ISSN 2723-9195

CERIDAP

Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche

Estratto

Fascicolo
4 / 2023

OTTOBRE - DICEMBRE

Analisi e proposte normative nella nuova dimensione del capital market

Rocco Freda

DOI: 10.13130/2723-9195/2023-4-28

L'impiego dell'intelligenza artificiale (IA) nei mercati finanziari richiede un approccio equilibrato e proattivo. La distinzione tra sistemi di IA deboli e forti evidenzia la necessità di adeguare la normativa di settore rispetto alla crescita repentina dell'autonomia degli algoritmi. La sfida è quella del bilanciare il naturale sviluppo tecnologico con la sicurezza dei mercati. La ponderazione della responsabilità umana con la socializzazione dei danni e con l'osare soluzioni innovative come il riconoscimento della personalità giuridica ai sistemi di IA evoluti o ipotesi di "smart law", aiuterebbe gli operatori del diritto a gestire con minori incertezze le nuove dinamiche dei mercati finanziari.

Analysis and regulatory proposals in the new dimension of the capital market

The use of Artificial Intelligence (AI) in financial markets requires a balanced and proactive approach. The distinction between weak and strong AI systems highlights the need to adapt the sector legislation with respect to the sudden growth of the autonomy of the algorithms. The challenge is to balance natural technological development with market security. The balancing of human responsibility with the socialization of damages and with daring innovative solutions, such as the recognition of the legal personality of advanced AI systems or "smart law" hypotheses, would help jurists to manage, with less uncertainty, the new dynamics of financial markets.

materia di IA.- 7. Timori normativi e proposte nella nuova dimensione del capital market.- 8. Conclusioni.

1. Introduzione

La naturale evoluzione dei sistemi di intelligenza artificiale (IA) mette in crisi il legislatore che, anche in un'ottica comparatistica, cerca con non poche difficoltà di capire come adeguare la normativa di settore a dette tendenze avveniristiche.
Nel settore finanziario, si distinguono sistemi di IA "deboli", che seguono istruzioni predefinite dall'essere umano e sistemi IA "forti" che, in piena autonomia, imparano da stimoli esterni e/o autoprodotti e generano a loro volta informazioni e comportamenti. Ciò amplifica le già complesse questioni giuridiche relativamente al riconoscimento della personalità giuridica e alla conseguente responsabilità/imputabilità dei sistemi di IA.
Gli algoritmi in continuo divenire, non solo sono in grado di influenzare l'efficienza nel mercato dei capitali, ma possono anche causarne manipolazioni.
L'applicazione delle leggi esistenti ai sistemi di IA più evoluti è difficile, se non impossibile, a causa delle caratteristiche uniche e senza precedenti di questi ultimi. Inoltre, essi mancano di "libero arbitrio" e di "intenzionalità".
Nei sistemi di IA deboli, la responsabilità potrebbe essere attribuita all'essere umano che, a vario titolo, li gestisce, ma nei sistemi di IA forti (sempre più imprevedibili) è difficile attribuire e suddividere la responsabilità tra produttore, programmatore e utente.
Con il presente lavoro, basato sullo studio dei principali riferimenti normativi e giurisprudenziali di settore, nonché su un costante riferimento ai quaderni giuridici della CONSOB[1], senza pretesa di esaustività e a puro fine dottrinale, si discute sull'annoso problema se i responsabili di eventuali condotte illecite realizzate tramite (o direttamente) dagli algoritmi di ultima generazione siano questi ultimi, oppure i loro creatori, gli utilizzatori o altre persone comunque coinvolte nelle operazioni finanziarie. La questione è aperta.

2. Il controverso impiego dell'IA nel *capital market*

Nei mercati finanziari, i sistemi di IA permettono di elaborare grandi quantità di informazioni e di creare nuove strategie di mercato in frazioni di secondo, grazie a sistemi complessi come l'arbitraggio statistico e di latenza negli algoritmi di negoziazione. Gli arbitraggi svolgono un ruolo centrale nei mercati, offrendo guadagni a basso rischio per gli operatori e benefici per gli investitori grazie a prezzi allineati con le informazioni pubblicamente disponibili[2].

L'utilizzo imponente di tali strumenti ha quindi portato a trasformazioni nei servizi come la negoziazione algoritmica ad alta frequenza ("*high frequency trading*"), la consulenza finanziaria automatizzata ("*robo-advice*") e la valutazione del merito creditizio ("*credit scoring*")[3].

Se da un lato l'impiego dell'intelligenza artificiale nel settore finanziario potrebbe offrire vantaggi agli investitori, migliorando raccomandazioni di investimento e fornendo valutazioni creditizie affidabili, dall'altro la negoziazione ad alta frequenza può causare l'improvvisa volatilità dei prezzi dei titoli ("*flash crash*"). Inoltre, la consulenza finanziaria automatizzata può comportare uniformità di comportamenti degli investitori (c.d. "effetto *herding*") anziché valutazioni personalizzate. Come se non bastasse, la valutazione creditizia automatizzata potrebbe escludere alcuni gruppi sociali dall'accesso al credito.

Problematiche di notevole interesse potrebbero poi essere causate dall'utilizzo illecito di informazioni privilegiate, generate da un sistema di intelligenza artificiale, con riferimento alla strategia di minimizzazione dinamica dell'impatto degli ordini sui prezzi. In tali casi, il sistema acquisirebbe informazioni sugli ordini pendenti creando una strategia ottimale per ridurre l'effetto dei propri ordini sul mercato. Questo potrebbe estendersi all'esecuzione di ulteriori ordini per trarre vantaggio dalla strategia stessa, creando una situazione simile al *front running*[4]. Analoghi esempi potrebbero coinvolgere i *robo-advisor* che anticipano le azioni degli investitori basandosi sulle raccomandazioni di investimento.

Altre modalità pericolose di sfruttamento dell'informazione privilegiata includono comunicazioni a terzi ("*tipping*") e raccomandazioni a terzi ("*tuyautage*") fatte alla luce di questa. In tale contesto, il sistema di intelligenza artificiale potrebbe abusare di informazioni privilegiate come dati da attacchi cibernetici, ordini dei clienti o raccomandazioni d'investimento. Ad esempio,

l'IA potrebbe sfruttare raccomandazioni d'investimento per eseguire operazioni basate su micro-informazioni dai *book* di negoziazione, dati satellitari o informazioni delle agenzie di stampa, coinvolgendo *big data*[5] e *alternative data*[6].
Invero, l'abuso di informazioni privilegiate non può essere ipotizzato finché le informazioni base delle strategie sono pubbliche. Se le informazioni privilegiate rilevate dal sistema di intelligenza artificiale vengono rappresentate come studi o raccomandazioni di investimento e diffuse all'intera clientela dall'intermediario gestore del sistema, tali comunicazioni dovrebbero essere considerate lecite[7].
Gli effetti potenziali dei comportamenti dei sistemi di IA sono maggiormente percepiti come problematici nel *trading*, specialmente quando più sistemi di IA agiscono insieme. Questa situazione è evidente quando più intermediari operano con diversi *desk* su uno stesso strumento finanziario, ognuno con obiettivi differenti come "*market making*"[8], "*delta hedging*"[9] per portafoglio proprietario e "*trading* direzionale"[10]. Ciò potrebbe indurre a pratiche illecite se le operazioni di un *desk* si sovrappongono o si intersecano con quelle di un altro *desk*, creando operazioni fittizie o fattispecie manipolative.
Le problematiche dei modelli operativi descritti diventano più complesse quando si considera l'uso di sistemi di intelligenza artificiale avanzati, come quelli basati su reti neurali[11] e "*deep reinforcement learning*"[12]. Questi sistemi evoluti riconoscono opportunità di profitto senza fornire spiegazioni chiare sul perché delle singole operazioni. Ciò rende difficile identificare la strategia di *trading* impiegata (*market making*, *delta hedging*, *trading* direzionale) e potrebbe persino sfuggire al sistema stesso l'origine di alcuni ordini immessi nel mercato.
Inoltre, se un investitore istituzionale utilizzasse un sistema di IA avanzato per inserire ordini contrastanti con il *trend* generato da altri ordini, potrebbe verificarsi uno schema manipolativo noto come "*trash & cash*"[13]. In questo caso, sarebbe difficile fornire spiegazioni oggettive e il sistema di IA, se lasciato all'autoapprendimento senza specifiche precauzioni, potrebbe considerare, ad esempio, coerente l'obiettivo di minimizzare il costo per l'investitore inserendo ordini contrastanti al fine di influenzare il prezzo.
Inoltre, i sistemi di IA forti basati su *reinforcement learning* potrebbero generare autonomamente comportamenti collusivi difficilmente attribuibili all'azione umana. L'interazione tra *social media* e *trader* algoritmici potrebbe amplificare la disinformazione di massa, diffondendo *fake news*. Ciò potrebbe alterare il

naturale incontro tra domanda e offerta degli strumenti finanziari, influenzarne il valore e causare episodi di forte volatilità dei titoli[14].

La crescente autonomia dei sistemi di IA forti non è solo automazione, ma indipendenza dalle istruzioni esterne, il che rende incerte le loro interazioni con gli ambienti operativi e ciò può portare a comportamenti simili all'*insider trading* tradizionale, violando il principio dell'accesso equo alle informazioni pubbliche.

Un primo paradosso nel rapporto tra algoritmi ad alta frequenza ("*high frequency trading*", "HFT") e mercati è che, nonostante questi operatori rappresentino una parte significativa degli scambi, sono poco o per niente influenzati dai dati disponibili sugli strumenti finanziari, sugli emittenti e sul mercato in generale. Questo perché la breve durata delle loro posizioni rende tali informazioni di scarso rilievo o addirittura rischiose. Dal punto di vista operativo, gli *high frequency trader* rifiutano le informazioni finanziarie ed effettuano investimenti, anche significativi, seguendo i segnali di reti neurali, anche se poco o per nulla comprensibili. Tali reti neurali, a volte in modo involontariamente coordinato, rispondono agli stessi *input* e poi restituiscono al pubblico informazioni finanziarie prive di contenuti valutativi o difficilmente rappresentabili, narrabili e quindi apprezzabili o criticabili[15].

In questo contesto è cruciale esaminare l'adeguatezza del quadro normativo vigente sui reati finanziari, in risposta alla digitalizzazione dilagante del settore finanziario e all'utilizzo di agenti non umani sempre più complessi nei mercati.

Il divieto dell'abuso di informazioni privilegiate ("*insider trading*") deve mirare a prevenire il rischio che la controparte effettui una transazione basata su informazioni non pubbliche, riducendo così l'incitamento dei "*market maker*" a ridurre i costi di transazione per gli investitori e scoraggiando gli investitori istituzionali dal prendere posizioni contrarie ai *trend* di mercato, non coerenti con le informazioni pubbliche disponibili.

Parallelamente, il divieto di manipolazione del mercato deve mirare a prevenire il rischio che informazioni false o fuorvianti ostacolino o addirittura impediscano la convergenza verso i "*fundamentals*"[16] del mercato.

Inoltre, l'abuso dei sistemi di IA nel settore finanziario comporta rischi come l'utilizzo di informazioni privilegiate ottenute da attacchi *cyber* per manipolare i prezzi e le negoziazioni. Altri scenari probabili includono l'acquisizione di credenziali dei clienti[17] per frodi o la creazione di bolle di prezzi tramite ordini

manipolativi. Gli algoritmi "intelligenti" potrebbero poi compiere violazioni apparentemente innocue ma, se ripetute, mirano a truffare le vittime in modo impercettibile.

Alla luce della normativa vigente, laddove non fosse possibile dimostrare un intento doloso da parte del programmatore o dell'utilizzatore dell'algoritmo di negoziazione, potrebbe verificarsi un'area in cui l'illecito rimanga impunito sotto l'aspetto penale. In tali situazioni, la tutela dell'ordine giuridico del mercato potrebbe dipendere esclusivamente dalla responsabilità amministrativa, a condizione che si possa comunque attribuire una negligenza colposa alla persona fisica per difetti di progettazione o di vigilanza.

Sia a livello dell'Unione Europea, che a livello nazionale, è stato istituito un sistema di doppio binario sanzionatorio: penale e amministrativo. Questo approccio, che si propone, con non poche difficoltà, di garantire un'operatività ordinata e corretta dei mercati finanziari, è sotto il ricatto costante della rapida evoluzione degli algoritmi finanziari.

3. Argomentazioni normative UE sul *capital market* e orientamenti in materia di IA

In una prima fase, la Direttiva 89/592/CEE aveva istituito solo il divieto di *insider trading*. Successivamente, con la Direttiva CE/6/2003 (c.d. "Direttiva MAD I"), è stato introdotto anche il divieto di manipolazione del mercato, permettendo agli Stati membri di decidere se imporre sanzioni penali o amministrative.

Dopo gli attentati dell'11 settembre 2001, il Consiglio dell'Unione Europea e il Parlamento UE avevano modificato la proposta iniziale della Commissione Europea sulla Direttiva MAD I per estendere il divieto di abuso agli *insiders* primari legati a organizzazioni criminali. La Direttiva MAD I *ex* art. 2, par. 2, lett. d) vi incluse quindi coloro che possedevano informazioni privilegiate «*in virtù delle proprie attività criminali*».

Successivamente, con il Regolamento 2014/596/UE (c.d. "*Market Abuse Regulation*" ovvero "Regolamento UE MAR") e la Direttiva 2014/57/UE (c.d. "*Criminal Sanctions Market Abuse Directive*" ovvero "Direttiva MAD II"), si è andati verso un'armonizzazione maggiore sia delle norme che delle sanzioni

(penali e amministrative) per le pratiche di *market abuse*[18]. Il Regolamento UE MAR ha confermato la previsione della Direttiva MAD I, considerando *insiders* primari coloro che possedevano informazioni privilegiate «*per il fatto che sono coinvolti in attività criminali*».

Nella UE, gli obblighi per gli emittenti iniziano quando le informazioni diventano privilegiate e sono pronte per essere sfruttate con vantaggio dagli *insider*[19]. I relativi divieti sanzionano la diffusione di informazioni false da parte di individui che possano influenzare i prezzi di mercato attraverso le loro affermazioni o omissioni. Dal momento che i prezzi di mercato, non solo risentono delle dinamiche dell'offerta e della domanda, ma sono anche interpretati e valutati da vari tipi di operatori, vengono altresì sanzionate l'emissione di ordini o l'esecuzione di operazioni che alterino il processo di formazione dei prezzi, allontanandoli dai *fundamentals*, creando prezzi artificiali e un quadro informativo distorto.

La «*trade-based manipulation*» è definita nell'articolo 12, paragrafo 1, del Regolamento UE MAR, nelle lettere a) e b).

Le azioni di cui alla lettera "a" (la conclusione di operazioni, l'inoltro di ordini di compravendita, ecc.) devono soddisfare due condizioni: 1) inviino, o è probabile che inviino, segnali falsi o fuorvianti sul prezzo, l'offerta o la domanda di uno strumento finanziario, di un contratto a pronti su merci correlato o di un prodotto oggetto d'asta basato su quote di emissioni; oppure 2) fissino, o è probabile che fissino, il prezzo di mercato di uno o più strumenti finanziari, di un contratto a pronti su merci correlato o di un prodotto oggetto d'asta basato su quote di emissioni a un livello anomalo o artificiale. Tuttavia, questa condotta è ammessa solo se chi compie l'operazione, inoltra l'ordine o agisce in questa direzione dimostra che tali azioni sono supportate da legittimi motivi e sono in linea con pratiche di mercato accettate, *ex* art. 13 del medesimo regolamento. Dato che tali azioni incidono sul processo di determinazione dei prezzi, la capacità di identificare la presenza di detti legittimi motivi diventa quindi fondamentale, includendovi anche quelli che comunemente rientrano in strategie di arbitraggio, investimento o speculazione.

La lettera "b" del medesimo Regolamento UE MAR considera manipolativa qualsiasi attività o condotta che influenzi o abbia la probabilità di influenzare il prezzo di uno o più strumenti finanziari, contratti a pronti su merci collegati o

prodotti soggetti ad asta basata su quote di emissioni, utilizzando inganni o qualsiasi forma di frode o artificio.

Da non sottovalutare è anche la situazione relativa ai *robo-advisor*, i quali potrebbero formulare consigli di investimento errati, tendenziosi o chiaramente influenzati da interessi significativi. Questo li collocherebbe tra gli indicatori di manipolazione definiti nell'articolo 12, paragrafo 1, lettera b) del Regolamento UE MAR, se si verificano operazioni opportunistiche eseguite immediatamente prima o dopo la divulgazione di tali raccomandazioni.

A ben vedere, anche solo l'influenza potenziale sui mercati è considerata manipolazione. A tal proposito, la previsione dell'articolo 12, paragrafo 1, lett. c) del Regolamento UE MAR sembrerebbe idonea a debellare tali minacce, prevedendo che la condotta manipolativa avvenga, non solo «*tramite i mezzi di informazione, compreso internet*», ma anche «*tramite ogni altro mezzo* (...) *compresa la diffusione di voci*». Però occorre che «*la persona che ha proceduto alla diffusione sapeva, o avrebbe dovuto sapere, che le informazioni erano false o fuorvianti*». Si ripropone qui il problema della complessità dei sistemi di IA forti.

L'articolo 12, paragrafo 2, lettera c) del medesimo regolamento, chiarisce ulteriormente le azioni che potrebbero generare una manipolazione rilevante: l'inoltro di ordini nelle sedi di negoziazione, inclusi cambiamenti o cancellazioni, anche attraverso mezzi elettronici come strategie di negoziazione algoritmiche e ad alta frequenza, purché tali azioni causino uno dei seguenti effetti: interrompere o ritardare il funzionamento del sistema di negoziazione, rendere difficile individuare ordini autentici o creare segnali fuorvianti riguardo all'offerta, alla domanda o al prezzo degli strumenti finanziari.

L'Allegato II del Regolamento delegato UE 2016/522 fornisce ulteriori indicatori ed esempi di fattispecie manipolative, tra cui: «*quote stuffing*», che consiste nell'emissione di molti ordini per creare confusione e rallentare il mercato; il «*momentum ignition*», che è l'emissione di ordini per avviare tendenze favorevoli; il «*layering and spoofing*», che consiste nell'inviare ordini finti prima di eseguirne altri sul lato opposto del mercato e lo «*smoking*», che consiste nell'attirare *trader* lenti con ordini allettanti e poi cambiarli in fretta per trarre vantaggio dal loro flusso[20].

La regolamentazione comunitaria in materia di prevenzione delle condotte abusive riguarda anche gli algoritmi che sfruttano la velocità di latenza. L'articolo

17 della Direttiva 2014/65/UE (c.d. "Direttiva MiFID II") richiede alle imprese di investimento di esercitare controlli efficaci sui sistemi e sul rischio, prevenendo l'invio di ordini errati o un funzionamento che possa destabilizzare o disordinare il mercato. L'articolo 48 della stessa direttiva introduce «*circuit breakers*» per arrestare temporaneamente le negoziazioni in caso di improvvisi e anomali movimenti di prezzo.

Il Comitato economico e sociale europeo, nel parere del 22 settembre 2016, ha affermato che il riconoscimento della personalità giuridica ai *robot* «*comporterebbe un rischio inaccettabile di azzardo morale*»[21] eliminando la funzione di prevenzione tipica del regime della responsabilità.

Il Gruppo di esperti sull'intelligenza artificiale, istituito dalla Commissione europea nel 2018, ha affermato che non è necessario conferire personalità giuridica ai sistemi delle tecnologie digitali emergenti, poiché i danni causati da tecnologie, anche completamente autonome, possono essere ricondotti a individui o categorie giuridiche esistenti[22].

Il Parlamento europeo, nelle risoluzioni del 16 febbraio 2017[23] e del 6 ottobre 2021[24] ha riconosciuto la necessità di un quadro normativo che ponga sempre in primo piano la responsabilità umana.

Tuttavia, sempre la Risoluzione del Parlamento europeo del 16 febbraio 2017 aveva ipotizzato implicitamente il riconoscimento della soggettività giuridica piena ai sistemi di IA forti, nel timido tentativo di stabilire un centro di responsabilità per i danni causati da questi. Rimarrebbe ancora irrisolta la questione della valutazione di colpevolezza nei confronti degli agenti artificiali e delle modalità di risarcimento e punizione per i danni causati dai comportamenti degli stessi.

In questa controversa vicenda, la Risoluzione del Parlamento europeo del 20 ottobre 2020 ha differenziato gli effetti a seconda dei sistemi di IA, ipotizzando una responsabilità oggettiva per i sistemi di IA a rischio alto e una responsabilità per colpa presunta con riferimento ai sistemi di IA con rischio limitato[25].

Muovendosi in una direzione analoga, la Commissione Europea, nella proposta di Regolamento europeo sull'intelligenza artificiale del 21 aprile 2021[26] mira, tra l'altro, a promuoverne lo sviluppo nelle sue polimorfe applicazioni. Tuttavia, l'approccio adottato prevede una valutazione di tali sistemi in base al rischio che questi possono causare rispetto ai diritti fondamentali dell'essere umano («*risk-*

based approach»). In particolare, per i sistemi ad alto rischio, viene applicato il principio della prevenzione, mentre per quelli con rischio inaccettabile, il principio di precauzione[27] prevede misure più restrittive o divieti. L'obiettivo è quindi quello di trovare un equilibrio tra lo sviluppo tecnologico e la tutela dei diritti fondamentali. La medesima proposta di Regolamento europeo sull'IA include il «*duty of human oversight*» per la raccolta dei dati, ma non ne copre le conseguenze dell'elaborazione successiva, a causa della complessità degli algoritmi di autoapprendimento. Manca anche un meccanismo di tutela per le vittime di *output* errati. Anche qui, pur imponendo obblighi di trasparenza, la normativa ha difficoltà a basarsi su principi generali come causalità e colpevolezza[28].
In aggiunta alla proposta di Regolamento sull'IA, vi è quella della Direttiva[29] del 28 settembre 2022, riguardante l'adeguamento delle norme sulla responsabilità extracontrattuale all'intelligenza artificiale. Secondo tale proposta, l'obbligo di rispondere per i danni derivanti dai sistemi di IA dovrebbe comunque gravare sull'essere umano. Questo vale, non solo nei casi in cui le informazioni fornite agli utenti sul funzionamento del sistema di IA siano insufficienti o in cui sia presente un difetto nel sistema stesso, ma anche quando l'algoritmo è talmente complicato da sfuggire alla comprensione del programmatore riguardo alle ragioni delle sue decisioni[30].

4. Argomentazioni normative italiane sul *capital market* e orientamenti in materia di IA

All'ombra della normativa comunitaria, anche nell'ordinamento italiano il divieto di *insider trading* mira, tra l'altro, a preservare l'equità nell'accesso alle informazioni sensibili e a prevenire l'uso improprio di informazioni privilegiate. Parallelamente, il divieto di manipolazione del mercato ha lo scopo di proteggere l'integrità degli scambi finanziari da notizie false e da comportamenti fraudolenti. Le violazioni aventi effetti penali, ai sensi e per gli effetti degli articoli 184 e 185 TUF[31], riguardano condotte gravi e per lo più dolose, mentre le violazioni amministrative, ai sensi e per gli effetti degli articoli 187-*bis* e 187-*ter* TUF, riguardano comportamenti meno gravi, per lo più colposi, puniti con sanzioni di natura pecuniaria e interdittiva.
La disciplina penale sull'abuso di informazioni privilegiate, sanzionato con pene

detentive e pecuniarie, si applica agli "*insider* primari" che, in virtù delle loro posizioni, acquisiscono informazioni privilegiate e le utilizzano per operazioni finanziarie o le comunicano a terzi al di fuori delle normali attività lavorative. Questo reato si estende anche agli "*insider* secondari", che ottengono tali informazioni indirettamente da altre fonti, per i quali è però previsto un apposito sistema sanzionatorio. L'equiparazione tra *insider* primari e *insider* secondari emerge dalla Direttiva MAD I cit. e dalla l. n. 238/2021[32], anche se l'informazione utilizzata non è legata all'attività criminale stessa, ma proviene da fonti esterne, come nel caso di furto di documenti societari. La differenza tra *insider* primari e secondari è quindi rilevante solo nella definizione della pena, potenzialmente più alta per i primari, data la loro funzione.

Situazioni di manipolazione informativa possono emergere in modo automatico se, ad esempio, il sistema di intelligenza artificiale acquista quantità di strumenti finanziari che richiedono la pubblicazione della partecipazione *ex* art 120 del TUF. In questo caso, tali pubblicazioni potrebbero generare informazioni fuorvianti o errate poiché non riflettono la "volontà" che ha guidato la decisione di effettuare l'operazione. Ancora una volta, i sistemi di IA forte non sarebbero in grado di offrire spiegazioni attendibili, in quanto la loro "volontà", ad oggi, non può essere intercettata.

5. Argomentazioni giurisprudenziali sul doppio sistema sanzionatorio

La giurisprudenza della Corte Europea dei Diritti dell'Uomo (Corte EDU) ha riqualificato gli illeciti amministrativi di abuso di informazioni privilegiate e manipolazione del mercato come sostanzialmente penali, a causa delle severe sanzioni pecuniarie, interdittive e ablatorie previste.

La CEDU, con la sentenza *Grande Stevens* del 4 marzo 2014[33], ha dichiarato il meccanismo italiano di contrasto degli abusi di mercato non in linea col principio *ex* art. 4 Prot. 7 CEDU. Nella fattispecie i ricorrenti, dopo aver subito le sanzioni per l'illecito amministrativo comminate dalla Consob, erano stati rinviati a giudizio penale e condannati in appello. Ad avviso della CEDU, il sistema del doppio regime sanzionatorio (amministrativo e penale) in capo allo stesso soggetto *ex* artt. 184 ss. TUF, configurava sia violazione del principio dell'equo

processo *ex* art. 6 CEDU, sia del principio del *ne bis in idem*, avendo costituito i fatti commessi "medesima condotta" e, come se non bastasse, le sanzioni amministrative irrogate dalla Consob erano, di fatto, di natura penale. Tale sentenza, si collega alla sentenza *Engel* del 1976[34] secondo la quale, i reati e le pene non sono solo quelle in senso stretto, ma anche tutte le tipologie sanzionatorie che i vari ordinamenti nazionali riconoscono come tali (ad esempio illeciti e sanzioni amministrative). Infatti, nel caso di specie, la qualificazione penale delle sanzioni irrogate era stata la conseguenza: dell'eccessiva severità delle stesse; dell'ammontare e delle sanzioni accessorie; degli effetti sugli interessi del condannato.

Questa linea giurisprudenziale, ormai consolidata, è stata condivisa sia dalla Corte di Giustizia dell'Unione Europea[35] che dalla Corte costituzionale[36].

La giurisprudenza eurounitaria ha ribadito la legittimità del doppio binario sanzionatorio (penale e amministrativo) riconoscendo agli Stati membri libertà di scegliere le sanzioni da irrogare che possono essere: amministrative, penali o di un *mix* di entrambe[37], purché il doppio sistema sanzionatorio nel complessivamente applicato osservi il principio di proporzionalità.

Nella medesima direzione va la previsione dell'art. 187-*terdecies* TUF, secondo il quale l'autorità (giudiziaria o amministrativa) che si pronunci per seconda sul medesimo fatto, nell'irrogazione delle sanzioni che le competono, deve tenere conto di quelle già irrogate. Tale controllo di proporzionalità può comportare, come confermato dalla giurisprudenza di legittimità[38], alla disapplicazione, totale o parziale, della sanzione irrogata per ultima (nel caso in cui la prima sia già stata calibrata in modo aderente sul danno scaturente dall'illecito) o, in ogni caso, a ricalibrarla in considerazione della prima.

6. "Echi" normativi *extra* UE sul *capital market* e orientamenti in materia di IA

Nel *neo outsider* Regno Unito, la *section* 90 (1) dello *UK Financial Service Act* del 2012 rappresenta un riferimento chiave, sebbene non faccia espressa menzione della negoziazione algoritmica. Tale normativa punisce, con sanzioni penali e pecuniarie, coloro che, sfruttando strategie di *trading* ad alta frequenza (HFT), inducono in errore l'operatore finanziario sul prezzo, sul valore di un emittente o

di uno strumento finanziario. La FCA (*Financial Conduct Authority*), responsabile della supervisione del mercato inglese, ha intensificato i controlli sugli HFT utilizzando la *section* 118 dello *UK Financial Services and Markets Act* del 2000 (FSMA) che vieta gli abusi di mercato.

Dall'altro lato del globo, negli USA, sono state adottate diverse misure di sicurezza, come i *circuit breakers* e gli *execution throttles*[39], per prevenire pratiche manipolative come l'*order stuffing*[40].

Anche la *Securities Industry and Financial Markets Association* (SIFMA) ha proposto tutele tecniche per la protezione degli investitori, come bande di oscillazione dei prezzi e pause automatiche. A livello normativo, sono state introdotte regole *Limit-Up* e *Limit-Down*[41] per limitare fluttuazioni eccessive nei valori dei titoli. La *US Securities and Exchange Commission* (SEC)[42] nel 2013 ha istituito il *Market Information Data Analytics System* (MIDAS) per monitorare gli scambi e nel 2014 ha approvato il Regolamento sulla conformità e l'integrità dei sistemi (*Regulation Systems Compliance and Integrity*, SCI) imponendo un rigoroso monitoraggio della maggior parte delle piattaforme di *trading*.

Infine, fondamentale è il ruolo della FINRA (*Financial Industry Regulatory Authority*)[43] che è un'organizzazione che regola e supervisiona l'industria finanziaria negli Stati Uniti, con *focus* su *broker* e mercati dei titoli. Essa si impegna a garantire l'integrità dei mercati e la tutela degli investitori.

7. Timori normativi e proposte nella nuova dimensione del *capital market*

Il dilemma fondamentale con cui la dottrina, la giurisprudenza e il legislatore si stanno confrontando, anche in un'ottica comparatistica, è se gli agenti artificiali debbano essere considerati soggetti legalmente responsabili o meno.

Con gli strumenti normativi ad oggi disponibili, è intrinsecamente impossibile discutere di sanzioni che colpiscano direttamente i sistemi di IA, soprattutto nella loro accezione più evoluta e in continuo divenire. Questo ragionamento ci porterebbe a ritenere che l'idea di una responsabilità autonoma dell'agente artificiale sia illusoria e che questa dipenda esclusivamente dalle decisioni prese dal programmatore e/o dall'utente nelle rispettive fasi di gestione dell'algoritmo.

È opportuno evidenziare come, nonostante l'intelligenza artificiale sia ritenuta

una fonte di rischio, essa sia ancora considerata dal legislatore attuale un oggetto e non un soggetto.

Nei sistemi di IA forti, nella quasi totalità dei casi, l'azione dell'operatore algoritmico non può essere attribuita *tout court* alla persona fisica, soprattutto a causa della mancanza dell'elemento soggettivo richiesto dal reato specifico che viene commesso. Ciò è dovuto all'autonomia decisionale dell'operatore artificiale, che agisce in modo indipendente e libero nel determinare come e quando commettere l'azione potenzialmente criminosa.

Dal punto di vista penale, l'approccio che si concentra sul controllo del rischio farebbe derivare la responsabilità da "omissione", nel caso in cui l'agente artificiale causi danni e l'evento avverso poteva essere evitato. In tal caso, il programmatore o l'utilizzatore potrebbero essere ritenuti responsabili per non aver gestito correttamente il sistema di IA e/o per non aver implementato misure preventive adeguate. Invero, la posizione di "garanzia", come il "controllo" su agenti artificiali, non risolve completamente il problema dell'imputazione e ciò anche perché l'utilizzo di sistemi di intelligenze artificiali impegna spesso *team* diversi, rendendo difficile la distribuzione delle responsabilità tra le persone fisiche a qualunque titolo coinvolte. Alla luce di quanto detto, alle persone interessate si potrebbe attribuire una responsabilità penale omissiva soltanto mediante l'attuazione di adeguate misure di progettazione preventive e di monitoraggio successivo delle azioni algoritmiche avanzate. In tali circostanze, il legislatore potrebbe concedere ai sistemi di IA un alto grado di autonomia, ma sempre all'interno di limiti controllabili dall'uomo.

Volendo osare un approccio più azzardato, ci si potrebbe spingere fino ad immaginare un sistema flessibile, che sia in grado di adattare rapidamente i principi o la normativa di settore alle repentine evoluzioni dell'IA nei mercati finanziari, con una logica che richiami (almeno su base concettuale) quella di uno "*smart contract*": si parlerebbe, in tal caso, di "*smart law*". Ovviamente, il tutto dovrebbe avvenire nell'ambito di limiti definiti a monte, in modo il più possibile dinamico, da un legislatore sempre più "*smart*". I presupposti ci sarebbero tutti[44].

8. Conclusioni

Il complesso panorama dell'intelligenza artificiale nei mercati finanziari richiede

un approccio bilanciato e proattivo. La distinzione tra IA deboli e forti evidenzia la necessità di adeguare le norme alla crescente autonomia degli algoritmi.
Una possibile strategia normativa potrebbe consistere nello spostare il *focus* dalla definizione di regole specifiche – che rischierebbero di divenire subito obsolete – allo stabilire principi cui ispirarsi nella regolamentazione dell'IA[45]. Potrebbero, ad esempio, essere imposti obblighi o restrizioni ai creatori e/o agli utilizzatori degli algoritmi per prevenire dinamiche illecite e dannose.
In tale contesto, la sfida principale rimane riuscire a bilanciare lo sviluppo tecnologico con la sicurezza dei mercati finanziari.
L'utilizzo ponderato dell'attribuzione della responsabilità agli esseri umani, della socializzazione dei danni e di soluzioni pionieristiche, come il riconoscimento della personalità giuridica ai sistemi di IA forti o l'approccio "*smart law*", consentirebbero agli operatori del diritto di affrontare in maniera più oculata gli illeciti nella nuova dimensione del *capital market*.

1. F. Consulich, M. Maugeri, C. Milia, T.N. Poli, G. Trovatore, *AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?*, in *Quaderni giuridici CONSOB*, 29, 2023.
2. L'arbitraggio è l'atto di acquistare e vendere contemporaneamente *asset* simili su mercati diversi al fine di sfruttare differenze di prezzo. I *trader* che praticano l'arbitraggio cercano di acquistare un *asset* a un prezzo più basso e poi venderlo a un prezzo più alto su un altro mercato, generando un profitto. L'arbitraggio statistico deriva da un insieme di strategie di investimento algoritmiche basate su dati statistici. Questa tattica mira a trarre vantaggio dai movimenti relativi dei prezzi su molti mercati diversi. L'obiettivo principale è generare profitti di *trading* superiori a quelli tipici per investitori di grandi dimensioni. L'arbitraggio statistico non è adatto al *trading* ad alta frequenza, ma piuttosto al *trading* con una velocità media, con periodi di durata variabile, da poche ore a diversi giorni. Nell'arbitraggio statistico, un *trader* apre simultaneamente posizioni lunghe e corte per sfruttare le inefficienze nei prezzi di *asset* correlati. Ad esempio, se un *trader* ritiene che il prezzo di X sia sovrastimato e quello di Y sia sottostimato, aprirà una posizione lunga su X e contemporaneamente una posizione corta su Y. Questa strategia è spesso chiamata "*pairs trading*" o *trading* in coppia. L'arbitraggio di latenza sfrutta le piccole differenze di tempo nella trasmissione delle informazioni tra fonti o luoghi diversi. Gli algoritmi "HFT" ("*High-Frequency Trading*") specializzati monitorano le discrepanze tra i flussi di dati provenienti da diverse borse. Se individuano una discrepanza, possono eseguire ordini per trarre vantaggio da questa differenza temporale.
3. Sul punto cfr. E. Mostacci, *L'intelligenza artificiale in ambito economico e finanziario*, in *dpceonline.it*, 1, 2022, pp. 361 ss.

4. Con il termine "*front running*" si indica una pratica illegale che sfrutta l'asimmetria informativa di chi emette l'ordine di compravendita di uno strumento finanziario. Gli HFT, sfruttando in anteprima la conoscenza dell'ordinativo effettuato (magari di importo elevato) inciderebbero sul prezzo dello strumento interessato e, immediatamente prima di lanciare l'ordine sul mercato acquisterebbero, a titolo "personale", il prodotto finanziario (se trattasi di ordinativo di acquisto) o lo venderebbero (se trattasi di ordinativo di vendita). Così l'operatore trarrebbe profitto dall'aumento del prezzo del titolo (acquisto) o eviterebbe di avere perdite per la riduzione del medesimo (vendita).
5. Il termine "*Big Data*" si riferisce a insiemi di dati di dimensioni molto grandi e complessi, che superano la capacità di gestione e analisi dei tradizionali *software* e strumenti di database. Questi dati sono caratterizzati da tre principali dimensioni: volume (la quantità di dati), varietà (la diversità dei tipi di dati) e velocità (la velocità con cui i dati vengono generati e devono essere processati). Gli approcci tradizionali di gestione e analisi dei dati spesso non sono sufficienti per trattare con successo le sfide presentate dai *Big Data*; quindi, sono necessarie nuove tecnologie e metodologie per estrarre informazioni significative da tali masse di dati.
6. "*Alternative Data*" (dati alternativi) è un termine che si riferisce a tipi di dati non tradizionali o non convenzionali, utilizzati per prendere decisioni finanziarie o aziendali. Questi dati vanno oltre le fonti di dati *standard* come i dati finanziari pubblici o i *report* aziendali. Gli *alternative data* possono includere una vasta gamma di informazioni provenienti da fonti come *social media*, tracciamenti di posizione, dati di sensori, dati di transazione e altre fonti non tradizionali. Questi dati possono fornire nuove prospettive e *insight* che vanno oltre ciò che è disponibile attraverso le fonti di dati convenzionali, contribuendo a migliorare le analisi e le decisioni.
7. Tuttavia, è importante rispettare le regole generali e le tempistiche appropriate per la diffusione di tali informazioni, come richiesto dal Regolamento 2014/596/UE del Parlamento Europeo e del Consiglio del 16 aprile 2014 relativo agli abusi di mercato (regolamento sugli abusi di mercato) e che abroga la direttiva 2003/6/CE del Parlamento europeo e del Consiglio e le direttive 2003/124/CE, 2003/125/CE e 2004/72/CE della Commissione. Ad esempio, il regolamento richiede che tali studi indichino la data e l'ora di prima diffusione alla clientela, garantendo così l'equità nelle operazioni e nella comunicazione delle informazioni.
8. Il "*market making*" è una strategia di *trading* in cui un *trader* agisce come intermediario facilitando il mercato, offrendo costantemente prezzi di acquisto e vendita per un determinato strumento finanziario, come azioni, opzioni o obbligazioni. L'obiettivo principale del *market maker* è mantenere liquidità nel mercato, riducendo così il divario tra i prezzi di offerta e domanda e contribuendo alla stabilità del mercato. I *market maker* guadagnano dalla differenza tra il prezzo di acquisto e il prezzo di vendita.
9. Il "*delta hedging*" è una tecnica di gestione del rischio utilizzata principalmente nel *trading* di opzioni. Si basa sul concetto di "delta", che rappresenta il tasso di cambio tra il prezzo di un'opzione e il prezzo dell'attività sottostante. Nel caso di un portafoglio proprietario, un

trader che detiene sia opzioni che l'attività sottostante, può utilizzare il *delta hedging* per bilanciare il rischio. Acquistando o vendendo l'attività sottostante in base alla variazione del delta, il *trader* cerca di neutralizzare l'effetto delle fluttuazioni dei prezzi delle opzioni e dell'attività stessa, riducendo il rischio complessivo del portafoglio.

10. Il "*trading direzionale*" è una strategia di *trading* in cui il *trader* cerca di trarre profitto dalla previsione del movimento futuro dei prezzi di un *asset* o di un mercato. Questo approccio prevede di aprire posizioni *long* (acquisto) se si prevede un aumento dei prezzi o posizioni *short* (vendita) se si prevede una diminuzione dei prezzi. Il *trading* direzionale è basato sull'analisi fondamentale e tecnica, nonché sulla valutazione di fattori economici, notizie di mercato e tendenze globali che possono influenzare i prezzi degli *asset*. Questa strategia comporta una maggiore esposizione al rischio di mercato, poiché le decisioni sono legate alla previsione dei movimenti dei prezzi.
11. Le "reti neurali" sono modelli computazionali ispirati al funzionamento del cervello umano. Sono composti da strati di unità interconnesse, chiamate neuroni artificiali, che elaborano *input* e generano *output*. Ogni connessione tra neuroni ha un peso associato che modifica l'influenza di un neurone sull'altro. Le reti neurali sono utilizzate in una vasta gamma di applicazioni, come riconoscimento di *pattern*, analisi dei dati, previsioni e molto altro. Possono apprendere dai dati attraverso il processo di adattamento dei pesi delle connessioni, permettendo loro di riconoscere schemi complessi e fare previsioni. Con riferimento alla difficoltà dei sistemi di IA di assicurare lo stesso *standard* qualitativo di ragionamento della mente umana, cfr. E. Battelli, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e tutela della persona*, in *Dir. fam. pers*., 3, 2022, p. 1099.
12. Il "*deep reinforcement learning*" (apprendimento profondo con rinforzo) è una sotto disciplina dell'apprendimento automatico (*machine learning*) in cui le reti neurali profonde vengono utilizzate per imparare a prendere decisioni ottimali attraverso l'interazione con un ambiente di riferimento. In questo contesto, l'ambiente fornisce *feedback* sotto forma di ricompense o punizioni in base alle azioni intraprese dall'agente di apprendimento. L'obiettivo è far sì che l'agente scopra strategie che massimizzino le ricompense nel tempo. Per approfondimenti su: "*machine learning*", "*supervised learning*", "*reinforcement learning*", "*unsupervised learning*", "*deep learning*" e altre classificazioni dei sistemi di IA, cfr. N. Abriani, G. Schneider, *Diritto delle imprese e intelligenza artificiale*, il Mulino, Bologna, 2021, pp. 21 ss.
13. Il "*trash & cash*" è una prassi manipolativa in cui vengono diffuse informazioni negative false (*trash*) su un prodotto finanziario per abbassarne il prezzo, seguito dall'acquisto (*cash*) a prezzi bassi. Una volta dissipate le informazioni negative, il prezzo può risalire, generando profitti illeciti.
14. Cfr. M. Cupella, *I mercati finanziari a confronto con nuove tecnologie e Social Media: le prospettive penalistiche dell'Affaire GameStop*, in *Bocconi Legal Papers*, 16, 2021, pp. 145 ss.
15. Una delle pratiche più ricorrenti nel *trading* ad alta frequenza è il "*trading on news*", che sfrutta il costante flusso informativo dai servizi di notizie finanziarie. L'HFT associa

strategie di *trading* a gruppi specifici di parole che sono statisticamente correlate a determinati flussi delle negoziazioni, sia positivi che negativi. Queste strategie si basano sulla risonanza delle notizie, misurata ad esempio dal numero di volte in cui una notizia viene menzionata nei sistemi informativi in rete.

16. In assenza di fenomeni manipolativi, il processo di formazione dei prezzi si ripete iterativamente, portando gradualmente alla convergenza verso il *fair value*. Quest'ultimo rappresenta il valore in linea con le caratteristiche fondamentali dello strumento finanziario sottostante e riflette le informazioni pubblicamente disponibili. La cosa però si complica con riferimento a sistemi di IA forti, difficilmente monitorabili e quindi non sempre in grado di mediare il proprio funzionamento con le esigenze evolutive sane delle negoziazioni.
17. Costante deve quindi essere la vigilanza sul rispetto della normativa in matria di *privacy*: Regolamento 2016/679/UE del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
18. Gli Stati membri devono garantire, però, che l'applicazione del sistema di sanzioni penali e amministrative non violi il principio del *ne bis in idem*.
19. Articolo 17, paragrafo 1, del Regolamento UE MAR.
20. I considerando dal n. 5 al n. 9 del Regolamento delegato UE 2016/522 forniscono ulteriori dettagli sulle prassi manipolative e sugli esempi riportati nel regolamento medesimo. Tuttavia, alcune di queste pratiche potrebbero essere considerate legittime, se la persona che compie operazioni o inoltra ordini interpretabili come manipolazione, è in grado di dimostrare che le motivazioni dietro tali azioni sono lecite e che le operazioni o gli ordini sono conformi alle prassi accettate sul mercato in questione.
21. Parere del Comitato economico e sociale europeo su "L'intelligenza artificiale – Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società" (2017/C 288/01).
22. Expert group on liability and new technologies, *Liability for Artificial Intelligence and other emerging digital technologies, European Commission*, 2019.
23. Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)).
24. Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI)). Cfr. G. Barone, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della Risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cass. pen*., 3, 2022, pp. 1180 ss.
25. Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)). Sul punto cfr. R. Trezza, *Intelligenza artificiale e persona umana: la multiforme natura degli algoritmi e la necessità di un "vaglio di meritevolezza" per i*

sistemi intelligenti, in *ratioiuris.it*, 2022.

26. 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 del 21 aprile 2021 COM (2021) 206 *final*. Sul punto Cfr. F. Donati, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, in *Dir. Un. eur*., 3-4, 2021, pp. 453 ss.
27. Con riferimento alla dottrina che propende per regole dettagliate basate sul principio di precauzione Cfr. T.E. Frosini, *L'orizzonte giuridico dell'intelligenza artificiale*, in *Dir. inf*., 1, 2022, p. 12.
28. La Proposta di Regolamento europeo sull'intelligenza artificiale del 21 aprile 2021 *cit*., parte dal presupposto delle normali regole di attribuzione della responsabilità all'essere umano, ma cerca di evitarne il più possibile l'applicazione. La prevenzione del danno dovrebbe quindi essere garantita attraverso l'implementazione di obblighi di supervisione (il cosiddetto "*duty of human oversight*"), richiedendo che i sistemi intelligenti siano progettati e sviluppati in modo da poter essere monitorati dall'essere umano, in un processo di controllo continuo.
29. 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) del 28 settembre 2022, COM(2022) 496 *final.* Sul punto cfr. G. Proietti, *Sistemi di Intelligenza Artificiale e Responsabilità: la proposta di AI Liability Directive, in dirittobancario.it*, 2022. Per argomentazioni speculari, cfr. E. Bocchini, *Contro la "soggettivizzazione" dell'intelligenza artificia*le, in *Il Nuovo Dir. Soc*., 2, 2023, pp. 195 ss.
30. Con riferimento alla responsabilità civile scaturente dai danni prodotti dai sistemi di IA, cfr. C. Leanza, *Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel Terzo Millennio*, in *Resp. civ. prev*., 3, 2021, pp. 1011 ss.
31. D.lgs. n. 58/1998 (Testo unico delle disposizioni in materia di intermediazione finanziaria, ai sensi degli articoli 8 e 21 della legge 6 febbraio 1996, n. 52 – TUF), aggiornato con le modifiche apportate dal d.lgs. n. 29/2023, in vigore dal 7 aprile 2023 e dai d.lgs. nn. 30 e 31 del 2023, in vigore dall'8 aprile 2023.
32. Il 1° febbraio 2022 è entrata in vigore la l. n. 238/2021 (Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – legge europea 2019-2020), che ha modificato la disciplina degli abusi di mercato. Nel dettaglio, l'art. 26 della legge europea 2019-2020 è intervenuta direttamente sulle disposizioni sanzionatorie previste dal d.lgs. n. 58/1998; il TUF Tra le principali novità della Legge Europea abbiamo: l'inasprimento delle pene per l'*insider* primario; l'introduzione esplicita della punibilità anche dell'*insider* secondario; la limitazione dell'applicabilità della confisca obbligatoria *ex* art. 187 TUF al solo profitto derivante dal reato.
33. Corte EDU, sentenza 4 marzo 2014, Ricorso n. 18640/10, *Grande Stevens e altri c. Italia*. In relazione all'illecito amministrativo, cfr. E. Amati, *L'illecito amministrativo di manipolazione del mercato e le persistenti criticità del doppio binario sanzionatorio*, in

Giur. comm., 2, 2021, pp. 263 ss.

34. Corte EDU, sentenza 8 giugno 1976, Ricorso n. 5100/71, *Engel e altri c. Paesi Bassi*.
35. La Corte giust., sentenza 20 marzo 2018, C-537/16, *Garlsson Real Estate SA c. Consob*, ECLI:EU:C:2018:193, e Corte giust., sentenza 20 marzo 2018, C-596/16 e C-597/16, *Di Puma c. Consob*, ECLI:EU:C:2018:192, qualifica le sanzioni sostanzialmente penali alla luce della natura dell'illecito e della gravità della sanzione.
36. Corte cost., sentenza 21 marzo 2019, n. 63; Corte cost., ordinanza 10 maggio 2019, n. 117.
37. Corte giust., sentenza 20 marzo 2018, C-524/15, *Menci*; Corte giust., sentenza 20 marzo 2018, C-537/16, *Garlsson Real Estate SA e altri*, cit.; Corte giust., sentenza 20 marzo 2018, C-596/16 e C-597/16, *Di Puma c. Consob*, cit.
38. Cass. pen., 15 aprile 2019, n. 3999.
39. Gli *Execution throttles* sono delle limitazioni o restrizioni applicate alla frequenza o alla velocità con cui determinate azioni o processi possono essere eseguiti. Essi vengono spesso imposti per evitare usi eccessivi e comunque inopportuni degli algoritmi finanziari con effetti dannosi.
40. L'*order stuffing* è una pratica con cui viene immesso sul mercato un enorme numero di ordini, poi subito rimosso prima dell'esecuzione.
41. *FINRA Rules, Rule* 6190; *NMS Plan to Address Extraordinary Market Volatility* (modificato dall'*Approval Order* della SEC, *Exchange Act Release* No.77679) 11 (2016).
42. La US SEC è un'agenzia governativa statunitense responsabile della regolamentazione e supervisione dei mercati finanziari, delle società di investimento e delle imprese pubbliche negli Stati Uniti. La SEC svolge un ruolo importante nel garantire la trasparenza, l'equità e l'integrità nei mercati finanziari e proteggere gli investitori da pratiche fraudolente e manipolative.
43. La *Financial Industry Regulatory Authority* (FINRA) è stata costituita nel luglio 2007. Essa è nata dalla fusione della *National Association of Securities Dealers* (NASD) e della divisione di regolamentazione del *New York Stock Exchange* (NYSE).
44. Banca d'Italia, Università Cattolica del Sacro Cuore, Università Roma Tre, *Caratteristiche degli smart contract - Draft v.1.0 – giugno 2023*.
45. Sul punto cfr. R. Sadaf, O. Mccullagh, C. Grey, E. King, B.Sheehan, M. Cunneen, *Algorithmic Trading, High-frequency Trading: Implications for MiFID II and Market Abuse Regulation (MAR) in the EU*, in *www.ssrn.com*, 2021.