORRO A., *High Frequency Trading: una panoramica,* in *Questioni di Economia e Finanza (Occasional Papers)*, Consob, 2013.

Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, *Gazzetta ufficiale dell'Unione europea*, 18 luglio 2018, C 252/239

ROMANÒ L.*, La responsabilità penale al tempo di chatgpt: prospettive de iure condendo in tema di gestione del rischio da intelligenza artificiale generativa*, in *Sistema Penale*, 2023.

ROPPO V., *Diritto Privato*, Giappichelli, Torino, 2018.

RUFFOLO U., *XVI lezione: machina delinquere potest*, in *XXVI lezioni di diritto dell'intelligenza artificiale* a cura di U. Ruffolo, Torino, Giappichelli ed., 2020.

SALVADORI I.*, Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale,* in *Riv. it. dir. proc. pen,* fasc.1, marzo 2021.

SANDRELLI G., *I Reati di Market Abuse*, 2006, in www.rivista231.it

SCORDAMAGLIA I., *Il diritto penale della sicurezza sul lavoro tra principi di prevenzione e precauzione*, in Diritto Penale Contemporaneo, 2012.

SEMINARA S., *Diritto penale commerciale*, I, *Il diritto penale del mercato mobiliare*, Torino, 2018.

SGUBBI F., FONDAROLI D., TRIPODI A.F., *Diritto Penale del Mercato Finanziario*, CEDAM, Padova, 2013.

SINISCALCO M., *Autore Mediato (dir. pen) (IV,1959)*, in *Enc. Dir.,* Giuffrè, 1959.

TABOGA A., *Dolo nel concorso di persone, commento a sentenza Cass, sez. I, 1° agosto 2008, n. 32433*, in *Giurisprudenza italiana*, marzo 2009.

TOM C. W. L., *Reasonable Investor(s),* in *95 Boston University Law Review*, 2015.

TURING A., *Calcolatori e intelligenza*, in *L'io della mente*, a cura di D. R. Hofstadter, D. C. Dennet, Milano, 1981, p. 64.

VENDITTI R., *Actio libera in causa (I,1958)*, in *Enc. Dir.*, Giuffrè, 1958.

YADAV Y., *The Failure of Liability in Modern Markets*, in Virginia Law Review, vol. 102, 2016.

SITOGRAFIA

https://www.agendadigitale.eu/cultura-digitale/danni-causati-dallintelligenza-artificiale-chi-paga-cosa-prevede-la-proposta-di-direttiva-ue/

Artificial intelligence and Big Data are now a reality for the AMF, disponible al seguente link https://www.amf-france.org/en/news-publications/news/artificial-intelligence-and-big-data-are-now-reality-amf

https://definitions.uslegal.com/m/marking-the-close/

https://www.finanzaonline.com/notizie/flash-crash-europa-scatenato-da-errore-trading-desk-citigroup-panico-alla-borsa-di-stoccolma-ecco-cosa-e-successo

https://www.federalregister.gov/documents/2010/11/02/2010-27547/antidisruptive-practices-authority-contained-in-the-dodd-frank-wall-street-reform-and-consumer

ICY, la nouvelle plateforme de surveillance de l'AMF, est opérationnelle, disponible al seguente link https://www.amf-france.org/fr/actualites-publications/actualites/icy-la-nouvelle-plateforme-de-surveillance-de-lamf-est-operationnelle

https://www.sec.gov/divisions/marketreg/subpenny612faq.htm

https://www.sec.gov/divisions/marketreg/nmsfaq610-11.htm

https://www.sec.gov/news/press-release/2013-222

https://www.sec.gov/news/press-release/2014-229