LUISS

Dipartimento di Giurisprudenza

Cattedra di Macchine Intelligenti e Diritto

TRADING ALGORITMICO ED INTELLIGENZA ARTIFICIALE: ANALISI E VALUTAZIONI DEL SISTEMA NORMATIVO IN TEMA DI MANIPOLAZIONI DI MERCATO E CYBERSECURITY

Chiar.mo Prof. Giuseppe Corasaniti

RELATORE

Chiar.mo Prof. Gianluigi Ciacci

CORRELATORE

Pietro Maria Frati

Matr. 191183

CANDIDATO

Anno Accademico 2024/25

INDICE

CAPITOLO II – LE MANIPOLAZIONI DI MERCATO E IL TRADING ALGORITMICO

GLI ABUSI DI MERCATO: IL QUADRO NORMATIVO

LE CONDOTTE MANIPOLATIVE TRAMITE HIGH FREQUENCY TRADING

TRADING ALGORITMICO, INTELLIGENZA ARTIFICIALE E IMPLICAZIONI GIURIDICHE

CAPITOLO III – LA CYBERSECURITY E IL TRADING ALGORITMICO

LA CYBERSECURITY: IL QUADRO NORMATIVO DI RIFERIMENTO

CYBERSECURITY E TRADING ALGORITMICO

VALUTAZIONI

INTRODUZIONE

A partire dagli anni ’60 e ’70 del Novecento l’invenzione dei *transistor*, dei *computers*, dei primi linguaggi di programmazione nonché la diffusione delle reti e delle telecomunicazioni (ad es. *internet*) hanno dato luogo a quella che oggi è solita essere definita con il termine di “Terza rivoluzione industriale”. Tale rivoluzione ha pervaso innumerevoli settori interessando, in particolare, quello delle negoziazioni finanziarie. Grazie alla sempre maggior digitalizzazione dei flussi informativi e alla automazione dei processi le classiche modalità di *trading,* svolte da operatori umani, sono state con il tempo superate lasciando il posto a forme di negoziazione in cui la componente umana risulta essere assente e dove gli stessi *computer*, algoritmi e modelli matematici complessi regolano il funzionamento degli scambi. Tali modelli prendono il nome di *Trading* algoritmico (AT) e di *High Frequency Trading* (HFT).

Sulla scia di questa evoluzione tecnologica, a partire dalla seconda metà degli anni 2000, grazie all’aumento della capacità di calcolo dei microprocessori, unitamente alla proliferazione di enormi quantità di dati (i c.d. *big data*), si sono sempre più diffusi i sistemi di Intelligenza Artificiale (IA). In questa prospettiva, che si orienta verso la c.d. “Quarta rivoluzione industriale”,[1] gli operatori economici, come banche o imprese di investimento, hanno proceduto ad implementare direttamente i suddetti sistemi di IA all’interno dei modelli di *trading* algoritmico e ad alta frequenza “tradizionali”, allo scopo di incrementarne precisione, accuratezza ed efficacia.

Si evidenzia, come, da eventuali malfunzionamenti, errori o *bug* dei sistemi e anche da condotte opportunistiche degli stessi operatori economici (le c.d. manipolazioni di mercato) possano derivare significative turbolenze sui mercati e, data la forte interconnessione degli operatori nel settore finanziario, possano, altresì, verificarsi veri e propri rischi sistemici, con possibili ripercussioni sull’economia reale. In un siffatto contesto, è necessario che le istituzioni governative predispongano ed emanino normative adeguate, atte a regolare tali fenomeni onde garantirne un funzionamento controllato, corretto e sicuro. Pertanto, scopo del presente elaborato è quello di indagare e valutare

[1] SCHWAB, K. (2018). La quarta rivoluzione industriale (2ª ed.). FrancoAngeli.

quanto la normativa attuale in materia di *trading* algoritmico possa ritenersi appropriata rispetto ai rischi e pericolosità che discendono dall'impiego di una siffatta tecnologia.

In particolare, nel capitolo I la disamina sarà volta a inquadrare, a livello generale, il fenomeno del *trading* algoritmico e dell'*high frequency trading*, attenzionando, gli effetti prodotti sui mercati nonché la normativa europea di riferimento. In tale contesto, sarà introdotto il concetto di *Trading algoritmico 2.0,* un termine che intende alludere alla più recente versione di *trading* algoritmico, caratterizzata da un massivo ricorso all'intelligenza artificiale, da una sempre minor presenza umana e da una maggior autonomia del modello. In riferimento a tale ultima applicazione innovativa, sarà condotta un'analisi della legislazione UE allo scopo di comprendere se tale assetto normativo, originariamente predisposto per le forme "tradizionali" di negoziazione algoritmica, possa ritenersi adeguato a disciplinare anche forme di *trading* basate su IA, ovvero risulti essere obsoleto e tale da necessitare di un aggiornamento.

Nel capitolo 2 sarà invece approfondito il profilo concernente il comportamento "esterno" della macchina, ossia le possibili forme di manipolazione di mercato perpetrabili tramite i sistemi di *trading* algoritmico. In tale contesto, si analizzerà in che modo il ricorso all'intelligenza artificiale permetta di raggiungere non solo un miglioramento degli schemi operativi (*manipulation AI enanched*) ma, anche, di creare veri e propri "agenti autonomi" in grado di compiere l'illecito di manipolazione indipendentemente da istruzioni umane inserite all'interno dei programmi (*autonomous AI-driven manipulation).*

Preso atto del ruolo che l'IA è in grado di rivestire negli illeciti di manipolazione di mercato, si procederà a valutare l'adeguatezza della normativa europea ed italiana di riferimento.

In tale prospettiva, si cercherà di comprendere, in primo luogo, se le disposizioni che sanzionano tali illeciti siano adatte a ricoprire anche i casi di manipolazione realizzati tramite sistemi di intelligenza artificiale ovvero sorgano difficoltà di applicazione delle medesime norme in presenza di modelli algoritmici avanzati e complessi. In secondo luogo, la disamina procederà ad indagare i profili concernenti l'attribuzione delle responsabilità, una volta che l'illecito dovesse essere compiuto. Invero, laddove la manipolazione di mercato venisse perpetrata da un modello di *trading* potenziato con IA e dotato di autonomia operativa e decisionale, si potrebbero verosimilmente prospettare significativi problemi circa l'individuazione di un soggetto responsabile. Sul punto, si cercherà, quindi, di comprendere se l'assetto normativo vigente fondato sui tradizionali criteri di imputazione del dolo e della colpa riferiti al singolo individuo possa ritenersi ancora validamente appropriato ovvero si renda necessario elaborare nuove soluzioni, come, ad esempio, quella di dotare la macchina di un apposito *status* giuridico al fine di renderla responsabile.

Da ultimo, il capitolo 3 verterà sulla dimensione "interna" della macchina algoritmica affrontando il tema della *cybersecurity*. La trattazione di quest'ultimo argomento risulta essere necessaria in quanto le possibilità che dalla macchina possano discendere effetti pregiudizievoli e distorsivi sui mercati derivano non solo da un'attività "esterna" della medesima, qualificabile nei termini di una manipolazione di mercato, ma anche da eventuali incidenti o attacchi alle reti e sistemi informativi interni che ne consentono, in concreto, il funzionamento.

In questa prospettiva, dopo aver analizzato la legislazione eurounitaria ed italiana nonché le principali tipologie di minacce informatiche che possono colpire i sistemi di negoziazione algoritmica, si procederà ad una valutazione *de iure condito* della normativa, al fine di verificare se dalla disciplina in vigore emergano eventuali lacune o criticità applicative e se siano, conseguentemente, ipotizzabili soluzioni *de iure condendo* allo scopo di rafforzarne il quadro regolatorio.

CAPITOLO I

IL TRADING ALGORITMICO E l'HIGH FREQUENCY TRADING

TRADING ALGORITMICO E HIGH FREQUENCY TRADING: CONSIDERAZIONI INTRODUTTIVE

1.1 GLI ORDINI DI BORSA E I MERCATI FINANZIARI

L'analisi del funzionamento del *trading* algoritmico e dell'*high frequency trading,* oggetto della presente ricerca, presuppone un approfondimento introduttivo circa il mercato dei capitali attraverso la disamina del procedimento di formazione, trasmissione ed esecuzione degli ordini di borsa. Tale premessa si rende opportuna in relazione all'elevato grado di tecnicità degli argomenti trattati.

Da un punto di vista terminologico e concettuale, "*l'ordine di borsa*" consiste in una vera e propria "*proposta di negoziazione*" [2] che esprime la volontà di un soggetto di acquistare o vendere, su una piattaforma elettronica di negoziazione, una certa quantità di strumenti finanziari a un determinato prezzo.[3] Quando un investitore intende comprare o vendere uno strumento finanziario si rivolge, secondo la terminologia adottata dal legislatore italiano, ad un "intermediario" affinché questo esegua i suoi ordini dietro pagamento di un corrispettivo o commissione, dal momento che l'investitore non ha diritto di operare direttamente in borsa.[4]

---

[2] PERRONE, A. (2024). Il diritto del mercato dei capitali, Giuffrè Francis Lefebvre, Milano, p. 297.

[3] DE JONG, F., & RINDI, B. (2009). The microstructure of financial markets. Cambridge University Press, p. 21. (Finding that:" *Orders are traders' statements of their intention to trade. Orders stipulate the terms of the contract offered by market participants. They specify the agents' willingness to trade and the modality of execution*").

[4] LEIS, D. (2012). High-frequency trading: Market manipulation and systemic risks from an EU perspective (Working paper), p. 2.

Le principali categorie di ordini sono quelli "al limite" ("*limit orders"*), in cui l'investitore fissa il prezzo al quale è disposto a comprare o vendere, e gli ordini "al mercato" ("*market orders"*), che vengono invece eseguiti al miglior prezzo disponibile in quel momento.[5]

Il processo di negoziazione si compone, inoltre, di una serie di "*fasi*" [6] che nel loro complesso rappresentano il "ciclo di vita dell'ordine". Tale ciclo prende avvio con una decisione di negoziazione da parte del singolo *trader* in cui vengono fissati i parametri essenziali dell'ordine, come prezzo e quantità (fase di "*inizializzazione e generazione*" dell'ordine) e successivamente tale istruzione viene trasmessa all'intermediario.

L'intermediario finanziario è colui che è abilitato a svolgere "*servizi e attività di investimento*" [7] e che è in possesso di una apposita autorizzazione conferita dalle Autorità competenti dei singoli Stati membri per esercitare tale attività. Questa riserva di attività è prevista, nel nostro ordinamento, all'art. 18 comma 1, TUF [8] ed è rivolta principalmente alle SIM (ossia "società di intermediazione immobiliare", chiamate nel diritto europeo

---

[5] A proposito dei degli ordini di mercato vale la pena riportare la efficace analisi di Michael Lewis nel libro Flash Boys, best seller quando si tratta il tema HFT, in cui si riporta: "*Si consideri, ad esempio, un investitore che desidera acquistare 100 azioni di Procter & Gamble. Al momento in cui inserisce il suo ordine, il mercato delle azioni P&G presenta, poniamo, una quotazione di 80–80,02. Se l'investitore immette un market order, pagherà il prezzo in lettera — in questo caso, 80,02 dollari per azione. Tuttavia, un ordine a mercato comporta un rischio: il mercato potrebbe muoversi tra il momento in cui l'ordine viene inserito e il momento in cui raggiunge effettivamente il mercato. Il flash crash fu un'illustrazione drammatica di questo rischio: alcuni investitori che avevano inserito ordini a mercato finirono per pagare 100.000 dollari per azione P&G e per vendere quelle stesse azioni per un solo centesimo. Per limitare il rischio associato a un ordine a mercato, è stato ideato un secondo tipo di ordine: il limit order. L'acquirente delle azioni P&G potrebbe dire, ad esempio: «Acquisterò cento azioni, con un limite di 80 dollari e 3 centesimi per azione». In questo modo, egli si assicura di non pagare 100.000 dollari per azione; ma questo può comportare una mancata esecuzione — potrebbe infatti non riuscire ad acquistare le azioni, perché il prezzo desiderato non viene mai raggiunto")*. Si veda: LEWIS, M. (2014). Flash boys: A Wall Street revolt. W. W. Norton & Company, p. 169.

[6] PUJOL, G. (2009). Smart order routing and best execution (AMCIS 2009 Proceedings, Paper 155). Association for Information Systems, p. 4.

[7] Gli intermediari possono svolgere sia "servizi e attività di investimento" sia "gestione collettiva del risparmio". Nel primo caso le prestazioni dell'intermediario sono rese su base individuale a un cliente; nel secondo caso, invece, l'attività dell'intermediario si caratterizza per la raccolta di capitali tra una pluralità di investitori e nel loro investimento in modo collettivo e secondo una politica di gestione predeterminata. Ai fini del presente elaborato rilevano solamente quegli intermediari rientranti nella prima categoria.

[8] Decreto legislativo 24 febbraio 1998, n. 58, recante "Testo unico delle disposizioni in materia di intermediazione finanziaria" (TUF).

con il termine di "imprese di investimento"), alle imprese di investimento UE (gli omologhi esteri delle SIM) e alle banche.[9]

Tra i vari servizi e attività di investimento che l'intermediario può offrire figurano, per quello che interessa il presente elaborato, la "*negoziazione per conto proprio*" e la "*esecuzione di ordini per conto dei clienti*" quando le medesime hanno ad oggetto "*strumenti finanziari*" (Art. 1 comma 5, TUF).

Per quanto concerne il primo servizio di investimento, ovvero la "negoziazione per conto proprio", esso viene definito dall'art 5 *bis* del TUF come "*l'attività di acquisto e vendita di strumenti finanziari, in contropartita diretta"* per tale intendendosi la situazione in cui l'intermediario si renda controparte del contratto che ha ricevuto l'ordine di concludere. La caratteristica distintiva risiede nel fatto che l'intermediario impegnerà il proprio patrimonio nel compimento della operazione. La legge include nella nozione di "*negoziazione per conto proprio*" anche l'attività di "*market making*" che l'art. 5-*quater* definisce come la pratica in cui "*una persona si propone, nelle sedi di negoziazione e/o al di fuori delle stesse, su base continuativa, come disposta a negoziare per conto proprio acquistando e vendendo strumenti finanziari in contropartita diretta ai prezzi dalla medesima definiti".*

La "*esecuzione di ordini per conto dei clienti*" viene definita invece dal TUF come l'attività che comporta *"la conclusione di accordi di acquisto o di vendita di uno o più strumenti finanziari per conto dei clienti, compresa la conclusione di accordi per la sottoscrizione o la compravendita di strumenti finanziari emessi da un'impresa di investimento o da una banca al momento della loro emissione" (*Art 5, comma 5-*septies.1,* TUF*).* In questa circostanza l'intermediario, anziché porsi come controparte diretta del contratto, consente all'investitore di impartire un ordine sul mercato (ad es. per la compravendita di azioni) i cui effetti si ripercuoteranno nella sfera giuridica del cliente stesso, senza che vada ad intaccare il patrimonio dell'intermediario.[10] Nel concreto,

[9] Si noti che la dicitura "intermediario finanziario" presente nel TUF viene declinata nel diritto europeo (MiFID II) con il termine di "impresa di investimento".
[10] PERRONE, A. (2024). Il diritto del mercato dei capitali, Giuffrè Francis Lefebvre, Milano p. 215.

compito dell'intermediario è quindi quello di "*ricercare una o più controparti in vista dell'esecuzione di una operazione di vendita o acquist*o" [11].

Quando l'intermediario riceve l'ordine dal cliente, è suo dovere di indirizzalo al mercato (fase di "*trasmissione*" o "*routing*"). Una volta raggiunta la sede di negoziazione, l'ordine viene abbinato con un altro di segno opposto con le stesse caratteristiche di prezzo e quantità (fase di "*matching*") ed è in tale momento che il contratto potrà dirsi concluso e pronto per essere "eseguito". La successiva fase è quella di "*clearing*" (o "compensazione") in cui per neutralizzare il rischio di inadempimento (pagamento prezzo da parte del compratore e consegna dello strumento da parte del venditore) una controparte centrale (CCP) si inserisce nel contratto, assumendo la posizione di venditore nei confronti dell'acquirente e acquirente nei confronti del venditore. L'ultima fase consiste infine nel "*settlement*" (o "regolamento") nella quale avviene il trasferimento effettivo dei titoli e denaro tra le parti.

In questo *iter*, ruolo centrale dell'intermediario è quello di permettere al singolo investitore di tradurre in "*concreta*" la scelta "*astratta*" di *trading* e, pertanto, di favorire il collegamento con la piattaforma di negoziazione. Al giorno d'oggi esistono una molteplicità di mercati verso cui l'intermediario può instradare gli ordini, tanto da parlarsi di una vera e propria "*frammentazione*" [12] dei medesimi: accanto alle tradizionali borse valori (oggi conosciute con il termine di "*mercati regolamentati*"), [13] sono sorte, grazie alla disciplina europea, piattaforme alternative quali ad esempio, i "*sistemi multilaterali di negoziazione"* (*multilateral trading facilities,* MTF), [14] "*sistemi organizzati di*

[11] ANNUNZIATA, F. (2023). La disciplina del mercato dei capitali. Giappichelli, Torino, p. 105.
[12] MACKENZIE, D. (2018). Material signals: A historical sociology of high-frequency trading. *American Journal of Sociology, 123*(6), p. 1651.
[13] Per "Mercato Regolamentato" si intende un "sistema multilaterale amministrato e/o gestito da un gestore del mercato, che consente o facilita l'incontro, al suo interno e in base alle sue regole non discrezionali, di interessi multipli di acquisto e di vendita di terzi relativi a strumenti finanziari, in modo da dare luogo a contratti relativi a strumenti finanziari ammessi alla negoziazione conformemente alle sue regole e/o ai suoi sistemi" (Art. 1, co. 1, lett *w-ter*, TUF).
[14] Per "Sistema Multilaterale di Negoziazione" si intende "un sistema multilaterale gestito da un'impresa di investimento o da un gestore del mercato che consente l'incontro, al suo interno e in base a regole non discrezionali, di interessi multipli di acquisto e di vendita di terzi relativi a strumenti finanziari" (Art. 1, co 5-*octies*, lett. *a*, TUF).

negoziazione" (*organised trading facilities,* OTF), [15] "*internalizzatori sistematici"* (*systematic internaliser*, IS).[16]

Generalmente i mercati vengono distinti in due grandi macrocategorie: "*order driven*", chiamati anche "sistemi ad asta" e "*quote driven*", noti come "sistemi del *market maker*".

Nel caso di mercati *order-driven* gli ordini di acquisto e vendita, immessi dagli intermediari per conto degli investitori, vengono abbinati automaticamente, senza l'intervento di terze parti. I *limit order*s [17] vengono infatti inseriti ed esposti nel *book* di negoziazione secondo la regola della priorità prezzo-tempo: sul lato delle proposte di acquisto (*bid*) in ordine decrescente di prezzo; sul lato proposte di vendita (*ask*) in ordine crescente di prezzo. L'ordine presente sul *book* viene eseguito quando viene "colpito" da un *market order* (ossia un ordine al miglior prezzo) di segno opposto ovvero quando è già presente nel *book* un *limit order* corrispondente sul lato opposto. In mancanza di tali condizioni, il *limit order* permane nel *book* in attesa di esecuzione.[18] Un esempio di questa tipologia di mercato è costituito dal Mercato Telematico Azionario (MTA).

[15] Per "Sistema Organizzato di Negoziazione" di intende "un sistema multilaterale diverso da un mercato regolamentato o da un sistema multilaterale di negoziazione che consente l'interazione tra interessi multipli di acquisto e di vendita di terzi relativi a obbligazioni, strumenti finanziari strutturati, quote di emissioni e strumenti derivati" ((Art. 1, co 5-*octies*, lett. *c*, TUF).
[16] Per "Internalizzatore Sistematico" si intende "un'impresa di investimento che in modo organizzato, frequente, sistematico e sostanziale negozia per conto proprio eseguendo gli ordini dei clienti al di fuori di un mercato regolamentato, di un sistema multilaterale di negoziazione o di un sistema organizzato di negoziazione senza gestire un sistema multilaterale" (Art. 1, co. 5-*ter,* TUF).
[17] Per la definizione di *limit order* si rinvia a quanto descritto a p. 5.
[18] LEIS, D. (2012). High-frequency trading: Market manipulation and systemic risks from an EU perspective (Working paper), p.3.

proposte di acquisto			proposte di vendita		
Num. Proposte	Quantità titoli contrattati	Prezzo denaro (euro)	Prezzo lettera (euro)	Quantità titoli contrattati	Num. Proposte
2	1000	9.1 €	9.6 €	2000	4
4	1300	9.0 €	9.4 €	2500	1
7	600	8.9 €	9.3 €	1300	3
1	700	8.6 €	9.1 €	500	2

Fig. 1: esempio di libro ordini o book di negoziazione.

Al contrario, un mercato *quote driven* è guidato dalle quotazioni generate dai *market makers.* In altre parole*,* Il *market maker* espone con continuità due prezzi: un prezzo in "denaro" (*bid*) al quale è disposto ad acquistare e un prezzo in "lettera" (*ask*,) al quale è disposto a vendere. La differenza tra i due prezzi è denominata differenziale denaro-lettera (*bid-ask spread*).[19] Il vantaggio principale di questa seconda tipologia di mercato è l'immediatezza, in quanto il *market maker* assicura sempre la possibilità di effettuare negoziazioni in contropartita con il *market maker* stesso. Un esempio di questo mercato è il Nasdaq negli Stati Uniti.

Di fronte a un ampio numero di piattaforme di negoziazione, la disciplina europea ha imposto agli intermediari una serie di regole di comportamento che, nel complesso, mirano a proteggere l'investitore da potenziali rischi.

Tra queste, la regola della "*best execution*" impone agli intermediari – nell' esecuzione degli ordini dei clienti – l'obbligo di ottenere le migliori condizioni possibili, "*avendo riguardo al prezzo, ai costi, alla rapidità e alla probabilità di esecuzione e regolamento, alle dimensioni e della natura dell'ordine o di qualsiasi altra considerazione pertinente ai fini della sua esecuzione*" (art. 27 comma 1, MiFID).[20] Nel concreto, il compito dell'intermediario consiste nel redigere una procedura "scritta", da sottoporre al cliente, in cui sono individuate una serie di piattaforme di negoziazione. Una volta ricevuto l'ordine dal cliente, verrà successivamente selezionata quella che permetterà di ottenere

[19] Borsa Italiana. (n.d.). Mercato quote driven [Glossario]. Borsa Italiana. https://www.borsaitaliana.it/borsa/glossario/mercato-quote-driven.html.
[20] Direttiva 15 maggio 2014, 2014/65/UE del Parlamento europeo e del Consiglio, recante "Direttiva relativa ai mercati degli strumenti finanziari e recante modifica della direttiva 2002/92/CE e della direttiva 2011/61/UE" (MiFID II).

il miglior risultato, tenendo conto di una serie di fattori, tra i quali il prezzo dello strumento finanziario ma anche i costi relativi all' esecuzione (es. le commissioni praticate dalla piattaforma). In tal senso, il "*garantire il miglior risultato possibile* ha una valenza unicamente "*con riguardo a quelle sedi che l'intermediario ha preventivamente selezionato quali possibili venues* (piattaforme, n.d.r.) *all' atto dell'elaborazione della strategia*".[21]

Al fine di perseguire l'obiettivo della "*best execution*", sono stati sviluppati e impiegati nel corso del tempo, da parte degli intermediari, sistemi automatici attraverso cui ottimizzare i processi di instradamento ed esecuzione degli ordini. Il riferimento è ai cosiddetti "*Automated Order Systems*" (AOR) e "*Smart Order Systems*" (SOR). [22] Essi sono strumenti di *routing* che intervengono nella fase di instradamento verso la piattaforma di negoziazione. In queste ipotesi è il programma informatico stesso a inviare l'ordine al mercato migliore. [23]

Più in particolare, i SOR "*selezionano la sede di esecuzione appropriata su base dinamica, ossia utilizzando in tempo reale i flussi di dati di mercato attraverso un insieme di regole. Tali disposizioni consentono un'allocazione dinamica dell'ordine verso la sede di esecuzione che offre le condizioni migliori al momento dell'immissione dell'ordine, includendo o escludendo i costi di transazione espliciti e/o altri fattori*".[24]

In conclusione, il procedimento di formazione, trasmissione ed esecuzione degli ordini costituisce l'impianto attraverso cui si realizza l'attività di negoziazione sui mercati finanziari. La comprensione delle diverse fasi del ciclo di vita dell'ordine, dei sistemi di accesso diretto al mercato, degli strumenti di instradamento automatizzato (SOR e AOR), nonché dei vincoli normativi cui gli intermediari sono soggetti, risulta cruciale per analizzare in maniera consapevole il funzionamento di sistemi complessi quali il *trading* algoritmico e, in particolare, il *trading* ad alta frequenza.

---

[21] ANNUNZIATA, F. (2023). La disciplina del mercato dei capitali. Giappichelli, Torino, p. 145.
[22] Sulla differenza si rinvia al paragrafo 1.2.
[23] STOLL, H. R. (2006). Electronic trading in stock markets. *Journal of Economic Perspectives, 20*(1), p. 156.
[24] GOMBER, P., ARNDT, B., LUTAT, M., & UHLE, T. E. (2011). High-frequency trading (Working paper), p. 18.

1.2 DEFINIZIONI NORMATIVE

L'obiettivo di regolare i fenomeni della negoziazione algoritmica (*trading* algoritmico o AT) e della negoziazione ad alta frequenza (*High Frequency Trading* o HFT) in modo da limitarne i potenziali impatti negativi e ridurne i rischi, ha spinto il legislatore europeo ad adottare due differenti pacchetti normativi: la Direttiva n. 65 del 2014 MiFID II, che si sostituisce alla precedente Direttiva n. 39 del 2004 (MIFID I) [25] e il Regolamento n. 600 del 2014 (MiFIR). [26]

Entrambe rappresentano le fonti normative di riferimento che disciplinano i mercati finanziari, assieme ad un più ampio novero di fonti di livello secondario (*Regulatory Technical Standards,* RTS) [27] che ne costituiscono una specifica attuazione.

Da un punto di vista definitorio la MiFID II qualifica il *trading* algoritmico all'Art 4(1)(39) come la *«tecnica di negoziazione di strumenti finanziari in cui un algoritmo informatizzato determina automaticamente i parametri individuali degli ordini come, ad esempio, se e quando avviare l'ordine, i tempi, il prezzo o la quantità dell'ordine o come gestire l'ordine dopo la sua presentazione, con intervento umano minimo o nullo e non comprende i sistemi utilizzati unicamente per trasmettere ordini a una o più sedi di negoziazione, per trattare ordini che non comportano la determinazione di parametri di trading, per confermare ordini o per eseguire il trattamento post-negoziazione delle operazioni eseguite».*

L'art. 4(1)(40) definisce, altresì, l'*High Frequency Trading* come *«qualsiasi tecnica di negoziazione algoritmica caratterizzata da: a) infrastrutture volte a ridurre al minimo le latenze di rete e di altro genere, compresa almeno una delle strutture per l'inserimento algoritmico dell'ordine: co-ubicazione, hosting di prossimità o accesso elettronico*

---

[25] Direttiva 21 aprile 2004, 2004/39/CE del Parlamento europeo e del Consiglio, recante "Direttiva relativa ai mercati degli strumenti finanziari, recante modifica delle direttive 85/611/CEE e 93/6/CEE del Consiglio e della direttiva 2000/12/CE del Parlamento europeo e del Consiglio, e recante abrogazione della direttiva 93/22/CEE del Consiglio" (MiFID I), in GUUE L 145, pp. 1–44.

[26] Regolamento (UE) 15 maggio 2014, n. 600/2014 del Parlamento europeo e del Consiglio, recante "Regolamento relativo ai mercati degli strumenti finanziari e recante modifica del regolamento (UE) n. 648/2012" (MiFIR), in GUUE L 173, pp. 84–148.

[27] I Regulatory Technical Standards (RTS) sono adottati dalla Commissione europea, su proposta dell'ESMA, ai sensi dell'art. 10 del regolamento (UE) n. 1095/2010, e specificano aspetti tecnici dell'attuazione della normativa di settore. Pur non avendo natura di atti legislativi in senso stretto, tali atti sono giuridicamente vincolanti e direttamente applicabili negli ordinamenti nazionali.

diretto a velocità elevata; b) determinazione da parte del sistema dell'inizializzazione, generazione, trasmissione o esecuzione dell'ordine senza intervento umano per il singolo ordine o negoziazione, e c) elevato traffico infragiornaliero di messaggi consistenti in ordini, quotazioni o cancellazioni».

Analoghe sono le definizioni contenute all'interno del Testo Unico Finanziario (TUF), all'articolo 1 co. 6-*quinquies* (per la definizione di Negoziazione Algoritmica) e *septies* (concernente la definizione di Negoziazione ad Alta Frequenza), i quali, senza sostanziali differenze, riprendono le formulazioni contenute nella MIFID II.

Dalle definizioni sopra riportate possiamo tracciare le seguenti linee di confine: la prima concerne il rapporto tra *trading* algoritmico e qualsiasi altro strumento di negoziazione non algoritmico; la seconda concerne invece il rapporto tra *trading* algoritmico e *high frequency trading.*

Rispetto alla prima distinzione, la Direttiva MIFID II fornisce due di criteri chiave per comprendere quando una negoziazione possa considerarsi "algoritmica".[28] Innanzitutto, l'art. 4(1)(39) indica come primo requisito l'"*intervento umano minimo o nullo*". Tale formulazione viene specificata dal regolamento delegato n. 565 del 2017 [29] che all'art. 18 afferma: *"un sistema è considerato operare in assenza o con un limitato intervento umano se, per qualsiasi processo di ordine o di generazione della quotazione o per qualsiasi processo volto a ottimizzare l'esecuzione dell'ordine, un sistema automatizzato prende le decisioni in qualsiasi fase dell'inizializzazione, della generazione, della trasmissione o dell'esecuzione degli ordini o delle quotazioni in base a parametri predeterminati".*

Dalla formulazione in questione si ricava che si è in presenza di un intervento umano "*minimo o nullo*" ogniqualvolta un sistema automatizzato interviene con decisioni autonome, prese in base parametri predeterminati in qualsiasi fase del ciclo di vita dell'ordine comprendente l'inizializzazione, la generazione, la trasmissione e la esecuzione.

[28] Per algoritmo, in informatica, si intende generalmente l'insieme di istruzioni che una macchina esegue per compiere un'elaborazione o risolvere un problema.

[29] Regolamento delegato (UE) 25 aprile 2016, 2017/565 della Commissione, recante "Regolamento che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda gli obblighi organizzativi e le condizioni di esercizio dell'attività delle imprese di investimento nonché le definizioni ai fini di detta direttiva" (Regolamento delegato MiFID II), in GUUE L 87, pp. 1–83.

L'art 4(1)(39) individua poi come secondo requisito "*l'impiego di algoritmi informatizzati che determinano automaticamente i parametri individuali degli ordini"*, quali, ad esempio, l'avvio dell'ordine, la tempistica, il prezzo e la quantità (la c.d. fase di "*generazione dell'ordine*").

Tuttavia, come indicato dal Considerando n. 21 del Reg. Del. 565/2017, la negoziazione algoritmica può ricorrere anche nella fase di "*esecuzione dell'ordine".* Invero, laddove l'ordine, già generato, venga eseguito tramite un algoritmo che incida su parametri rilevanti dell'ordine stesso, diversi dalla mera scelta della sede di negoziazione alla quale è destinato, [30] si configura, anche in questa ipotesi, una "negoziazione algoritmica". [31] [32]

In tale prospettiva sono idonei a rientrare nella nozione di negoziazione algoritmica i c.d. Smart Order Routers (SOR), intesi come sistemi di trasmissione degli ordini che impiegano algoritmi in grado di incidere su parametri dell'ordine diversi dalla mera scelta della sede di negoziazione. [33]

In particolare, lo *Smart Order Router (SOR) è in grado di suddividere l'ordine principale (parent order) in ordini secondari più piccoli (child orders) o di determinare quando tali ordini secondari devono essere immessi sul mercato*. [34]

Al contrario, restano esclusi dall'ambito applicativo dell'*algorithmic trading* gli *Automated Order Routers* (AOR), i quali, pur facendo uso di algoritmi, si limitano a determinare solamente la sede o le sedi di negoziazione in cui l'ordine deve essere inserito, senza modificarne alcun parametro sostanziale.[35] [36]

Quindi, in sintesi, il *trading algoritmico* consiste in uno strumento di negoziazione in cui: a) l' intervento umano è nullo o limitato; b) algoritmi informatizzati sono impiegati nel determinare i parametri individuali degli ordini o nella fase di "*generazione dell'ordine*",

---

[30] Considerando n. 22 reg. delegato (UE) 2017/565.
[31] EUROPEAN SECURITIES AND MARKETS AUTHORITY. (2014). Final report: ESMA's technical advice to the Commission on MiFID II and MiFIR (ESMA/2014/1569). ESMA, Paris, p. 323.
[32] EUROPEAN SECURITIES AND MARKETS AUTHORITY. (2022). Questions and answers on MiFID II and MiFIR market structures topics (ESMA70-872942901-38). ESMA, Paris, p. 34.
[33] Si veda nota n. 29.
[34] BUSCH, D. (2017). MiFID II: Regulating high frequency trading, other forms of algorithmic trading and direct electronic market access, *Law and Financial Markets Review, 10*(2), 2016), p. 78.
[35] EUROPEAN SECURITIES AND MARKETS AUTHORITY. (2014). Final report: ESMA's technical advice to the Commission on MiFID II and MiFIR (ESMA/2014/1569), p. 324.
[36] CONSOB. (2023). Guida operativa – Algo-Trading e High Frequency Trading: mappatura del quadro regolamentare e degli obblighi di comunicazione alla Consob (Sez. 2, par. 2.1.5).

o nella fase di "*esecuzione dell'ordine*" a patto che in quest'ultimo caso l'algoritmo incida su parametri diversi dalla mera scelta della sede di negoziazione (in tal caso si parlerà di "*ottimizzazione del processi di esecuzione dell'ordine*").

Restano esclusi dalla nozione di AT secondo l'art 4 (1)(39) tutti quei sistemi utilizzati per "*trasmettere ordini a una o più sedi di negoziazione"*; per "*trattare ordini che non comportano la determinazione di parametri di trading"*; per "*confermare ordini"* o per "*eseguire il trattamento post-negoziazione delle operazioni eseguite.* Queste ultime ipotesi fanno riferimento a sistemi che svolgono la funzione di mero supporto informatico e *"la cui operatività, seppur automatizzata, non è in grado di influire in maniera significativa sul processo di determinazione degli elementi* (i parametri dell'ordine, n.d.r.) *che qualificano gli ordini di trading*" .[37]

La seconda distinzione da approfondire rispetto al presente studio concerne il rapporto tra il *trading* algoritmico e il *trading* ad alta frequenza. Quest'ultimo si qualifica come *un sottoinsieme specifico della negoziazione algoritmica, in cui un sistema di trading analizza i dati del mercato a velocità elevata per poi inviare o aggiornare un gran numero di ordini entro un tempo brevissimo*.[38]

L' art 4(1)(40) indica le caratteristiche che contraddistinguono l'*High Frequency Trading*.

La prima viene indicata alla lett. a) e fa riferimento all'infrastruttura tecnologica che ne permette in concreto il funzionamento. Essa comprende: la co-ubicazione, *l'hosting* di prossimità e l'accesso elettronico diretto a velocità elevata. Affinché possa ricorrere la negoziazione "ad alta frequenza" è necessario, pertanto, che l'operatore faccia ricorso ad almeno una di queste infrastrutture.

Per le prime due ipotesi, si tratta di sistemi *hardware* in grado di ridurre i tempi di latenza, ossia il tempo di trasmissione degli ordini al mercato.[39]

---

[37] ARACINO, U., & MARGARIA, R. (2015). Negoziazione algoritmica e mirror trading: dinamiche operative e qualificazioni giuridiche. Diritto Bancario – Approfondimenti. https://www.dirittobancario.it/art/negoziazione-algoritmica-e-mirror-trading-dinamiche-operative-e-qualificazioni-giuridiche/ (accesso 20 luglio 2025).

[38] Considerando 61 Direttiva n. 65 del 2014 (MiFID II).

[39] «Tempo di latenza (o solo latenza): il lasso di tempo che intercorre tra il momento in cui viene inviato un comando di lettura o scrittura a una unità periferica e il momento in cui effettivamente inizia il trasferimento dei dati». *Treccani. (n.d.). Latenza [Vocabolario on line]. Istituto dell'Enciclopedia Italiana Treccani.* *https://www.treccani.it/vocabolario/latenza* *(ultimo accesso 20 luglio 2025.* Nel contesto dei

Con *co-location* si fa riferimento, in particolare, al servizio commerciale, offerto dalle piattaforme di negoziazione, che consente agli operatori ad alta frequenza di prendere in locazione degli appositi spazi (‘*racks*’) presso le sedi di negoziazione, al fine di posizionarvi i propri *server*.[40] Dal punto di vista normativo, l’art. 48, par. 12, lett. *d*), MiFID II richiede alle sedi di negoziazione che “*i servizi di co-ubicazione siano trasparenti, equi e non discriminatori*”, cercando di garantire, in tal senso, un *level playing field*.

Un’alternativa alla *co-location* è il c.d. *proximity central hosting*, e cioè un servizio di ospitalità informatica che un soggetto terzo, diverso dalla piattaforma di negoziazione, offre agli interessati per consentire a questi ultimi di operare i propri ordini di mercato da una posizione fisica prossima a quella della piattaforma prescelta.[41]

Per quanto concerne invece il termine “accesso elettronico diretto a velocità elevata”, ci si riferisce a una variante rispetto alla tradizionale modalità di generazione, trasmissione ed esecuzione degli ordini.[42]

Secondo l’art. 1 comma 6 *sexies* del TUF per “*accesso elettronico diretto*” (DEA) si intende “*un accordo in base al quale un membro o un partecipante o un cliente di una sede di negoziazione consente a un terzo l’utilizzo del proprio codice identificativo di negoziazione per la trasmissione in via elettronica direttamente alla sede di negoziazione di ordini relativi a uno strumento finanziario, sia nel caso in cui l’accordo comporti l’utilizzo da parte del terzo dell’infrastruttura del membro, del partecipante o del cliente, o di qualsiasi sistema di collegamento fornito dal membro, partecipante o cliente per trasmettere gli ordini (accesso diretto al mercato, DMA) sia nel caso in cui non vi sia tale utilizzo (accesso sponsorizzato, SA)*”.

Con il DMA i soggetti possono, pertanto, accedere al mercato senza diventarne membri dello stesso, utilizzando le infrastrutture messe a disposizione da un partecipante al mercato e il codice identificativo di negoziazione di quest’ultimo.

---

mercati finanziari il tempo di latenza risulta essere quindi il tempo che intercorre tra l’invio di un’istruzione (es. un ordine di acquisto o vendita) e la sua esecuzione effettiva sul mercato.

[40] CAIVANO, V., et al. (2012). Il trading ad alta frequenza – Caratteristiche, effetti, questioni di policy (CONSOB Discussion Paper No. 5), p. 10.

[41] DI CIOMMO, F. (2019). Smart contract e (non-)diritto: Il caso dei mercati finanziari. *Nuovo Diritto Civile, IV* (1), p. 279.

[42] Per la descrizione circa la modalità tradizionale di generazione e trasmissione di ordini si faccia riferimento a quanto descritto nel paragrafo 1.1.

Lo *Sponsored Access (SA)* consente, invece, l'accesso diretto alla piattaforma di negoziazione utilizzando solamente il codice identificativo del partecipante (e non anche l'infrastruttura di quest'ultimo).

La seconda caratteristica dell'HFT (indicata alla lett. b) concerne il grado di autonomia del sistema. Nel caso dell'HFT gli algoritmi sono coinvolti nell'intero ciclo di vita dell'ordine, dalla fase di inizializzazione-generazione sino a quella di esecuzione, con esclusione completa dell'intervento umano. A tal riguardo, si può ragionevolmente concludere che, se l'AT si basa su un grado di autonomia "ampio" del sistema di negoziazione, in quanto vi è spazio per un intervento "umano" (l'art 1 co. 39 parla infatti "*intervento umano minino o nullo*"), nel caso dell'HFT il grado di autonomia è "totale", in quanto l'intervento umano è completamente assente.

La terza e ultima caratteristica (alla lett. c) riguarda invece il criterio quantitativo "*dell'elevato traffico giornaliero di messaggi, consistenti in ordini, quotazioni e cancellazioni*".

L'art. 19 del già citato regolamento delegato 565/2017 specifica che "*Un elevato traffico infragiornaliero di messaggi ai sensi dell'articolo 4, paragrafo 1, punto 40, della direttiva 2014/65/UE consiste nella presentazione in media di uno dei seguenti: a) almeno 2 messaggi al secondo in relazione a un singolo strumento finanziario negoziato nella sede di negoziazione; b) almeno 4 messaggi al secondo in relazione a tutti gli strumenti finanziari negoziati nella sede di negoziazione".* A tal proposito è opportuno precisare che i messaggi in questione devono essere relativi a strumenti finanziari per cui vi è un mercato "liquido" inteso come "*il mercato di uno strumento finanziario o di una categoria di strumenti finanziari in cui vi siano venditori e compratori pronti e disponibili su base continua"* (Art. 2, paragrafo 1, punto 17, del Reg. UE n. 600/2014 MiFIR).

Nonostante le definizioni contenute nella MiFID II cerchino di intercettare il fenomeno del *trading* algoritmico e di quello ad alta frequenza da un punto di vista molto ampio, *una enorme varietà di definizioni alternative circa l'HFT può essere ancora trovata in documenti ufficiali e nella letteratura accademica;*[43] ciò è dovuto principalmente al fatto che una enunciazione unitaria ancora non esiste a causa della natura multiforme e

[43] LERCH, M. P. (2022). Algorithmic trading and high-frequency trading. In R. Veil (Ed.), *European capital markets law* (3rd ed.), p. 46.

variabile di questa tecnologia. In ogni caso, le definizioni contenute nella MiFID II sembrano essere sufficientemente chiare da inquadrare il fenomeno in esame. Tuttavia, Il punto maggiormente critico pare essere il concetto di "intervento umano minimo o nullo" presupposto, dell'AT.

Dalla lettura dell'art. 18 non risulta essere di immediata intuizione in che misura la presenza dell'algoritmo sia tale da configurare una negoziazione "algoritmica", e in che misura "l'intervento umano" sia tale da escluderla. In altre parole, la norma non fornisce un'indicazione sufficientemente precisa circa l'individuazione di una soglia di intervento umano "minimo" entro la quale si possa considerare integrata la fattispecie di "negoziazione algoritmica" ed oltre la quale invece la medesima deve essere esclusa.

1.3 EVOLUZIONE STORICA

Apprendere il funzionamento dei sistemi algoritmici ad alta frequenza presuppone necessariamente una comprensione dell'impatto che questi hanno avuto nell'evoluzione del mercato dei capitali da un punto di vista storico.

Al riguardo, si rende necessaria un'analisi che ripercorra le tappe principali che hanno condotto alla comparsa e alla successiva affermazione di sistemi elettronici ed automatici nel contesto mercati finanziari, premettendo che si tratta di un fenomeno che si origina e sviluppa prevalentemente negli Stati Uniti d'America per poi diffondersi anche in Europa.

Fino agli anni '70 i mercati finanziari erano caratterizzati dalla presenza di pochi operatori, da una gestione completamente manuale e con negoziazioni che avvenivano per il tramite di intermediari, o *brokers,* che contattavano telefonicamente i clienti per proporre loro idee di investimento: questi ultimi, qualora avessero acconsentito, avrebbero dettato per telefono l'ordine di acquisto. Una volta ricevuta l'istruzione di compravendita dal cliente, il *broker* avrebbe poi contattato uno specialista ("*specialist*") che, nel *"trading floor"* della borsa, urlando tra la folla degli operatori, avrebbe cercato di abbinare l'ordine con un altro di segno opposto per poi eseguirlo, dando quindi conferma all'intermediario, che a sua volta avrebbe informato il cliente.[44] Questo processo risultava essere lento e spesso inficiato da errori, tra i quali, il più rilevante, quello della erronea comprensione dell'ordine da parte del *broker*.[45]

Nel 1976 fu introdotto presso il New York Stock Exchange (NYSE)[46] il "*designated order turnaround*" (DOT) e nel 1984 il Super-DOT. Questi sistemi permettevano la trasmissione elettronica di ordini dai *brokers* direttamente agli *specialists,* evitando conversazioni telefoniche e rappresentando, nel complesso, un primo passaggio verso una forma di *trading* elettronico.[47]

Durante gli anni '80, il Nasdaq,[48] una piattaforma di negoziazione completamente elettronica in cui le negoziazioni avvenivano con controparti i *market makers*[49]*,* introdusse un sistema noto come *Small Order Execution System* (SOES).[50]

A differenza dei mercati tradizionali, dove l'abbinamento e l'esecuzione di un ordine richiedevano ancora l'intervento umano dello *specialist*, il sistema SOES permetteva non solo l'invio elettronico dell'ordine a mercato (come nel caso del già citato DOT e SUP-dot) ma anche l'abbinamento e l'esecuzione automatica dello stesso, senza la necessaria presenza di uno specialista. In tale contesto, una particolare categoria di *traders,* noti come i "*SOES Bandits*",[51] iniziò ad effettuare numerose operazioni di *trading* al giorno,

---

[44] LEWIS, M. (2014). Flash Boys: A Wall Street Revolt. W. W. Norton & Company, p. 3.
(Finding that: "*The picture I'll bet most people have of the markets is still a picture a human being might have taken. In it, a ticker tape runs across the bottom of some cable TV screen, and alpha males in color-coded jackets stand in trading pits, hollering at each other*").

[45] ALDRIDGE, I. (2013). High-frequency trading: A practical guide to algorithmic strategies and trading systems (2nd ed.). John Wiley & Sons.

[46] Il *New York Stock Exchange* (NYSE) è il maggiore mercato azionario del mondo per capitalizzazione e per volume di scambi e il secondo (dopo il Nasdaq) per numero di società quotate.

[47] MCGOWAN, M. J. (2010). The rise of computerized high frequency trading: Use and controversy. *Duke Law & Technology Review, 9*(1), pp. 4–5.

[48] NASDAQ è l'acronimo di *National Association of Securities Dealers Automated Quotation*, cioè in italiano "Quotazione automatizzata dell'Associazione nazionale degli operatori in titoli". Questo mercato è stato istituito a Wall Street l'8 febbraio 1971 ed è stata la prima borsa al mondo esclusivamente elettronica. Cfr. Nota 21.

[49] Il Nasdaq è quindi un tipo di mercato *quote driven*.

[50] LEE, J., & SCHU, L. (2021). Regulation of algorithmic trading: Frameworks for human supervision and direct market interventions. *European Business Law Review*, p. 1.

[51] Per una lettura più approfondita si veda: HARRIS, J. H., & SCHULTZ, P. H. (1998). The trading profits of SOES bandits. *Journal of Financial Economics, 50*(2), pp. 39–62.

con lo scopo di trarre vantaggio da minime oscillazioni del prezzo degli strumenti finanziari o da ritardi nell'aggiornamento delle quotazioni dei *market makers*.[52]

L'alto numero di negoziazioni giornaliere assieme ad una elevata velocità di esecuzione, hanno portato a considerare tali *traders* come i precursori dell'HFT.[53]

Tuttavia, il vero punto di svolta lo si deve alla creazione nel 1997 della piattaforma di negoziazione *Island*. [54] Tale sede di negoziazione completamente elettronica permetteva una interazione *computer-to-computer,* [55] senza la necessita di controparti come *market makers* (NASDAQ) o *specialists* (NYSE), in cui gli abbinamenti, cancellazioni ed esecuzioni di ordini avvenivano in maniera completamente automatica e con commissioni molto basse.[56]

La piattaforma, grazie alle sue caratteristiche, ospitò le negoziazioni di numerose HFT *firms* (società di *trading* ad alta frequenza) permettendo loro di crescere e svilupparsi. Il successo fu tale che iniziarono a diffondersi altre sedi di negoziazione con caratteristiche analoghe che presero il nome di *Electronic Communication Networks* (ECN) alternative alle borse tradizionali (NYSE e NASDAQ). Tra i vantaggi apportati da queste nuove piattaforme si ricordano, in particolare, la riduzione dei costi di transazione, favorita da una maggior concorrenza tra ECN e borse tradizionali ma anche la possibilità di effettuare negoziazioni al di fuori degli orari di contrattazione tradizionali (le c.d. negoziazioni "*after hour*").[57]

Da un punto di vista normativo, decisivi sono stati infine i contributi della *Security Exchange Commission* (SEC, autorità federale preposta alla vigilanza delle borse statunitensi) che, con una serie di interventi, ha spianato definitivamente la strada all'affermazione dei sistemi di negoziazione ad alta frequenza: in particolare, si ricorda

---

[52] DI CIOMMO, F. (2019). Smart contract e (non-)diritto: Il caso dei mercati finanziari. *Nuovo Diritto Civile, IV* (1) p. 177.
[53] PUORRO, A. (2013). High frequency trading: Una panoramica (Banca d'Italia, Occasional Paper n. 198), p. 6.
[54] MACKENZIE, D. (2018). Material signals: A historical sociology of high-frequency trading. *American Journal of Sociology, 123*(6), p. 1668.
[55] *Ibidem.*
[56] La piattaforma *Island* può essere considerata a tutti gli effetti un esempio di mercato *order driven.*
[57] LEIS, D. (2012). High-frequency trading: Market manipulation and systemic risks from an EU perspective (Working paper), p. 8.

l'adozione nel 1998 del *Regulation Alternative Trading System* (Reg. ATS) [58] con cui è stato ufficialmente consentito l'utilizzo di piattaforme di *trading* alternative ai mercati regolamentati, ampliando così il novero delle sedi di negoziazione.

Nel 2005 la SEC ha poi varato il *Regulation National Market System* (Reg. NMS) [59] con lo scopo di modernizzare e rafforzare il mercato azionario nazionale. Al suo interno, rilevante da ricordare è la *Sub-Penny Rule* (*Rule* 612), che tutt'ora obbliga le sedi di negoziazione a adottare il sistema decimale nella quotazione dei titoli azionari con prezzo pari o superiore a un dollaro. Nel dettaglio, questa decimalizzazione mira a uniformare e ridurre l'incremento minimo di prezzo, fissandolo in modo univoco a 0,01. Una siffatta previsione ha pertanto spinto gli operatori a "*sviluppare sistemi in grado di sfruttare il nuovo minimo intervallo possibile di profitto, dal momento che la rischiosità di tale strategia è proporzionalmente diminuita (1 centesimo per azione) e le opportunità di trading, sebbene di valore atteso minore, sono incrementate*".[60]

Analogamente, anche in Europa a partire dagli anni duemila si è assistito ad importanti cambiamenti. Tra i più significativi, vi è stata l'adozione della Direttiva n. 39 del 2004, meglio nota come MiFID I [61] che ha abolito la "concentrazione" obbligatoria degli scambi su mercati regolamentati e ha aperto a nuove sedi di negoziazione come, ad esempio, i *Multilateral Trading Facilities* (MTF).

---

58 U.S. SECURITIES AND EXCHANGE COMMISSION. (1998, December 8). Regulation of Exchanges and Alternative Trading Systems (Securities Exchange Act Release No. 34-40760). *Federal Register, 63*, 70844–70951, spec. p. 70844.

59 U.S. SECURITIES AND EXCHANGE COMMISSION. (2005, June 9). Regulation National Market System (Regulation NMS) (Securities Exchange Act Release No. 34-51808; 17 C.F.R. pt. 242). *Federal Register, 70*(123), p. 37496 ss.

60 PUORRO, A. (2013). High frequency trading: Una panoramica (Banca d'Italia, Occasional Paper n. 198), p. 7.

61 Direttiva 21 aprile 2004, 2004/39/CE del Parlamento europeo e del Consiglio, recante "Direttiva relativa ai mercati degli strumenti finanziari, recante modifica delle direttive 85/611/CEE e 93/6/CEE del Consiglio e della direttiva 2000/12/CE del Parlamento europeo e del Consiglio, e recante abrogazione della direttiva 93/22/CEE del Consiglio" (MiFID I), in GUUE L 145 del 30 aprile 2004, pp. 1–44.

I cambiamenti sinora descritti hanno permesso una notevole evoluzione dei mercati finanziari. Le nuove tecnologie unite a cambiamenti normativi hanno contribuito tanto ad ampliare il novero dei soggetti che operano sui mercati quanto le stesse modalità di negoziazione. A questo si deve inoltre aggiungere un'elevata "frammentazione"[62] dei mercati che ha condotto alla presenza di numerose sedi di negoziazione alternative alle borse tradizionali e ha permesso un incremento delle opportunità di *trading*.

1.4 TRADING AD ALTA FREQUENZA ED EFFETTI SUI MERCATI

Per poter assicurare un'adeguata ed efficiente regolazione, ogni fenomeno destinato ad avere una rilevanza giuridica necessita di una comprensione, almeno nelle linee essenziali, del suo impatto e rilevanza. Comprendere quindi gli effetti che discendono da una siffatta tecnologia di negoziazione, positivi o negativi che siano, risulta essere fondamentale in quanto giustifica un intervento normativo che, a seconda delle circostanze, potrà essere più o meno severo

L'analisi a seguire sarà pertanto volta ad approfondire l'impatto che i sistemi di *trading* algoritmico e *high frequency trading* hanno sui mercati. *In primis,* verranno attenzionati quali siano gli operatori di *trading* ad alta frequenza nonché il volume delle negoziazioni riconducibili a tali sistemi automatizzati; *in secundis.* la disamina procederà poi ad indagare quali siano gli effetti positivi che discendono dall'impiego di una siffatta tecnologia di negoziazione nonché gli effetti negativi che possono in concreto ripercuotersi sui mercati.

1.4.1 DATI E VOLUMI SCAMBIATI

Da un punto di vista soggettivo, i principali attori coinvolti nel campo dell'AT e HFT sono imprese di investimento operanti con capitale proprio ("*HFT firms*") che costituiscono la maggioranza degli operatori (circa 48%); seguono unità operative

[62] MACKENZIE, D. (2018). Material Signals: A Historical Sociology Of High-Frequency Trading. *American Journal Of Sociology*, 123(6) p. 1651.

all'interno di intermediari finanziari chiamate "*proprietary trading desk of a multi service broker dealer*" (circa 46%) ed infine, in minima parte, fondi speculativi (6%).[63]

Da un punto di vista quantitativo, le negoziazioni effettuate tramite algoritmi hanno conosciuto nel tempo una sempre maggior diffusione. Bisogna premettere che un'indagine che ne quantifichi in termini numerici l'esatto numero risulta parecchio complicata, anche a causa dell'assenza di posizioni unanimi su che cosa si debba intendere per "negoziazioni ad alta frequenza". Ricerche da studi avanzati indicano, tuttavia, un largo impiego di questo strumento: nei mercati azionari statunitensi è stato registrato come il volume di scambi condotti tramite HFT sia giunto fino al 55 % del volume totale [64] con picchi addirittura fino al 73%, nel periodo compreso tra il 2009 e 2011. [65] Parallelamente, in Europa la quota di scambi sui mercati azionari effettuata tramite HFT è oscillata tra il 19 e 40% nel 2011, con un valore degli scambi pari al 39% nel 2012.[66]

Inoltre, merita essere riportato il più recente *Final Report* del 2021 [67] in cui l'ESMA ha raccolto dati provenienti sia da mercati regolamentati sia da sistemi multilaterali di negoziazione, forniti da circa 52 piattaforme di diversi 24 paesi europei, nel periodo compreso tra il 2018 e 2019. L' indagine è stata condotta su base trimestrale in riferimento a tre categorie di strumenti finanziari (azioni, obbligazioni e strumenti derivati) e tiene in considerazione le tre differenti modalità di *trading*: negoziazione algoritmica, HFT e negoziazione non algoritmica.

Per quanto concerne il mercato azionario, l'ESMA ha notato come i volumi riconducibili al *high frequency trading* rappresentino la parte più consistente con circa il 60 % dei volumi scambiati, a cui segue circa un 30% condotto tramite *trading* algoritmico e

---

[63] CHLISTALLA, M. (2011). High-frequency trading: Better than its reputation? (Research Briefing). Deutsche Bank Research, Frankfurt am Main, Germany, pp. 1–7.
[64] GERIG, A. (2015). High-frequency trading synchronizes prices in financial markets (Working paper), p.1; ALVARO, S., & VENTORUZZO, M. (2016). «High-frequency trading»: note per una discussione. *Banca Impresa Società, 35*(3), p. 418; BALP, G., & STRAMPELLI, G. (2018). Preserving capital markets efficiency in the high-frequency trading era (Bocconi Legal Studies Research Paper No. 3097723), p. 3.
[65] HENDERSHOTT, T. J., JONES, C. M., & MENKVELD, A. J. (2011). Does algorithmic trading improve liquidity? *The Journal of Finance, 66*(1), p. 2.
[66] ALVARO, S., & VENTORUZZO, M. (2016). «High-frequency trading»: note per una discussione. *Banca Impresa Società, 35*(3), p. 418.
[67] EUROPEAN SECURITIES AND MARKETS AUTHORITY. (2021). MiFID II/MiFIR review report on algorithmic trading (Ref. ESMA70-156-4572). ESMA, Paris, France.

un'ultima parte, pari circa al 10%, in forma non algoritmica. Il grafico di seguito riportato (fig.1) conferma l'analisi.

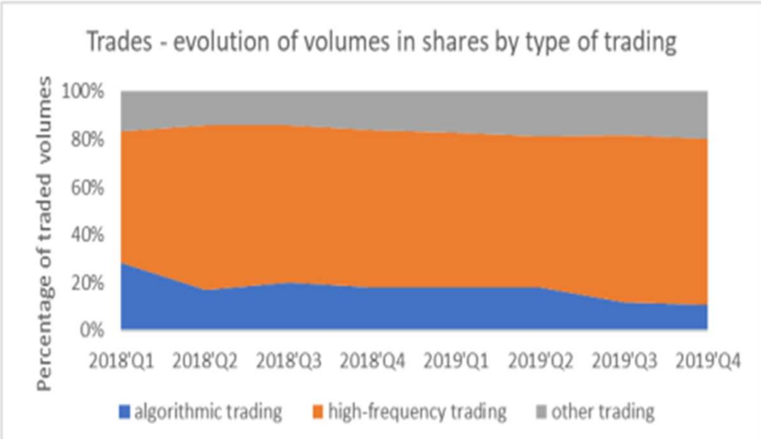

Fig. 2: grafico dell'evoluzione dei volumi per tipologia di trading (Fonte: https://www.esma.europa.eu/sites/default/files/library/esma70-156-4572_mifid_ii_final_report_on_algorithmic_trading.pdf).

Diverso è il caso invece delle obbligazioni e strumenti derivati: in entrambi le quote scambiate tramite HFT risultano essere marginali o, come nel caso dei derivati, quasi nulle. Questo, secondo l'ESMA, può essere spiegato dalla natura meno liquida [68] di tali strumenti.[69]

Complessivamente, il quadro che ne consegue mostra come il ricorso all'AT e HFT risulti essere sempre più costante e in crescita nel corso del tempo, tanto da spingere qualcuno a parlare di una *"quarta rivoluzione industriale"* [70] anche nel contesto dei mercati finanziari.[71]

---

[68] Per liquidità di uno strumento finanziario si intende la facilità con cui il medesimo può essere acquistato o venduto, in termini di tempo e costi.
[69] Vedi nota n. 67 p. 22.
[70] LUCANTONI, P. (2019). L'«high frequency trading» nel prisma della vigilanza algoritmica del mercato. *Analisi Giuridica dell'Economia*, (1), p. 298.
[71] Per una analisi del termine "quarta rivoluzione industriale" si rinvia a SCHWAB, K. (2018). La quarta rivoluzione industriale (2ª ed.). FrancoAngeli.

1.4.2 EFFETTI POSITIVI

In letteratura esistono numerosi lavori e ricerche accademiche che riconducono in capo ai sistemi AT e HFT diverse conseguenze positive. Senza pretesa di esaustività, si riportano i principali contributi in materia.

Anzitutto, la Direttiva 2014/65/UE MiFID II riconosce espressamente in capo all'HFT effetti positivi affermando come "*tale tecnologia di negoziazione abbia apportato vantaggi al mercato e ai partecipanti stessi, come una più ampia partecipazione ai mercati, un aumento della liquidità differenziali più ridotti, minore volatilità a breve termine e i mezzi per ottenere una migliore esecuzione degli ordini per i clienti*" (considerando n. 62).

Tra i principali contributi scientifici, si cita il lavoro degli economisti Brogaard, Hendershott e Riordan (2014) [72] i quali sostengono che l'*High Frequency Trading* svolga un ruolo fondamentale nel processo di determinazione dei prezzi. Secondo gli autori, infatti, l'HFT facilita *l'efficienza dei prezzi negoziando nella direzione dei cambiamenti permanenti e in direzione opposta rispetto agli errori di prezzo transitori*. In sostanza, gli algoritmi, in presenza di cambiamenti stabili dei prezzi (al rialzo o al ribasso) tendono a comprare o vendere nella stessa direzione, accelerandone i movimenti; laddove invece individuino degli errori, operano in senso opposto contrastando le deviazioni dal valore fondamentale. Nel complesso, il *modus operandi* avrebbe come effetto quello di favorire una maggior *price discovery,* intesa come la capacità del prezzo dello strumento finanziario di riflettere il reale valore sottostante, migliorandone quindi l'efficienza informativa.

Agli HFT si riconosce, inoltre, grazie alla elevata mole di operazioni realizzate e ordini immessi, il merito di incrementare la liquidità nel mercato, intesa come la presenza di molte proposte di negoziazione a differenti livelli di prezzo nel libro ordini. [73]

[72] BROGAARD, J., HENDERSHOTT, T. J., & RIORDAN, R. (2013). High-frequency trading and price discovery (Working paper), p. 3.
[73] Maggiore è la liquidità su un mercato, più alta è la possibilità per gli investitori di poter vedere eseguiti i propri ordini di acquisto e vendita.

L'economista Hendershott (2010), [74] ma anche altri autori, [75] sul punto afferma esplicitamente che "*con l'introduzione di sistemi di negoziazione algoritmica a partire dal 1990, la liquidità nel mercato azionario ha subito un vertiginoso aumento*", evidenziando quindi una correlazione positiva tra i due elementi.

Uno degli effetti senza dubbio più riconosciuti è poi quello consistente nella riduzione del *bid-ask spread,* definito come differenza tra prezzo più alto che un compratore è disposto a pagare (*bid*) e prezzo più basso a cui un venditore è disposto a vendere (*ask*). In particolare, gli HFT, quando operano come *market maker,* [76] inseriscono numerosi ordini al limite di acquisto e vendita, con variazioni di prezzo pari al *tick* minimo consentito, [77] al fine di posizionarsi nei livelli più alti del *book* di negoziazione, in cui vi è una maggior probabilità di esecuzione.[78] L' effetto che ne deriva è quello di restringere la forbice di prezzo tra ordini al limite di acquisto e ordini al limite di vendita.[79] Questo ha come conseguenza ulteriore quella di esercitare una *pressione maggiore sul livello delle commissioni dei brokers, con il loro conseguente decremento medio.* [80] In altre parole, sembra che l'HFT abbia anche l'effetto di ridurre i costi di transazione.

---

[74] HENDERSHOTT, T. J., JONES, C. M., & MENKVELD, A. J. (2011). Does algorithmic trading improve liquidity? *The Journal of Finance, 66*(1), p. 3.
[75] Tra questi si riportano: CHLISTALLA, M. (2011). High-frequency trading: Better than its reputation? (Research Briefing). Deutsche Bank Research, Frankfurt am Main, Germany; LERCH, M. P. (2022). Algorithmic trading and high-frequency trading. In R. Veil (Ed.), *European capital markets law* (3rd ed.) p. 474; LEIS, D. (2012). High-Frequency Trading: Market Manipulation and Systemic Risks From an EU Perspective (Working Paper), p. 26.
(finding that: "*The most often mentioned benefit of HFT is the increase in liquidity on the markets provided by market makers, in particular for less traded products and on alternative trading venues*").
[76] Per la definizione di *market making* si rinvia a par. 1.1.
[77] Il *tick size* è il minimo incremento di prezzo per gli ordini inseriti nel book di negoziazione.
[78] Le differenze di prezzo tra gli ordini immessi dagli *High Frequency Traders* variano in misura decimale.
[79] Sul punto si consulti: PUORRO, A. (2013). High frequency trading: Una panoramica (Banca d'Italia, Occasional Paper n. 198), p. 22; ANGEL, J. J., HARRIS, L., & SPATT, C. S. (2010). Equity trading in the 21st century (Marshall School of Business Working Paper No. FBE 09-10). University of Southern California, Los Angeles, CA. p. 5.
[80] BERTANI, M. (2019). Trading algoritmico ad alta frequenza e tutela dello «slow trader». *Analisi Giuridica dell'Economia – Studi e discussioni sul diritto dell'impresa*, (1), p. 273.; sul punto anche LERCH, M. P. (2022). Algorithmic trading and high-frequency trading. In R. Veil (Ed.), *European capital markets law* (3rd ed.), p. 474 (finding that: "*it is claimed that AT e HFT have led to reduced transaction costs for investor as trading platforms compete for order flow by lowering costs, amongst other things*").

Infine, esso sembra favorire anche la "sincronizzazione dei prezzi di strumenti finanziari". Secondo uno studio dettagliato condotto dall' economista Gerig (2015),[81] qualora due azioni siano tra loro correlate (si pensi alle azioni di una azienda che opera nel settore dei semiconduttori e una operante nel settore della telefonia) i movimenti di prezzo che si verificano sulla prima tendono a riflettersi anche sulla seconda, e ciò è reso possibile proprio dai sistemi di negoziazione ad alta frequenza.

In conclusione, tra le diverse opinioni positive, si riporta quella contenuta nel saggio dello studioso Brogaard (2010)[82] che, dopo aver analizzato l'impatto che gli HFT hanno avuto sul mercato azionario statunitense, conclude affermando come i *trader* ad alta frequenza *"tendano complessivamente a migliorare la qualità del mercato".*

1.4.3 EFFETTI NEGATIVI

Se da un lato, parte della letteratura si sofferma sugli effetti positivi, non mancano, dall'altro, esperti che da più parti sottolineano numerose conseguenze negative.

Ad avvertire sin da subito sui potenziali rischi è la MiFID II che, al considerando n. 62, riconosce come *"tale tecnologia sia all'origine anche di una serie di rischi potenziali, come: un aumento del rischio di sovraccarico dei sistemi nelle sedi di negoziazione a causa del gran numero di ordini, i rischi che la negoziazione algoritmica generi ordini erronei o doppi o che comunque non funzioni correttamente e crei così un mercato disordinato. Esiste inoltre il rischio che i sistemi di negoziazione algoritmica reagiscano in modo eccessivo ad altri eventi di mercato, esacerbando così la volatilità qualora preesista un problema di mercato. Infine, la negoziazione algoritmica o la tecnica di negoziazione algoritmica ad alta frequenza possono, come ogni altra forma di negoziazione, prestarsi a talune forme di comportamento, se non utilizzate correttamente, vietate a norma del regolamento (UE) n. 596/2014".*

[81] GERIG, A. (2015). High-frequency trading synchronizes prices in financial markets (Working paper), p.2.
[82] BROGAARD, J. A. (2010). High frequency trading and its impact on market quality (Working paper). Northwestern University, Kellogg School of Management, Evanston, IL, p. 1.

L'idea che questa tecnologia sia all'origine di una serie di problematiche trova una spiegazione in relazione a una successione di eventi che si sono verificati sui mercati a partire dal 2010, nei quali l'HFT ha avuto un ruolo determinante.

Il primo è stato quello del *Flash Crash* del 6 maggio 2010, in cui i mercati finanziari statunitensi hanno sperimentato uno dei più turbolenti periodi della loro storia. La vicenda, descritta dettagliatamente nelle pagine del report della *Securities and Exchange Commission* (SEC) assieme alla *Commodity Futures Trading Commission* (CFCT, ossia l'agenzia incaricata di supervisionare i mercati dei derivati statunitensi),[83] prende avvio a seguito della decisione di un grande fondo comune di investimento di intraprendere un programma di vendita di circa 75.000 contratti E-Mini S&P500 *futures*.[84] La decisione fu eseguita per mezzo di un algoritmo (denominato "*Sell Algorithm*") senza tenere conto né del prezzo né del momento di esecuzione, con il risultato di immettere nel mercato una elevatissima quantità di ordini. La pressione fu poi amplificata dagli stessi *traders* ad alta frequenza che, in maniera opportunistica, decisero, da una parte di acquistare gli E-Mini *futures* e, dall' altro, di cedere le azioni correlate, [85] trasferendo così la spirale ribassista al mercato azionario. L'esito fu drammatico: un crollo di tutti i più importanti indici americani in appena 36 minuti (il Dow Jones, uno dei principali indici americani, [86] perse circa il 9% del suo valore). [87] Tuttavia, esso non durò a lungo: il mercato recuperò rapidamente la propria stabilità e chiuse in ribasso del 3%.[88]

[83] U.S. SECURITIES AND EXCHANGE COMMISSION, & U.S. COMMODITY FUTURES TRADING COMMISSION. (2010). Findings Regarding the Market Events of May 6, 2010: Report of the staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues (Report of the staffs of the CFTC and SEC). SEC/CFTC, pp. 1–104.
[84] Gli E-Mini S&P500 *futures* sono una serie di contratti derivati che replicano l'andamento di un indice, in questo caso l'indice è l'S&P500 che raccoglie cinquecento tra le maggiori società quotate degli US.
[85] Si tratta delle azioni di quelle società che rientrano nell' indice S&P500.
[86] Il DJ è l'indice che raccoglie 30 grandi società a larga capitalizzazione. A differenza dell'S&P500, che risulta essere ponderato sulla capitalizzazione di mercato (*market cap weighted*), il Dow Jones è ponderato sul prezzo delle azioni (*price weighted*).
[87] BUSCH, D. (2017). MiFID II: Regulating high frequency trading, other forms of algorithmic trading and direct electronic market access. *Law and Financial Markets Review, 10*(2), 2016), pg. 72.
[88] TREANOR, J. (2015). The 2010 'flash crash': how it unfolded. *The Guardian*. https://www.theguardian.com/business/2015/apr/22/2010-flash-crash-new-york-stock-exchange-unfolded

L'evento in questione ebbe una grande attenzione mediatica e sul banco degli imputati furono messi gli stessi sistemi di negoziazione ad alta frequenza, [89] tuttavia, studi successivi dimostrarono come gli HFT non causarono direttamente il *Flash Crash,* ma al contrario, contribuirono a uno straordinario aumento della volatilità.[90]

Molteplici sono gli autori che riconoscono ai *traders* ad alta frequenza la capacità di aumentare la volatilità. [91] Sul punto, vale la pena citare l'opinione dell'economista Valeria Caivano (2015) [92] che analizzando il mercato azionario italiano nel periodo compreso tra il 2011-2013 conclude affermando che "*un incremento esogeno del livello di attività HFT determina un significativo incremento della volatilità dei rendimenti giornalieri. Infatti, a seconda della specificazione utilizzata, un incremento di 10 punti percentuali del peso degli HFT 'puri' sul totale degli scambi determina un aumento della volatilità intraday compreso tra i 4 e i 6 punti percentuali*".

Il secondo e rilevante episodio da menzionare è quello poi verificatosi nell'aprile del 2013, noto come "*AP Flash Crash"* in cui, a seguito di un hackeraggio, l'account Twitter di *Associated Press* (una delle maggiori agenzie di stampa al mondo) ha diramato una notizia concernente delle esplosioni avvenute nella Casa Bianca e del ferimento del Presidente Obama. In tale contesto *"i sistemi di trading ad alta frequenza hanno immediatamente processato la notizia e iniziato a ritirare le proprie proposte di acquisto*

---

[89] Un sondaggio condotto da Market Strategies International tra il 23 e il 29 giugno 2010 ha riportato che oltre l'80% dei consulenti retail statunitensi riteneva che la "eccessiva dipendenza dai sistemi informatici e dal trading ad alta frequenza" fosse il principale fattore che aveva contribuito alla volatilità osservata il 6 maggio 2010.

[90] KIRILIENKO, A., KYLE, A. S., SAMADI, M., & TUZUN, T. (2014). The flash crash: The impact of high frequency trading on an electronic market (CFTC Working Paper). U.S. Commodity Futures Trading Commission, p. 4.

[91] BALP, G., & STRAMPELLI, G. (2018). Preserving capital markets efficiency in the high-frequency trading era (Bocconi Legal Studies Research Paper No. 3097723), p. 11 (finding that: "*HFTs exacerbate volatility and cause marketplaces to function in a disorderly manner*"); ZHANG, F. (2010). High-frequency trading, stock volatility, and price discovery (Working paper) (Finding that "*high-frequency trading is positively correlated with stock price volatility after controlling for firm fundamental volatility and other exogenous determinants of volatility*"); BOEHMER, E., FONG, K., & WU, J. (2021). Algorithmic trading and market quality: International evidence. *Journal of Financial and Quantitative Analysis, 56*(8), p. 2659 (finding that: "*On average, AT improves liquidity and informational efficiency but increases short-term volatility*"); BERSHOVA, N., & RAKHLIN, D. (2013). High-frequency trading and long-term investors: A view from the buy-side. *Journal of Investment Strategies, 2*(2), p. 25 (finding that: "*the increase in short term volatility and in trading costs due to HFT is more than offset by the narrowing of bid-ask spread*").

[92] CAIVANO, V. (2015). The impact of high-frequency trading on volatility: Evidence from the Italian market (CONSOB Working Paper No. 80), p. 24.

per sfruttare il probabile trend ribassista".[93] Ciò ha causato inevitabilmente un improvviso crollo del mercato azionario (l'indice *Dow Jones* ha registrato un calo di 143 punti)[94], salvo poi ritornare sui livelli iniziali nel giro di 5 minuti.

Da questo episodio possiamo rilevare le seguenti conclusioni. *In primis* si sottolinea come la diffusione delle notizie false abbia spinto gli HFT a ritirare le proprie proposte al limite di acquisto e di vendita causando una riduzione della liquidità. Questo sembra essere coerente con quello che alcuni autori [95] definiscono essere il fenomeno della "*ghost liquidity*" ovvero liquidità "ombra", ossia una liquidità che può apparire e scomparire nel giro di pochi millisecondi e di cui l'HFT è ritenuto essere il principale artefice. A tal riguardo, interessante è il contributo dello studioso Lin Tong (2015) [96] che afferma come, in generale, la liquidità offerta da parte degli HFT sia in realtà sia di breve durata, ossia limitata alla giornata, il che rende l'HFT simile ad un intermediario *intraday.*

In secundis, una parte della dottrina economica, contrariamente a quanto avanzato in precedenza (a proposito degli effetti positivi), conviene circa il fatto che *l'high frequency trading* non svolga affatto un ruolo verso una maggiore *price discovery* e *price efficiency***.** In tal senso, si ritiene che i sistemi ad alta frequenza "*possano cagionare errori nella valutazione dei prezzi, che i medesimi sfruttano inconsapevolmente a svantaggio degli investitori ordinari".*[97] Dubbi e pareri simili sono stati sollevati anche dall'economista

---

[93] PUORRO, A. (2013). High frequency trading: Una panoramica (Banca d'Italia, Occasional Paper n. 198), p. 28.
[94] MOORE, H., & ROBERTS, D. (2013). AP Twitter hack causes panic on Wall Street and sends Dow plunging. *The Guardian*. https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall.
[95] BERTANI, M. (2019). Trading algoritmico ad alta frequenza e tutela dello «slow trader». *Analisi Giuridica dell'Economia – Studi e discussioni sul diritto dell'impresa*, (1), p. 273; KIRILIENKO, A., KYLE, A. S., SAMADI, M., & TUZUN, T. (2014). The flash crash: The impact of high frequency trading on an electronic market (CFTC Working Paper). U.S. Commodity Futures Trading Commission; PUORRO, A. (2013). High frequency trading: Una panoramica (Banca d'Italia, Occasional Paper n. 198), p. 31; CAIVANO, V. (2015). The impact of high-frequency trading on volatility: Evidence from the Italian market (CONSOB Working Paper No. 80), p. 11.
[96] TONG, L. (2015). A blessing or a curse? The impact of high frequency trading on institutional investors (European Finance Association Annual Meetings 2014 Paper Series), p. 24 (finding that: "*such liquidity provision is short-lived, i.e., within a day; therefore, a more accurate description of the liquidity provision role of HF traders is that they serve as intraday intermediaries and quickly pass the imbalances from institutions to other market participants*").
[97] JARROW, R. A., & PROTTER, P. (2011). A dysfunctional role of high frequency trading in electronic markets (Johnson School Research Paper Series No. 08-2011). Cornell University, Samuel Curtis Johnson Graduate, p. 1. (finding that: "*high frequency traders can create a mispricing that they unknowingly exploit to the disadvantage of ordinary investors*").

Zhang (2010)[98] il quale evidenzia come "*il trading ad alta frequenza è negativamente correlato alla capacità del mercato di incorporare nelle quotazioni le informazioni sui fondamentali delle imprese. I prezzi azionari tendono infatti a reagire in modo eccessivo alle notizie fondamentali quando il volume del trading ad alta frequenza è elevato".*

A tal proposito, merita essere riportato il fondamentale contributo dei giuristi Balp e Strampelli (2018)[99] che mettono in guardia rispetto al pericolo del "*free riding informativo*": in particolare gli autori evidenziano come gli algoritmi, grazie alle loro elevate capacità di calcolo e velocità, possano intravedere in anticipo ordini nel mercato lasciati da investitori istituzionali che elaborano le loro strategie sulla base di approfondite ricerche.[100] Captando tali ordini "informati", gli HFT possono negoziare nella stessa direzione, sfruttando gratuitamente l'informazione prodotta da altri. Questo, nel lungo periodo risulta essere particolarmente nocivo e dannoso in quanto, secondo gli autori, scoraggerebbe investimenti nella ricerca.[101]

Infine, dall'episodio "*AP Flash Crash*" si ricava anche l'incredibile capacità degli algoritmi di riuscire a captare, in maniera autonoma, indicazioni operative dal flusso informativo di coloro che forniscono notizie di mercato. Attraverso una strategia che prende il nome di "*Trading on news"* tali sistemi *sono in grado di associare le strategie di negoziazione a determinati pattern di parole presenti nelle notizie, adattando le strategie alla risonanza della notizia stessa.*[102]

---

[98] ZHANG, F. (2010). High-frequency trading, stock volatility, and price discovery (Working paper), pp. 1-2.

[99] BALP, G., & STRAMPELLI, G. (2018). Preserving capital markets efficiency in the high-frequency trading era (Bocconi Legal Studies Research Paper No. 3097723), p. 13; STIGLITZ, J. E. (2014). Tapping the Brakes: Are Less Active Markets Safer and Better for the Economy? (Unpublished manuscript prepared for the Federal Reserve Bank of Atlanta). Federal Reserve Bank of Atlanta.

[100] YADAV, Y. (2015). How algorithmic trading undermines efficiency in capital markets. *Vanderbilt Law Review, 68*(6), p. 1615 (finding that: "*Notably, high-speed algorithmic traders have powerful advantages over more fundamental traders. Specifically, fast traders can decide how an informed trader is likely to transact and get to the trade before anyone else by free-riding on the intelligence of others, algorithmic traders save themselves time and money while also taking home a share of the winnings. Faced with diminishing gains, informed traders can end up with fewer incentives to invest in long-term research and analysis*").

[101] BALDAUF, M., & MOLLNER, J. (2020). High-Frequency Trading and Market Performance. *The Journal of Finance, 75*(3), p. 1495 (finding that: "*information production decreases because informed traders have less time to trade before HFTs react*").

[102] Cfr. nota n. 93, p. 16.

L'ultimo evento rilevante da ricordare concerne il noto caso "*Knight Capital*" del 2012.[103] La vicenda rappresenta un perfetto esempio di "*rogue algorithm*"[104] ossia un algoritmo malfunzionante e operante in maniera difforme da quella prevista. Più nello specifico, a causa di un algoritmo di *trading* difettoso, furono inseriti nel mercato, da parte della HFT *firm Knight Capital,* il 1° agosto 2012, milioni di ordini errati che provocarono forti oscillazioni e turbolenze dei prezzi azionari per ben 45 minuti.

Episodi di questo genere risultano essere assai pregiudizievoli per la stabilità del mercato in quanto i danni originati da algoritmi difettosi possono diffondersi rapidamente tra le diverse sedi di negoziazione e, dal momento che esse sono sempre più interconnesse e interdipendenti, possono dar luogo ad effetti a cascata ("*cascade effects").*[105] Come è stato infatti sottolineato, dato che le HFT *firms* eseguono le negoziazioni sulla base delle informazioni rilevate da altre negoziazioni, *"è molto probabile che il comportamento di un algoritmo fuori controllo inneschi altri algoritmi, i quali a loro volta portano algoritmi errati a negoziare su tali informazioni".* [106]

Infine, sia il *trading* algoritmico sia, in maggior parte, *l'high frequency trading* fanno sorgere serie problematiche qualora siano strumentali alla realizzazione di pratiche predatorie che pregiudichino l'equità e la stabilità del mercato. Invero, strategie come lo *stuffing, spoofing e layering* costituiscono vere e proprie manipolazioni di mercato. [107] Questa tematica, data la sua rilevanza, sarà compiutamente analizzata e trattata nel successivo capitolo 2.

---

[103] U.S. SECURITIES AND EXCHANGE COMMISSION. (2013). SEC charges Knight Capital with violations of market access rule (Press Release No. 2013-222). https://www.sec.gov/newsroom/press-releases/2013-222.

[104] ANNUNZIATA, F. (2023). Artificial intelligence and the regulation of market abuse: A European perspective. Edward Elgar Publishing, Cheltenham (UK)–Northampton, MA (USA), p. 115.

[105] *Ibidem*.

[106] LERCH, M. P. (2022). Algorithmic trading and high-frequency trading. In R. Veil (Ed.), *European capital markets law* (3rd ed.), p. 469-470 (finding that: "*Given that, to a large extent, HFT firms trade on information revealed by other trades, it is very likely that the behavior of a rogue algorithm triggers other algorithms, which in turn cause false algorithms to trade on that information*").

[107] *Ibidem*, p. 472-473.

1.4.4 VALUTAZIONI

Dare un giudizio definitivo sull'HFT è complicato. Come è stato rilevato nelle precedenti sezioni, la comparazione tra effetti positivi ed effetti negativi produce risultati contrastanti e spesso contraddittori: per esempio, se è ritenuto pacifico che i sistemi di *trading* ad alta frequenza favoriscano una maggior liquidità durante le normali condizioni di mercato, lo stesso può dirsi in situazioni di forte stress, in cui gli HFT, cancellando gli ordini, sottraggono liquidità.

I regolatori si trovano, pertanto, in una difficile posizione. Se risulta essere irragionevole da un lato un divieto assoluto per i sistemi AT e HFT, [108] in quanto ostacolo all'innovazione e sviluppo, ci si dovrebbe interrogare, dall' altro, su quali possano essere le misure normative da adottare al fine di preservare gli effetti positivi e limitare quelli negativi. L'obiettivo non è dei più agevoli in quanto il fenomeno dell'*High Frequency Trading* si presenta come mutevole e variabile, tanto da essere definito in dottrina come "*protean in nature*". [109] A tal riguardo, risulta indispensabile analizzare il quadro normativo euro unitario ad oggi vigente, la cui trattazione avverrà nel prosieguo del presente studio.

In ogni caso, è opportuno specificare che l'AT e HFT non rappresentino una vera e propria forma di investimento quanto, semmai, un mezzo avanzato di speculazione dato che risulta essere assente una logica di impiego del capitale orientata alla creazione di rendimento nel lungo periodo.

---

[108] *Ibidem*, p. 476.
[109] KORSMO, C. (2014). High-frequency trading: A regulatory strategy. *University of Richmond Law Review, 48*(2), p. 529. (finding that: "*HFTs are protean in nature, introducing new trading strategies and algorithms on a continuous basis*").

LA NORMATIVA E IL TRADING ALGORITMICO

1.5 PREMESSA

Preso atto degli effetti anche negativi che discendono dal *trading* algoritmico e ad alta frequenza è necessario esaminare la risposta che il legislatore europeo ha fornito dal punto di vista normativo. Più specificatamente, si analizzerà la disciplina contenuta nella Direttiva EU n. 65 del 2014 (MiFID II) e negli Standard Tecnici di Attuazione (*Regulatory Technical Standard*, o RTS) emanati dall' ESMA, Autorità europea di vigilanza e regolamentazione dei mercati finanziari. A seguire, sarà valutato se tale assetto normativo possa costituire una risposta sufficientemente efficace da preservare gli effetti positivi e limitare quelli negativi. In tale sede sarà inoltre valutato se l'impianto normativo attuale sia idoneo e appropriato a regolare anche taluni aspetti problematici, in particolare, quelli che vedono l'applicazione dei sistemi di intelligenza artificiale nel contesto *trading*. Invero, l'ingegneria finanziaria è riuscita, nel tempo, ad elaborare modelli sempre più complessi e sofisticati in cui l'IA viene direttamente implementata nei modelli algoritmici ad alta frequenza. Non si tratta più solamente di macchine programmate a prendere decisioni di investimento al realizzarsi di parametri "predeterminati" dall' uomo (modello "classico" di algoritmo di *trading*), quanto di modelli in cui è la macchina stessa ad elaborare tali parametri. In altre parole, se con i modelli classici le istruzioni che attivavano l'algoritmo erano appannaggio dell'essere umano ("se ricorre questa condizione, allora…"), adesso è la macchina stessa a definire tali condizioni, aprendo la strada a veri e propri "soggetti autonomi e indipendenti".

1.6 UN QUADRO REGOLATORIO MULTILIVELLO

La disciplina sulla negoziazione algoritmica, ma più in generale, il diritto europeo del mercato dei capitali risulta essere strutturato secondo un modello denominato "procedura di *Lamfalussy*", consistente in un'articolata ripartizione del potere decisionale tra le diverse istituzioni UE e finalizzata ad un processo decisionale più rapido e sensibile agli interessi dei soggetti coinvolti. [110]

[110] PERRONE, A. (2024). Il Diritto Del Mercato Dei Capitali. Giuffrè Francis Lefebvre, Milano, p. 65.

Il primo livello è rappresentato da quei provvedimenti-quadro emanati da Commissione, Parlamento e Consiglio nella forma di direttive e regolamenti contenenti i principi generali e fondanti della disciplina. Per la materia oggetto del presente studio, il riferimento è, da un lato, alla Direttiva UE n. 65 del 2014 (MiFID II) e al Regolamento UE n. 600 del 2014 (MiFIR) per quanto concerne il funzionamento dei mercati e delle imprese di investimento onde assicurare stabilità ed equità sui mercati ("*level playing field*"), dall' altro, alla Direttiva UE n. 57 del 2014 (MAD II) e al Regolamento UE n. 596 del 2014 (MAR) per quanto concerne la normativa sugli abusi di mercato.

Il secondo livello è rappresentato da "atti non legislativi di portata generale" adottati dalla Commissione aventi carattere tecnico e che precisano le previsioni dei provvedimenti quadro. Nell' emanare tali atti la Commissione si avvale del supporto dell'ESMA, che elabora a tal fine progetti di "norme tecniche di regolamentazione" (*regulatory technical standard*, RTS) e "norme tecniche di attuazione" (*implementing technical standard*, ITS).

Il terzo livello è costituito poi dalle raccomandazioni, linee guida e orientamenti (*soft law*) predisposti dall'ESMA al fine di favorire una interpretazione uniforme del diritto UE.[111] Infine, l'ultimo livello concerne il monitoraggio circa lo *status* di attuazione della disciplina da parte degli stati membri, ruolo ricoperto dal' ESMA e dalla Commissione.

Nel presente capitolo sarà approfondita la disciplina contenuta nel MiFID *package,*[112] rinviando quella specifica sugli abusi di mercato al capitolo secondo.

La normativa contenuta nella MiFID II si presenta, nel suo complesso, come un insieme di regole molto dettagliate e fondate sul principio del "controllo del rischio"[113] ("*risk based approach*"): l'idea ispiratrice è quella non tanto di "regolare e governare"

---

[111] Ai nostri fini si ricordano: EUROPEAN SECURITIES AND MARKETS AUTHORITY. (2012). Guidelines on systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities (ESMA/2012/122). ESMA. (Ritirate nel 2018 in quanto incorporate nella MiFID II e relative misure di attuazione).

[112] ANNUNZIATA, F. (2018). La disciplina delle trading venues nell'era delle rivoluzioni tecnologiche: Dalle criptovalute alla distributed ledger technology. *Orizzonti del Diritto Commerciale*, 6(3), 40–69, p. 26 (paginazione PDF).

[113] MYKLEBUST, T. (2020). Fairness and integrity in high-frequency markets – A critical assessment of the European regulatory approach. *European Business Law Review, 31*(1), p. 26.

l'algoritmo (rispetto al quale il legislatore rimane "tecnologicamente neutro"),[114] quanto quella di mitigare i rischi che possano eventualmente derivare da un maggior ricorso alla tecnologia. A tal proposito, sono stati predisposti controlli e misure specifiche rivolte sia alle imprese che effettuano negoziazioni algoritmiche, sia alle stesse piattaforme di negoziazione a cui tali imprese hanno accesso, [115] affinché non si creino mercati disordinati e tali tecnologie non siano impiegate per scopi contrari all'ordinamento. [116]

Nella disamina a seguire si analizza il regime "speciale"[117] che il legislatore ha ritagliato tanto per le imprese coinvolte in AT e HFT, quanto per le piattaforme di negoziazione o *trading venues*.

1.6.1 IMPRESE DI INVESTIMENTO ALGORITMICHE

Per quanto concerne le imprese che svolgono attività riconducibili al *trading* algoritmico, la norma iniziale da cui partire è contenuta nell'art. 2 par.1 lett. *d)*, punto n. iii) della MiFID II. In tale disposizione, il legislatore UE ha espressamente escluso, per tutti quei soggetti che negoziano per conto proprio e che ricorrono una "tecnica di negoziazione ad alta frequenza", l'esenzione dall' applicazione della presente direttiva. La norma ha due risvolti molto importanti: il primo consiste nel fatto che gli operatori algoritmici ad alta frequenza operanti con capitale proprio, al fine di poter esercitare legittimamente la loro attività, devono essere autorizzati come "imprese di investimento" [118] e, pertanto, sono tenuti a conformarsi sia agli obblighi previsti dalla MiFID II per le imprese di investimento in generale sia alle previsioni derivanti dall'applicazione regime "speciale" concernente il *trading* algoritmico. Il secondo risvolto consiste, invece, nella necessità di applicare i requisiti patrimoniali previsti per le imprese di investimento (art. 28 dir.

---

[114] In ambito finanziario, il principio di neutralità tecnologica stabilisce che la regolamentazione e la vigilanza devono focalizzarsi sulla natura dell'attività svolta e sui rischi correlati, anziché sulla tecnologia specifica utilizzata per erogare il servizio.
[115] Considerando 63 MiFID II.
[116] Considerando 64 MiFID II.
[117] ANNUNZIATA, F. (2023). Artificial intelligence and the regulation of market abuse: A European perspective. Edward Elgar Publishing, Cheltenham (UK)–Northampton, MA (USA), p. 125.
[118] L'art 4 della MiFID definisce "impresa di investimento" come "qualsiasi persona giuridica la cui occupazione o attività abituale consiste nel prestare uno o più servizi di investimento a terzi e/o nell'effettuare una o più attività di investimento a titolo professionale". Tale definizione coincide con quella di "intermediario finanziario" presente nel nostro ordinamento (TUF).

2013/36/UE – CRD IV),[119] comportando di per sé, il vincolo di impiegare capitali propri particolarmente significativi.[120]

Per quanto riguarda il regime "speciale", questo è contenuto nell'art. 17 della MiFID II denominato "negoziazione algoritmica" e le previsioni ivi riportate vengono poi elaborate in maniera più esaustiva dal regolamento delegato n. 589 del 2017 (RTS 6), [121] contenente le norme tecniche di regolamentazione (Livello 2 procedura di *Lamfalussy*).

La MiFID II impone, anzitutto, alle imprese di investimento di adottare "controlli dei sistemi e del rischio" efficaci e idonei per l'attività esercitata, in modo da garantire la "resilienza e una sufficiente capacità dei sistemi di negoziazione". Inoltre, tali sistemi di negoziazione devono essere tali da impedire l'invio di ordini erronei o causare un funzionamento disordinato del mercato. Allo stesso tempo, i controlli interni all'intermediario devono essere in grado di prevenire operazioni contrarie all'ordinamento - in particolare, il riferimento è diretto alla disciplina MAR (*Market Abuse Regulation*)[122] - nonché alle regole della *trading venue,* alle quali l'operatore aderisce. La presente direttiva, infine, chiede alle imprese di adottare meccanismi che assicurino la continuità operativa anche di fronte a malfunzionamenti dei sistemi di negoziazione.[123]

Per quanto concerne i doveri informativi, le imprese sono sottoposte ad una serie di obblighi di *disclosure.* Innanzitutto, sono tenute a notificare alle autorità competenti dello stato membro di origine e alle sedi di negoziazione presso cui operano il fatto di effettuare

---

[119] Direttiva 26 giugno 2013, 2013/36/UE del Parlamento europeo e del Consiglio, recante "Direttiva sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, recante modifica della direttiva 2002/87/CE e recante abrogazione delle direttive 2006/48/CE e 2006/49/CE" (CRD IV), in GUUE L 176 del 27 giugno 2013, pp. 338–436.

[120] GARGANTINI, M., & Siri, M. (2019). Il "prezzo dei prezzi": Una soluzione di mercato ai rischi dell'high frequency trading? (Relazione al X Convegno annuale dell'Associazione Italiana dei Professori Universitari di Diritto Commerciale "Orizzonti del Diritto Commerciale", "L'evoluzione tecnologica e il diritto commerciale", Roma), p. 14.

[121] Regolamento delegato (UE) 19 luglio 2016, 2017/589 della Commissione, recante "Regolamento che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda i requisiti organizzativi e le condizioni di funzionamento delle imprese di investimento che effettuano negoziazioni algoritmiche" (RTS 6), in GUUE L 87 del 31 marzo 2017, pp. 417–460.

[122] Regolamento (UE) 16 aprile 2014, n. 596/2014 del Parlamento europeo e del Consiglio, recante "Regolamento relativo agli abusi di mercato (regolamento sugli abusi di mercato) e recante abrogazione della direttiva 2003/6/CE del Parlamento europeo e del Consiglio e delle direttive della Commissione 2003/124/CE, 2003/125/CE e 2004/72/CE" (MAR), in GUUE L 173 del 12 giugno 2014, pp. 1–61.

[123] Art. 17 par. (1), MiFID II.

trading algoritmico. [124] [125] A questo flusso di informazioni attinente alla fase "iniziale" dell'attività, se ne aggiunge un secondo, di tipo "continuo", che matura invece durante lo svolgimento dell'attività: l'autorità competente dello stato membro d'origine può richiedere infatti, su base regolare o *ad hoc,* una descrizione della natura delle strategie di negoziazione, dettagli sui parametri o sui limiti di negoziazione imposti dall'algoritmo. È degno di nota sottolineare che questo potere informativo risulta essere particolarmente ampio in quanto l'autorità ha poi la possibilità di prescrivere in ogni momento *"ulteriori informazioni sulla negoziazione algoritmica da essa effettuata e sui sistemi utilizzati".*[126]

In proposito, è stato fatto notare come le imprese possano essere restie a rendere noti dati concernenti i loro algoritmi e le loro strategie, in quanto, costituendo essi il nucleo del loro modello di *business*, maggiore è il numero delle persone a conoscenza dei codici sorgente, tanto maggiore è il rischio che essi vengano, prima o poi, divulgati a concorrenti.[127]

Volgendo lo sguardo alla normativa tecnica, il regolamento delegato n. 589 del 2017 (RTS 6) individua i requisiti organizzativi che le imprese devono rispettare, in conformità all'art. 17 MiFID II.

Tale regolamento, in particolare, prevede quanto segue. Le imprese sono tenute a predisporre, prima dell'installazione (o aggiornamento sostanziale) del sistema di negoziazione, regole interne chiare e predefinite, al fine di sviluppare e "testare" i sistemi, gli algoritmi e le strategie. [128] I test in questione devono assicurare che il sistema di negoziazione algoritmica, l'algoritmo o la strategia di negoziazione : a) non si comportino in maniera imprevista; b) siano conformi agli obblighi imposti dal regolamento all' impresa; c) siano conformi alle regole e ai sistemi della sede di negoziazione a cui l'impresa ha accesso; e d) non contribuiscano a causare "condizioni di negoziazioni

---

[124] Art 17 par. (2), MiFID II.
[125] Da ciò ne deriva l'assenza di una autorizzazione obbligatoria per l'esercizio dell'attività in sé.
[126] Vedi nota 125.
[127] BUSCH, D. (2017). MiFID II: Regulating high frequency trading, other forms of algorithmic trading and direct electronic market access. *Law and Financial Markets Review, 10*(2), 2016), p. 82 (Finding that: "*The fact that competent authority can request information about AT and HFT strategies is bound to lead to debate in practice. The algorithms designed by an investment firm form the core of its business model and there will be a natural wish, for reasons of competition, to keep the source codes secret as far as possible. Although the competent authority is naturally not a competitor, the more people know about the source codes the greater the risk that they will sooner or later be divulged to competitors"*).
[128] Art. 5 par. (1) RTS 6.

anormali" , che funzionino correttamente anche in situazioni di forte stress di mercato e, laddove necessario, consentano la disattivazione del sistema di negoziazione o dell' algoritmo stesso.[129]

Dalla disamina delle disposizioni sopra riportate si comprende come il regolamento individui due tipologie di *test* da condursi all' interno di un quadro "metodologico" predefinito: i "*behavioural tests*" in cui si verifica che gli algoritmi si comportino correttamente e non creino disordine (lett. *a*, *b*, *d* del precedente elenco) e i "*conformance tests"* che riguardano invece l'interazione degli algoritmi con il sistema della sede di negoziazione (lett. *c* del precedente elenco).

I primi devono avvenire in un ambiente di prova distinto da quello di "produzione" (ossia l'ambiente in cui gli algoritmi sono effettivamente impiegati, vale a dire il mercato reale) che può essere, a seconda dei casi, sviluppato dalla stessa impresa ovvero fornito dalla sede di negoziazione o da un terzo. [130]

Una disposizione importante è, altresì, quella contenuta all'art. 8 del suddetto regolamento delegato in cui si prevede che prima dell'installazione dell'algoritmo di negoziazione l'impresa debba fissarne i limiti con riguardo al numero degli strumenti finanziari negoziati, il prezzo, valore e numero di ordini, le posizioni strategiche e il numero di sedi di negoziazione a cui gli ordini vengono trasmessi. Si tratta in questo caso di una rilevante norma che impone alle imprese di circoscrivere gli spazi entro i quali l'algoritmo può operare.

Il regolamento interviene, inoltre, anche sul profilo del monitoraggio circa i sistemi di negoziazione. A tal riguardo si individuano tre tipologie di controlli: controlli pre-negoziazione sull'immissione di ordini, [131] controlli svolti durante le ore in cui gli ordini vengono inviati[132] e controlli post negoziazione.[133]

---

[129] Art. 5 par. (4) RTS 6.
[130] Art. 7 par. (1) e (2) RTS 6.
[131] Art. 15 RTS 6, in particolare prevedendo l'applicazione di filtri di prezzo (che bloccano o cancellano gli ordini che non soddisfano parametri di prezzo prefissati), il valore e il volume massimo degli ordini e il limite massimo di messaggistica.
[132] Art. 16 RTS 6.
[133] Art. 17 RTS 6.

Ai suddetti controlli si aggiunge l'obbligo ulteriore previsto dall' art. 13 di monitorare tutte le attività di negoziazione per individuare potenziali manipolazioni di mercato. Si tratta di un controllo che viene effettuato per il tramite di un "sistema automatizzato di sorveglianza" in grado di monitorare, generare allarmi e produrre report e che concerne "l'intera gamma delle attività svolte dall' impresa".

Infine, il regolamento in esame prevede che le imprese, in caso di emergenza, siano sempre in grado di identificare il *trader* o l'algoritmo di negoziazione responsabile dell'ordine (*algorithmic flagging*) e cancellare immediatamente tutti gli ordini non eseguiti trasmessi a una o tutte le sedi di negoziazione (*kill-functionality)*. [134]

Da questa breve analisi della normativa, possiamo trarre due conclusioni. In primo luogo, il legislatore non ha disciplinato le modalità secondo le quali i test debbano avvenire. Da ciò ne deriva una procedura a carattere flessibile in cui l'impresa possiede ampi margini di discrezionalità nel decidere "come" procedere.

In secondo luogo, nella fase di *post test* non è prevista alcuna valutazione dei risultati da parte di un terzo indipendente, ma questa viene rimessa all'impresa algoritmica stessa tramite una autocertificazione da sottoporre alla sede di negoziazione, in cui si dichiara che "gli algoritmi sono provati al fine di evitare di contribuire o creare condizioni di negoziazione anormali" (Art. 10 comma 1, RTS 7). [135] Una previsione di questo tipo fa sorgere seri dubbi a proposito di comportamenti scorretti delle imprese, specie se si considera che le sedi di negoziazione non sono tenute a un controllo di "legalità sostanziale" sulla già menzionata certificazione quanto, semmai, a verificare l'avvenuta ricezione.[136]

[134] Art. 12 par. (1) RTS 12.
[135] Regolamento delegato (UE) 14 luglio 2016, 2017/584 della Commissione, recante "Regolamento che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda i requisiti organizzativi delle sedi di negoziazione" (RTS 7), in GUUE L 87 del 31 marzo 2017, pp. 380–416.
[136] Si veda in proposito il considerando 13 del RTS 7: "*Dovrebbe essere considerato come una garanzia sufficiente se le sedi di negoziazione ricevono una dichiarazione dai loro membri che conferma che tali prove hanno avuto luogo e indica i mezzi utilizzati per le prove, ma le sedi di negoziazione non dovrebbero essere tenute a convalidare l'adeguatezza di tali mezzi o i risultati di tali prove*".

1.6.2 SEDI DI NEGOZIAZIONE

Analogamente alla disciplina contemplata per le imprese di investimento, la MiFID II all'art. 48 e il già citato regolamento delegato 587/2017 (RTS 7) stabiliscono disposizioni specifiche per tutte le sedi di negoziazione. Come è stato sottolineato in dottrina,[137] quello per le piattaforme di negoziazione è un *corpus* di norme che, replicando in parte quello già previsto dall'art 17 della MiFID II, crea un sistema di regole completo, in cui sia la disciplina delle *trading venues* sia quella delle HFT *firms* si combinano secondo un approccio sinergico e complementare.[138]

Al riguardo, in primo luogo, la direttiva MiFID II all'art. 48 comma 1, rubricato "Resilienza dei sistemi, interruttori di circuito e negoziazione elettronica", impone alle sedi di negoziazione, con un linguaggio analogo quello utilizzato per le imprese di investimento, di essere "resilienti", intendendosi la capacità di gestire volumi elevatissimi di ordini e di garantire negoziazioni ordinate in condizioni di mercato critiche.[139]

A questo proposito, la normativa di Livello 2 (RTS 7) impone di effettuare una accurata *due diligence* sui partecipanti al mercato (art. 7) nonché di condurre test prima dell'installazione o aggiornamento del sistema di negoziazione onde accertare che il medesimo non si comporti in modo imprevisto e continui a funzionare efficacemente in caso di significativo aumento di ordini (art. 8).[140] Le sedi dovranno, inoltre, esigere dai loro membri "prove di conformità" affinché sia accertata la capacità del sistema o dell'algoritmo di interagire con la logica di abbinamento della sede di negoziazione (art. 9 RTS 7).[141] Ulteriori obblighi riguardano poi la governance delle sedi (art. 3 RTS 7) nonché l'assunzione del personale (art. 5 RTS 7), l'esternalizzazione delle funzioni (art 4 RTS 7) ed infine il "monitoraggio" dei sistemi (art. 12 e 13 RTS 7).

---

[137] LUCANTONI, P. (2019). L'«high frequency trading» nel prisma della vigilanza algoritmica del mercato. *Analisi Giuridica dell'Economia*, (1), p. 307.
[138] ANNUNZIATA, F. (2024). Intelligenza artificiale e disciplina degli abusi di mercato. XV Convegno Nazionale Orizzonti del Diritto Commerciale – Imprese e mercati: numeri e computer science (Atti dell'anno 2024). Orizzonti del Diritto Commerciale, p. 16.
[139] Art 48 (1) MiFID II.
[140] Come si può apprendere, questa tipologia di test costituisce il corrispettivo analogo del *behavioral test* condotto dalle imprese di investimento, questa volta non riguardante l'algoritmo bensì il corretto funzionamento dell'infrastruttura di mercato.
[141] In questo caso si tratta dei *conformance tests,* anticipati al paragrafo precedente.

In secondo luogo, la direttiva MiFID II elenca una serie di norme di centrale rilevanza al fine di contenere non solo gli effetti negativi derivanti dell'HFT, come una maggior volatilità o forti turbolenze, ma anche i potenziali abusi che possono essere perpetrati tramite gli strumenti algoritmici. In questo senso, merita essere di riportata la disposizione contenuta all'articolo 48 paragrafo 5 della MiFID II in cui il legislatore ha fatto discendere per sedi di negoziazione il dovere di dotarsi di sistemi che siano in grado di "sospendere o limitare temporaneamente le negoziazioni".

Si tratta in questo caso dei cosiddetti "*circuit breakers*" , ossia meccanismi che si attivano in presenza di forti oscillazioni dei prezzi di uno strumento finanziario e che sono in grado di interrompere totalmente le negoziazioni del titolo (*trading halts*) ovvero circoscriverne la negoziabilità entro determinate soglie (*price collars*) con la conseguenza di sospendere e rinviare tutti quegli ordini che fuoriescono dai *range* determinati.[142] Questi strumenti, che si applicano al singolo titolo e non a tutto il mercato ("*stock specific*"), [143] risultano essere molto efficaci potendo ridurre notevolmente i rischi di *flash crash* causati da algoritmi fuori controllo o da ordini errati.[144]

Il legislatore europeo è intervenuto molto saggiamente anche sulla disciplina relativa alle strutture commissionali praticate dalle *trading venues* nei confronti dei membri del mercato. Sovente accade che le piattaforme di negoziazione, al fine di attirare un maggior numero di clienti, applichino commissioni molto basse o dei veri e propri rimborsi per tutti quegli operatori HFT che inseriscano ordini al limite (*maker taker pricing*). [145] Sul punto è intervenuto l'art 48 par. 9 della MiFID II che ha imposto alle sedi di negoziazione di garantire che le commissioni per l'esecuzione delle operazioni, quelle accessorie e i rimborsi siano *"trasparenti, eque e non discriminatore e che non costituiscano un incentivo a inserire, modificare o cancellare ordini oppure a eseguire transazioni in*

---

[142] EUROPEAN SECURITIES AND MARKETS AUTHORITY (ESMA). (2017). Final report – Guidelines on the calibration of circuit breakers and the publication and reporting of trading halts under MiFID II (ESMA70-872942901-17). ESMA.

[143] LEE, J., & SCHU, L. (2021). Regulation of algorithmic trading: Frameworks for human supervision and direct market interventions. *European Business Law Review,* pp. 18-19.

[144] GOULD, A. L. (2011). Regulating high-frequency trading: Man v. machine. *Journal of High Technology Law*, 12, 273–281.

[145] La struttura commissionale chiamata *maker-taker pricing* consiste nell'applicazione di commissione più alte per coloro che sottraggono liquidità al mercato mediante ordini al mercato (*market order*) mentre commissioni più basse, se non veri e propri rimborsi a coloro che offrono liquidità, aumentando la profondità del *book* di negoziazione tramite *limit orders*.

modo tale da contribuire a creare condizioni di negoziazioni anormali o abusi di mercato".

Allo stesso tempo, si riconosce alle sedi la facoltà di adottare misure penalizzanti nei confronti delle imprese di investimento algoritmiche, nella forma di commissioni più elevate per gli ordini immessi e successivamente cancellati, in tutti quei casi in cui venisse oltrepassata una determinata soglia OTR (*order trade ratio*)[146] ovvero *fees* (tasse) direttamente penalizzanti per tutti coloro che "impieghino tecniche di negoziazione algoritmiche ad alta frequenza".[147] Tenuto conto della natura facoltativa della disposizione in parola, è legittimo domandarsi se tale ultima disposizione rischi di tradursi in lettera morta in quanto ad efficacia: per quale ragione una sede di negoziazione dovrebbe limitare l'operatività degli HFT *traders,* imponendo loro commissioni più elevate, e rinunciare a possibili guadagni?

1.7 VALUTAZIONI

Il *corpus* di norme vigente risulta essere, nel suo complesso, una disciplina completa e che tiene conto delle maggiori le problematiche emerse nel corso del tempo.[148] L'obiettivo di mitigare i rischi e la difficoltà per le autorità di regolazione di rimanere al passo con le evoluzioni tecnologiche, ha spinto il legislatore europeo ad adottare un sistema di controllo decentralizzato, basato su "tre linee difensive"[149] rispettivamente rappresentate dalle imprese di investimento, dalle sedi di negoziazione e dalle Autorità di regolazione, ciascuna con specifici obblighi di monitoraggio.

In questo schema a "gradini crescenti" il legislatore ha poi preferito costruire un impianto normativo basato sui principi (*principle based approach*) piuttosto che dettare regole

[146] L'OTR è un parametro utilizzato nei mercati finanziari per misurare la relazione tra il volume totale degli ordini inviati a una piattaforma di trading e il numero di scambi effettivamente eseguiti.
[147] Art. 48 par. (10) MiFID II.
[148] WOODWARD, M. (2017). The need for speed: Regulatory approaches to high frequency trading in the United States and the European Union. *Vanderbilt Journal of Transnational Law*, 50(5), p. 39–40.
[149] AZZUTTI, A. (2022). The algorithmic future of EU market conduct supervision: A preliminary check. In Böffel, L., & Schürger, J. (Eds.), Digitalisation, Sustainability, and the Banking and Capital Markets Union: Thoughts on Current Issues of EU Financial Regulation, pp. 53–98. Palgrave Macmillan, Cham, p. 63.

rigide e specifiche (*rule based approach*). [150] Di conseguenza, una certa discrezionalità è stata lasciata agli stati membri e agli operatori coinvolti, mediante la formulazione di *enabling rules (*norme abilitanti n.d.r.*)*, [151] affinché questi adottino a seconda delle circostanze, le misure a loro più congeniali. [152]

Le intenzioni sono meritevoli di considerazione: da un lato, legislazioni iper-specifiche e aggressive rischiano di far perdere l'attrattività di certi mercati, dando luogo a fenomeni di migrazione verso legislazioni più favorevoli e meno stringenti (*off shoring*); [153] dall'altro, una normativa flessibile è una normativa che sa meglio adattarsi alle sfide future senza eccessivi costi di cambiamento.

Pertanto, di fronte a tecnologie multiformi e mutevoli nel corso del tempo, la soluzione migliore parrebbe proprio essere quella di costruire un sistema di principi che favorisca gli operatori a trovare una risposta e una soluzione ai problemi del mercato. In altre parole, si tratta di costruire un sistema in cui scopo del legislatore non sia quello di intervenire direttamente nella soluzione dei problemi con regole *ad hoc*, bensì quello di delegare il compito agli operatori stessi.

Il quadro regolatorio sino ad ora analizzato riesce, in parte, a contenere gli effetti negativi descritti al paragrafo 1.4.3, e la dimostrazione risiede nel fatto che sin dalla sua introduzione nessun grave incidente di mercato, dovuto a difetti degli ambienti di negoziazione algoritmica, si è più verificato.[154]

[150] ČUK, T., & VAN WAEYENBERGE, A. (2020). European legal framework for algorithmic and high frequency trading (MiFID II and MAR): A global approach to managing the risks of the modern trading paradigm (Working paper), p. 8.
[151] GARGANTINI, M., & SIRI, M. (2019). Il "prezzo dei prezzi": Una soluzione di mercato ai rischi dell'high frequency trading? (Relazione al X Convegno annuale dell'Associazione Italiana dei Professori Universitari di Diritto Commerciale "Orizzonti del Diritto Commerciale", "L'evoluzione tecnologica e il diritto commerciale", Roma), p. 14.
[152] Si pensi, ad esempio, alla norma che dà la facoltà alle sedi di negoziazione di adottare misure penalizzanti verso i *traders* nella forma di commissioni più elevate in caso di ordini immessi e successivamente cancellati di cui all'art 48 par. (10) MiFID.
[153] BELL, H., & SEARLES, H. (2014). An analysis of global HFT regulation: Motivations, market failures, and alternative outcomes (Mercatus Center Working Paper No. 14-11). Mercatus Center at George Mason University, pp. 47–48.
[154] ANNUNZIATA, F. (2023). Artificial intelligence and the regulation of market abuse: A European perspective. Edward Elgar Publishing, Cheltenham (UK)–Northampton, MA (USA) p. 142.

Cionondimeno, al giorno d'oggi emergono alcune problematiche, tra cui quella dell'implementazione dei sistemi di intelligenza artificiale negli strumenti di *trading* algoritmico*:* nel prosieguo della presente analisi ne saranno esaminati gli aspetti più salienti.

VERSO UN TRADING ALGORITMICO 2.0

1.8 INTRODUZIONE

Quando ci si riferisce al termine *Intelligenza Artificiale* [155] si allude all'insieme di tutte quelle macchine computazionali in grado di eseguire compiti che tradizionalmente sono caratteristici dell'intelligenza umana.[156] Quello dell'IA non è un settore recente: già nella seconda metà del Novecento si cominciò a riflettere sulla possibilità di creare macchine in grado di simulare i processi cognitivi umani, ponendo le basi per i successivi sviluppi.

Al giorno d'oggi sono innumerevoli i settori in cui l'intelligenza artificiale trova una applicazione, permettendo di raggiungere risultati impressionanti e, talvolta, riuscendo a superare le stesse capacità dell'essere umano. [157] Tra i settori più interessati da questa rivoluzione tecnologica si ricorda quello dei servizi finanziari, in cui tecniche e strumenti basati sull'IA (FinTech) [158] permettono di migliorare sempre più le attività di *trading* e di investimento.[159]

---

[155] Il termine *intelligenza artificiale* viene attribuito al matematico e informatico statunitense John McCarthy, che lo coniò nel 1955 mentre stava preparando la proposta per un seminario di studio che si sarebbe tenuto l'anno successivo al Dartmouth College (New Hampshire, USA), nell'estate del 1956. Si rinvia in proposito a: MCCARTHY, J., MINSKY, M. L., ROCHESTER, N., & SHANNON, C. E. (1955). A proposal for the Dartmouth Summer Research Project on Artificial Intelligence [Proposta dattiloscritta non pubblicata]. Dartmouth College, Hanover, NH, pp. 1–17.

[156] PASCALE, N. (2022). Machine Learning e Deep Learning: applicazioni e dubbi etici. In NATALE, A. (a cura di), *Fintech. I confini dell'innovazione nella finanza*, p. 245. Giuffrè Francis Lefebvre, Milano, p. 245.

[157] FRASSO, E. (2023). Quando l'intelligenza artificiale batte gli umani: I casi più recenti. AI News, n.p. (https://ainews.it/quando-lintelligenza-artificiale-batte-gli-umani-i-casi-piu-recenti/; SGARLATO, G. (2023). Quando l'IA batte l'uomo: La storia di Lee Se-dol e le cinque fasi del lutto digitale. *Il Sole 24 Ore – 24+*, n.p. https://24plus.ilsole24ore.com/art/quando-l-ia-batte-l-uomo-storia-lee-se-dol-e-cinque-fasi-lutto-digitale-AHaQRtvB.

[158] Con il termine FinTech si allude all' impiego della tecnologia impiegata per fornire soluzioni finanziarie. Per un resoconto storico si consulti: ARNER, D. W., BARBERIS, J., & BUCKLEY, R. P. (2015). The evolution of FinTech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47, pp. 1271–1319.

[159] INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS [IOSCO]. (2021). The use of artificial intelligence and machine learning by market intermediaries and asset managers (FR06/2021, Final Report). International Organization of Securities Commissions, p. 9. (finding that: "*The rise in the use of electronic trading platforms and the increase of available data have led firms to consider the use of AI and ML in several areas, including for their trading and advisory activities, as well as for risk management and compliance"*).

Diversi sono i fattori trainanti del FinTech. Da una parte la crescita di tecniche di negoziazione basate sull'intelligenza artificiale risponde alle specifiche esigenze degli operatori di mercato, nell'ottica di offrire un servizio migliore ai propri clienti.[160] In questo senso, l'impiego di tali strumenti permette non solo una ottimizzazione interna dei processi riducendo i margini di errore e un incremento della produttività ma anche l'ottenimento di vantaggi competitivi significativi, data la grande capacità dell'IA di elaborare enormi quantità di dati. Al tempo stesso, la crescente complessità normativa ha spinto, da un lato, gli intermediari a dotarsi di sistemi "intelligenti" al fine di monitorare il rispetto e la corretta applicazione degli obblighi regolamentari (in dottrina tale fenomeno prende il nome di *RegTech*) e, dall'altro, a far sì che le autorità di vigilanza iniziassero a dotarsi di modalità di supervisione basate sull'intelligenza artificiale al fine di pervenire a una maggior efficacia nei controlli (*SupTech).*

Accanto a questi motivi strategici, economici e normativi i *market partecipants* hanno poi beneficiato anche della disponibilità di strumenti IA sviluppati per applicazioni in altri settori.[161] Sotto questo punto di vista, grazie allo sfruttamento delle "economie di diversificazione", è aumentata la capacità di calcolo dei *computer* e si sono ridotti i costi di archiviazione e analisi dei dati. Inoltre, determinante è stata l'enorme diffusione dei *big data* a partire dagli anni 2000 che ha consentito l'accesso a una mole gigantesca di informazioni che gli algoritmi sono in grado di processare.[162]

1.9 MACHINE LEARNING E DEEP LEARNING

Quando ci si riferisce all'espressione "*intelligenza artificiale applicata al trading*" si allude a un concetto dai contorni parecchio ampi e mutevoli nel corso del tempo. I primi modelli di *AI trading* sono stati definiti in dottrina con il termine di "*Good Old-Fashioned*

[160] AZZUTTI, A., RINGE, W.-G., & STIEHL, H. S. (2022). The regulation of AI trading from an AI life cycle perspective (European Banking Institute Working Paper No. 130), p. 6.
[161] FINANCIAL STABILITY BOARD (2017). *Artificial intelligence and machine learning in financial services: Market developments and financial stability implications* pg. 7-10.
[162] *Ibidem*.

AI” (GOFAI), [163] formula che si riferisce alle prime applicazioni di “AI simbolica” o “AI deterministica” impiegate a partire dagli anni ‘90.[164]

Tali sistemi si fondavano sull’inserimento esplicito, da parte di esperti umani, di conoscenze e ipotesi relative a un determinato dominio, all’interno dei programmi informatici (*software*). In particolare, compito della macchina era quello di generare meccanicamente un *output* (ad es. comprare o vendere determinati strumenti finanziari) al ricorrere delle condizioni fissate *ex ante* dai programmatori e inserite all’interno di una tabella chiamata *Knowledge Base* (KB), contenente le regole di comportamento della macchina. In altre parole, l’algoritmo leggeva i dati in ingresso provenienti dal mercato, li confrontava con le istruzioni condizionali contenute nella KB (*if / then: “*se” / “allora”) e laddove vi fosse stata una corrispondenza, avrebbe eseguito l’operazione. [165]

Questa impostazione aveva diversi limiti, tra i quali, il più rilevante, consisteva nel fatto che l’essere umano era tenuto a esplicitare tutto il suo patrimonio conoscitivo all’interno dei programmi.

Al fine di superare tale limite, a partire dagli anni 2000 si è assistito a un’evoluzione che ha portato all’implementazione dei sistemi di *machine learning* negli strumenti di negoziazione algoritmica, dando così vita alla “prima generazione di *machine learning* applicata al *trading*” (*second AI generation*).[166]

Con il termine *machine learning* (ML) si fa riferimento a una branca dell’intelligenza artificiale la cui caratteristica distintiva risiede nella *pattern recognition* ossia nella scoperta automatica di regolarità nei dati tramite algoritmi, e nell’ uso di tali regolarità per compiere azioni.[167] Più nel dettaglio, nei modelli di *machine learning*, l’algoritmo,

---

[163] AZZUTTI, A. (2024). AI governance and algorithmic trading: Some regulatory insights from the EU AI Act. *Banking & Finance Law Review*, 41(1), pp. 133–168.

[164] BODEN, M. A. (2014). GOFAI. In Frankish, K., & Ramsey, W. M. (Eds.), *The Cambridge handbook of artificial intelligence*. Cambridge University Press, pp. 89–107.

[165] JANIESCH, C., ZSCHECH, P., & HEINRICH, K. (2021). Machine learning and deep learning. *Electronic Markets*, 31(3), p. 686. (Finding that: “*Early AI research focused primarily on hard-coded statements in formal languages, which a computer can then automatically reason about based on logical inference rules. This is also known as the knowledge base approach).*

[166] BORCH, C., & MIN, B. H. (2023). Machine learning and social action in markets: From first- to second-generation automated trading. *Economy and Society*, 52(1), p. 37 (finding that: “*Where first-generation systems are based on human-defined rules,second-generation systems develop their trading rules independently”*).

[167] BISHOP, C. M. (2006). Pattern recognition and machine learning. Springer, New York, NY, p. 1.

durante la fase di addestramento (detta *training*) viene esposto ad un insieme molto vasto di dati, all'interno dei quali il medesimo è in grado di individuare schemi ricorrenti (*pattern*) e relazioni statistiche. Tali correlazioni vengono apprese e successivamente utilizzate, durante la fase operativa, per svolgere compiti specifici, come effettuare previsioni o classificazioni su nuovi dati mai visti prima.[168] Gli algoritmi, pertanto, usano modelli matematici complessi per ottenere informazioni direttamente dai dati e sono capaci di migliorarsi attraverso l'esperienza, man mano che gli *input* ricevuti crescono di numero.[169] Confrontando i primi modelli deterministici di intelligenza artificiale, basati su uno schema "regola-azione", con quelli più recenti, il rapporto in questione risulta essere invertito: la regola non occupa più la posizione a "monte" come condizione operativa, bensì viene ricavata ora dall' algoritmo "a valle", al termine di un processo di apprendimento.[170]

Le tipologie tramite le quali un *computer* di *trading* basato su *machine learning* può apprendere dai dati sono tre: l'apprendimento supervisionato (*supervised learning*, SL), l'apprendimento non supervisionato (*unsupervised learning*, UL) e apprendimento con rinforzo (*reinforcement learning*, RL).[171]

Nel primo caso, l'algoritmo viene addestrato su un insieme di dati "etichettati" in cui a ciascun input viene associato lo specifico output desiderato. Questa tipologia di apprendimento permette, durate la fase operativa, di effettuare regressioni (ossia previsioni tramite algoritmi di *regressione lineare*) ovvero classificazioni (ad es. ricorrendo ad algoritmi quali il *support vector machine* o alberi decisionali): ad esempio, un *trader* umano può fornire all'algoritmo dati storici di mercato (come prezzi, volatilità

---

[168] CHAHAL, A., & GULIA, P. (2019). Machine learning and deep learning. *International Journal of Innovative Technology and Exploring Engineering*, 8(12), p. 4910.

[169] È opportuno qui distinguere tra "dati di addestramento", ossia dati e informazioni che vengono fornite alla macchia nella fase di addestramento (o *training*) prima di un effettivo utilizzo, e "dati di *input"*, con cui si intendono le informazioni che l'algoritmo riceve quando viene effettivamente impiegato per operare sui mercati.

[170] MAGNUSON, W. J. (2020). Artificial financial intelligence. *Harvard Business Law Review*, 10(2), p. 344 (finding that: "*Machine learning, rather than relying on a set of rules established by a programmer, as in expert systems, instead starts with a data set and then attempts to derive rules on its own"*).

[171] FINANCIAL STABILITY BOARD [FSB]. (2017). Artificial intelligence and machine learning in financial services: Market developments and financial stability implications. Financial Stability Board, p. 5.

etc..) affinché sia in grado di prevedere l'andamento di prezzo di un'azione [172] ovvero di un indice.[173]

Il secondo modello di apprendimento viene definito "non supervisionato" (UL) in quanto l'algoritmo, durante la fase di addestramento, riceve solamente input "non etichettati", cioè, privi di indicazioni sul risultato desiderato. In tale contesto, l'algoritmo (tra i più noti si ricordano *K-means* e *BDSCAN*) si limita a individuare schemi o caratteristiche simili nei *dataset* con l'obiettivo di effettuare raggruppamenti (*clustering*). Ad esempio, il *trader* può impiegare l'algoritmo di UL per eseguire un'analisi di *cluster pre-trade* su un determinato portafoglio di strumenti finanziari in base alla probabilità che tali strumenti registrino un rendimento giornaliero positivo alla luce delle osservazioni passate, così da informare le successive decisioni di *trading*.[174]

Infine, l'ultima tipologia di apprendimento è quella "per rinforzo" (RL). In questo caso, l'algoritmo (uno dei più impiegati è quello denominato *Q-learning*) durante la fase di *training* interagisce con l'ambiente circostante — dal quale riceve costantemente informazioni e dati (ad es. segnali dall*'order book*) — ed esegue operazioni seguendo un meccanismo di ricompense e penalità: le azioni che portano a risultati positivi vengono premiate e quindi rinforzate, mentre quelle che producono esiti negativi vengono scoraggiate, permettendo al sistema di ottimizzare progressivamente il proprio comportamento. I sistemi che si basano sulla tecnologia RL costituiscono i modelli più avanzati di *machine learning* in quanto possono essere alla base di "*autonomous* (*software*) *agents*", ossia di agenti autonomi capaci riprodurre il modo in cui i *traders* umani agiscono tradizionalmente sui mercati finanziari, apprendendo dalle proprie esperienze di *trading* e sviluppando strategie per perseguire obiettivi di massimizzazione del profitto.[175]

---

[172] BALAJI, A. J., RAM, D. S. H., & NAIR, B. B. (2018). Applicability of deep learning models for stock price forecasting: An empirical study on BANKEX data. *Procedia Computer Science*, 143, pp. 947–953.
[173] SADAF ET AL. (2021). Algorithmic trading, high-frequency trading: Implications for MiFID II and Market Abuse Regulation (MAR) in the EU. SSRN, p. 8.
[174] AZZUTTI, A., RINGE, W.-G., & STIEHL, H. S. (2022). The regulation of AI trading from an AI life cycle perspective (European Banking Institute Working Paper No. 130), p. 7.
[175] AZZUTTI, A., RINGE, W.-G., & STIEHL, H. S. (2021). Machine learning, market manipulation and collusion on capital markets: Why the "black box" matters. *University of Pennsylvania Journal of International Law*, 43(1), p. 88.

I metodi di apprendimento per rinforzo (RL) possono essere direttamente implementati nei sistemi di *Trading* algoritmico e *High frequency trading* al fine di migliorare le prestazioni di negoziazione, prevedere i movimenti direzionali dei prezzi a partire dai segnali del *book* ordini, per ottimizzare l'esecuzione delle operazioni [176] ovvero per condurre strategie di *market making*.[177]

A partire dal 2010 è emersa infine un'ulteriore branca dell'IA che prende il nome di *deep computational finance,* termine entro il quale vengono ricomprese un ampio numero di applicazioni basate sul *deep learning* (DL).

Con il termine *deep learning* (o apprendimento profondo) si fa riferimento a una sottocategoria del *machine learning* basata su "reti neurali artificiali" (*artificial neural networks*, ANNs) ossia strutture computazionali ispirate al funzionamento del cervello umano. In particolare, la rete si caratterizza per la presenza di più strati (o *layers*) all'interno dei quali sono disposti diversi nodi (o "neuroni artificiali").

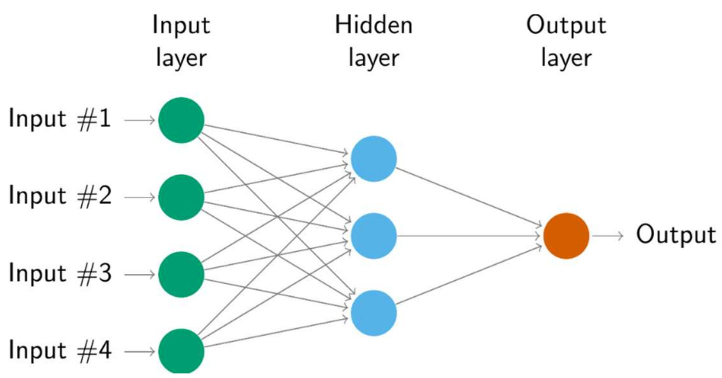

Fig. 3: rappresentazione di una rete neurale artificiale (Fonte: https://otexts.com/fppit/nnetar.html)

[176] KEARNS, M., & NEVMYVAKA, Y. (2013). Machine learning for market microstructure and high frequency trading. In Easley, D. A., López de Prado, M., & O'Hara, M. (Eds.), High-frequency trading: New realities for traders, markets and regulators. Risk Books, London, pp. 91–124*,* in cui si analizza come l'applicazione del RL all' HFT possa i) ottimizzare I processi di esecuzione degli ordini ii) predire i prezzi a partire dall' analisi dell'*order book* iii) ottimizzare l'esecuzione nelle *dark pools.*

[177] SPOONER, T., FEARNLEY, J., SAVANI, R., & KOUKORINIS, A. (2018). Market making via reinforcement learning. In Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS 2018). International Foundation for Autonomous Agents and Multiagent Systems, Stockholm, pp. 434–442.

La forza del DL risiede nel suo funzionamento: il primo strato (*input layer*) riceve un input dall'esterno (ad. es. informazioni concernenti prezzi, volatilità e volumi scambiati) e lo trasmette agli strati successivi (*hidden layers*).

All'interno di questi *layers* avviene un passaggio decisivo: gli input vengono "pesati", cioè ciascuno di essi viene moltiplicato per un valore numerico che ne esprime la sua rilevanza ai fini della decisione finale, e successivamente, i valori ottenuti vengono sommati. Una volta calcolato, tale valore viene elaborato da una funzione di attivazione che determina, secondo una logica non lineare, l'intensità del segnale da trasmettere ai neuroni dello strato successivo.[178] In questo modo "l'output del livello precedente diventa l'input di quello successivo", [179] permettendo una elaborazione sempre più profonda e precisa, così da favorire la scoperta di leggi più complesse a partire dai dati.

Nell' immagine che segue (Fig. 4) è rappresentato il processo di calcolo che ha luogo all' interno di ogni nodo: ciascun input viene moltiplicato per il suo peso e successivamente viene eseguita la sommatoria finale degli input pesati, indicata con il simbolo $\sum$.

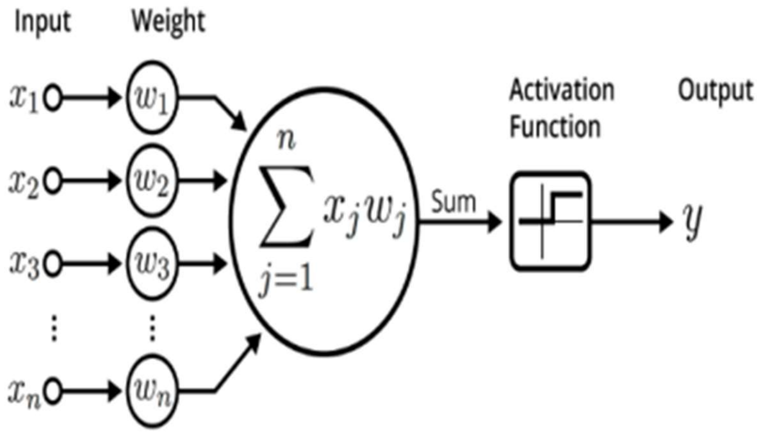

Fig. 4: rappresentazione del processo di calcolo in un neurone artificiale (Fonte: Gulia, P. (2019). Machine Learning and Deep Learning. International Journal of Innovative Technology and Exploring Engineering).

[178] CORASANITI, G. (2022). Data science e diritto, certezze digitali e benefici del dubbio. G. Giappichelli Editore, Torino, p. 81.
[179] PASCALE, N. (2022). Machine Learning e Deep Learning: applicazioni e dubbi etici. In NATALE, A. (a cura di), *Fintech. I confini dell'innovazione nella finanza*, p. 245. Giuffrè Francis Lefebvre, Milano, p. 253.

A differenza del *machine learning* tradizionale, in cui è l'essere umano a selezionare manualmente le caratteristiche rilevanti da fornire al modello (operazione nota come *feature engineering*) orientando la macchina verso un *output* finale, nel *deep learning* tale processo risulta avvenire in automatico. Le architetture complesse delle reti neurali consentono infatti al sistema di apprendere direttamente dai dati le rappresentazioni (*features*) più utili a distinguere le informazioni, senza che sia necessario un intervento esterno di definizione preliminare delle variabili rilevanti. In altre parole, il modello è in grado di estrarre autonomamente quali elementi del *dataset* siano significativi ai fini dell'analisi, realizzando così una forma di auto-apprendimento (*self-learning*) delle caratteristiche da elaborare. [180]

Le tecniche di *deep learning* possono trovare applicazione in innumerevoli settori, tra cui anche quello finanziario.[181] Essendo il DL una sottocategoria del *machine learning,* questa può essere applicata per l'apprendimento supervisionato, non supervisionato e rinforzato.[182]

In questo ultimo caso, la combinazione del *deep learning (DL)* con il *reinforcement learning (RL)* porta alla creazione dei sistemi di *deep reinforcement learning (DRL)* aprendo la strada a interessantissime considerazioni.[183] Combinando infatti vantaggi dei due modelli è possibile pervenire alla definizione di veri e propri "agenti autonomi" che interagiscono con l'ambiente circostante per apprendere i comportamenti ottimali e

---

[180] JANIESCH, C., ZSCHECH, P., & HEINRICH, K. (2021). Machine learning and deep learning. *Electronic Markets*, 31(3), pp. 685–695.

[181] OZBAYOĞLU, A. M., GUDELEK, M. U., & SEZER, O. B. (2020). Deep learning for financial applications: A survey. *Applied Soft Computing*, 93, Article 106384, (gli autori forniscono una analisi delle principali applicazioni del DL nel contesto dei mercati finanziari).

[182] FINANCIAL STABILITY BOARD [FSB]. (2017). Artificial intelligence and machine learning in financial services: Market developments and financial stability implications. Financial Stability Board, p. 5 (finding that: "*Deep learning algorithms, whose structure are called artificial neural networks, can be used for supervised, unsupervised, or reinforcement learning"*).

[183] Sul tema la letteratura è molto ampia: ARULKUMARAN, K., DEISENROTH, M. P., BRUNDAGE, M., & BHARATH, A. A. (2017). A brief survey of deep reinforcement learning. *IEEE Signal Processing Magazine*, 34(6), pp. 26–38; ZHANG, Z., ZOHREN, S., & ROBERTS, S. (2020). Deep reinforcement learning for trading. *The Journal of Financial Data Science*, 2(2), pp. 25–40; DENG, Y., BAO, F., KONG, Y., REN, Z., & DAI, Q. (2017). Deep direct reinforcement learning for financial signal representation and trading. *IEEE Transactions on Neural Networks and Learning Systems*, 28(3), pp. 653–664; LI, Y., ZHENG, W., & ZHENG, Z. (2019). Deep robust reinforcement learning for practical algorithmic trading. *IEEE Access*, 7, pp. 108014–108022; PRICOPE, T.-V. (2021). Deep reinforcement learning in quantitative algorithmic trading: A review (arXiv:2106.00123). arXiv, pp. 1–20.

migliorare nel tempo attraverso il meccanismo di ricompense e penalità.[184] In particolare, un algoritmo di *trading* basato su *deep reinforcement learning* è in grado di estrarre informazioni riguardo a un ambiente di negoziazione complesso grazie al *deep learning* (DL) e, in secondo luogo, di utilizzare il *reinforcement learning* (RL) per sperimentare, in modo flessibile, strategie di negoziazione ottimali.[185]

Come è facile notare, con l'avvento della *deep computational finance* le modalità di operare sui mercati finanziari mutano radicalmente: l'immagine cinica e spietata del *trader* in giacca e cravatta icasticamente raffigurata in svariate opere cinematografiche e già messa in discussione con le tecniche di negoziazione algoritmica e ad alta frequenza, risulta ora essere ancor più sfocata ed indebolita, lasciando così il posto a quella più grigia e fredda di enormi super *computer* in grado di agire in maniera libera e indipendente.

1.10 INTELLIGENZA ARTIFICIALE E PROBLEMI NORMATIVI

Nel paragrafo che precede è stato evidenziato come nel corso del tempo l'evoluzione delle modalità di *trading* abbia portato all'ideazione di tecnologie sempre più svincolate dall'essere umano. Questa evoluzione, tuttavia, non è immune da considerazioni circa il livello di allineamento dei parametri normativi e regolatori con i sistemi IA (*AI alignement*). In particolare, occorre chiedersi se la normativa attuale tenga adeguatamente in considerazione i fenomeni del *machine learning* e *deep learning* applicati nel più ampio contesto della negoziazione algoritmica e di quella ad alta frequenza.

Come è stato fatto notare in precedenza, la normativa concernete l'AT e l'HFT è incentrata sul principio di controllo dei rischi al fine di assicurare un corretto e ordinato funzionamento del mercato. Il legislatore ha previsto, pertanto, una serie di requisiti ed obblighi specifici sia per le imprese che svolgono HFT sia per le piattaforme di negoziazione, tra i quali lo svolgimento di appositi *test di comportamento.*[186]

---

[184] ARULKUMARAN, K., DEISENROTH, M. P., BRUNDAGE, M., & BHARATH, A. A. (2017). A brief survey of deep reinforcement learning. *IEEE Signal Processing Magazine*, 34(6), p. 26.
[185] AZZUTTI, A., RINGE, W.-G., & STIEHL, H. S. (2021). Machine learning, market manipulation and collusion on capital markets: Why the "black box" matters. *University of Pennsylvania Journal of International Law*, 43(1), p. 91.
[186] Si veda art. 6 Reg. 2017/589 (RTS 6).

Per quello che concerne ai nostri fini, di grande rilevanza è la formulazione contenuta nell'articolo 5, par. 4 del Reg. 2017/589 (RTS 6) in cui si stabilisce che tra gli obiettivi che il *behavioral test* deve perseguire vi è quello di assicurare un comportamento "*non imprevisto*" dell'algoritmo.

Per cogliere appieno il significato di tale affermazione, bisogna anzitutto comprendere quando un algoritmo funzioni in un modo tale da potersi definire "prevedibile". In breve, una tale situazione ricorre ogniqualvolta la macchina analizza i dati provenienti dal mercato, li confronta con le istruzioni in base alle quali è stata programmata e, laddove rilevi una corrispondenza, compie l'operazione [187] (ad esempio, eseguendo un ordine *limit* una volta raggiunta una soglia prefissata).[188] In questa accezione, il concetto di "prevedibilità" viene inteso come possibilità di prevedere *ex ante* il comportamento della macchina al ricorrere di determinate condizioni, implicando, perciò, un potere di controllo dell'uomo su di essa. Una simile situazione si confà perfettamente a tutti quei sistemi in cui il computer di *trading* è basato su algoritmi "statici" e "deterministici" *("good old fashion AI")*.

Tuttavia, il discorso muta radicalmente se il computer di *trading* si dovesse basare su un sistema di autoapprendimento come quello di *deep reinforcement learning* (DRL).[189] In tal caso, poiché è l'algoritmo stesso ad elaborare strategie di *trading* attraverso l'interazione con l'ambiente che lo circonda, aggiornandole a seconda delle condizioni di mercato, risulterebbe impossibile prevedere *ex ante* il comportamento della macchina. Una siffatta situazione rende, pertanto, l'algoritmo capace di agire in maniera del tutto imprevedibile e ciò fa sorgere dubbi circa la legittimità del medesimo. [190]

A tal proposito, non appare condivisibile l'interpretazione della norma nel senso di vietare sistemi di negoziazione "autonomi", e di ammettere solamente quelli "statici". Invero, regolando il fenomeno dell'AT e HFT all' interno della MiFID, il legislatore non ha solo

---

[187] RASCHNER, P. (2021). Algorithms put to test: Control of algorithms in securities trading through mandatory market simulations? (European Banking Institute Working Paper No. 87). SSRN, p. 6.
[188] BRUMMER, C. (2020). Fintech law in a nutshell. West Academic Publishing, St. Paul, MN, p. 248.
[189] Su punto, anche la autorità olandese per i mercati finanziari: DUTCH AUTHORITY FOR THE FINANCIAL MARKETS [AFM]. (2023). Machine learning in algorithmic trading: Application by Dutch proprietary trading firms and possible risks. Dutch Authority for the Financial Markets, p. 23
[190] SPINDLER, G. (2020). Control of algorithms in financial markets – The example of high frequency trading. In Ebers, M., & Navas, S. (Eds.), Algorithms and law. Cambridge University Press, p. 217.

implicitamente approvato tali strumenti ma ha altresì dimostrato un atteggiamento di apertura verso le innovazioni tecnologiche. In questo senso, un divieto categorico parrebbe un veto eccessivo allo sviluppo e all'innovazione, oltre ad essere contrario allo spirito di neutralità tecnologica che anima la direttiva MiFID II.

Un ulteriore punto problematico concerne i paragrafi 1 e 5 del medesimo articolo. Le norme chiedono infatti alle imprese di effettuare test aggiuntivi in caso di "*modifiche o aggiornamenti sostanziali*" degli algoritmi. [191]

Come nel caso precedente, *nulla quaestio* laddove il *computer* di *trading* faccia ricorso ad algoritmi statici. Ciononostante, la norma crea notevoli dubbi in quanto lascia gli operatori di mercato senza spiegazioni precise su come tale obbligo possa essere applicato al comportamento dinamico di un algoritmo di *machine learning.*[192] Un tale algoritmo è in grado di modificarsi continuamente nel corso del tempo adottando strategie e comportamenti nuovi per meglio ottimizzare la sua funzione; ne consegue che siffatti mutamenti potrebbero essere sempre considerati alla stregua di "modifiche sostanziali" tali da richiedere test aggiuntivi.

Da questa breve analisi, è possibile prendere atto come alcune tra le disposizioni contenute nei regolamenti delegati (ai quali la MiFID II rinvia), non sembrino tenere adeguatamente in considerazione il fenomeno del *machine learning,* nel contesto della negoziazione finanziaria. Al contrario, ad avviso di chi scrive, la definizione di "negoziazione algoritmica" formulata nell' art. 4(1)(39) (MiFID II) risulta essere sufficientemente ampia e neutra da ricomprendere anche i casi in cui un *computer* di *trading* dovesse ricorrere ad algoritmi di *machine learning.* Invero, quando viene formulato che il *trading* algoritmico consiste in una tecnica di negoziazione in cui un algoritmo "determina automaticamente i parametri degli ordini", la definizione chiarisce che in tali parametri possono rientrare, tra gli altri, anche il "se" il "quando" avviare l'ordine, ciò sottintendendo una dimensione di autonomia che è tipica degli algoritmi più avanzati.

---

[191] Si veda art. 5 Reg. 2017/589 (RTS 6).

[192] AZZUTTI, A. (2022). The algorithmic future of EU market conduct supervision: A preliminary check. In Böffel, L., & Schürger, J. (Eds.), Digitalisation, Sustainability, and the Banking and Capital Markets Union: Thoughts on Current Issues of EU Financial Regulatio. Palgrave Macmillan, Cham, p. 78.

CONCLUSIONI E OBIETTIVI DELLA RICERCA

Nel presente capitolo è stata tracciata una panoramica circa l'applicazione dei sistemi algoritmici nell'ampio contesto dei mercati finanziari. Sebbene tale inquadramento non possa definirsi esaustivo, dato l'elevato numero di argomenti e il carattere indubbiamente tecnico dei medesimi, si è cercato di ripercorrere i tratti fondamentali che caratterizzano il *trading* algoritmico e la sua applicazione più specifica (ovvero *l'high frequency trading)*. In questo senso, dopo aver esaminato le non poche complesse definizioni di AT e HFT, il lavoro si è concentrato sulla portata e sulle conseguenze che questi strumenti hanno sui mercati, attenzionando sia gli effetti positivi sia quelli negativi.

L'analisi delle conseguenze, in particolare di quelle negative, si è resa necessaria poiché sulla base di queste il legislatore europeo ha incentrato la disciplina speciale contenuta nella MiFID II. L'approfondimento della citata normativa ha evidenziato come la risposta fornita dal legislatore sia stata, nel complesso, capace di fronteggiare i rischi maggiori e le potenziali distorsioni derivanti da questi sistemi avanzati di *trading.* Tuttavia, dubbi ancora residuano in relazione alle forme più avanzate di negoziazione, in cui la presenza della macchina risulta essere totalizzante e prevalere nettamente sulla componente umana. Di tali ipotesi, come è stato dimostrato, la normativa attuale contenuta nei regolamenti delegati, non sembra tenerne pienamente conto, tanto da far emergere dubbi circa la liceità delle stesse.

La disamina degli argomenti sopra riportati ha avuto come obiettivo principale quello di fornire al lettore un quadro introduttivo e sistematico che gli permetta di districarsi meglio in un contesto reso ostico non solo dalla natura macchinosa e complessa degli strumenti in questione ma anche dalla stessa normativa che richiede elevate conoscenze tecniche e specifiche.

Muovendo da tale premessa, nel Capitolo 2 verrà approfondito il profilo concernente il comportamento "esterno" della macchina algoritmica, ed in particolare, le possibili forme di manipolazioni di mercato, attuabili mediante sistemi di *trading* ad alta frequenza. Obiettivo della ricerca sarà, pertanto, quello di indagare se l'attuale assetto normativo risulti adeguato a fronteggiare compiutamente i casi di manipolazione di mercato, compiute “mediante” o “da” un algoritmo di *trading,* con specifico riguardo anche ai correlati profili di responsabilità.

Nel Capitolo 3 si esaminerà invece il profilo concernente la dimensione “interna” della macchina algoritmica, intesa come complessa infrastruttura tecnologica composta da reti e sistemi informativi. In tale prospettiva, la predisposizione di adeguate misure di protezione rispetto a eventuali minacce informatiche si rivela essenziale non solo per l’operatore finanziario direttamente coinvolto, ma anche, data la forte interconnessione e interdipendenza dei soggetti operanti sui mercati, per la stabilità e l’integrità complessiva del sistema stesso.

L’analisi verterà, pertanto, sul quadro normativo vigente in materia di *cybersecurity* applicata ai sistemi di AT e HFT, e – come nel capitolo precedente – si cercherà di valutare, in termini qualitativi, se l’attuale assetto regolatorio possa ritenersi adeguato a garantire una risposta efficace di fronte a tali minacce**.**

.

CAPITOLO II

LE MANIPOLAZIONI DI MERCATO E IL TRADING AD ALTA FREQUENZA

GLI ABUSI DI MERCATO: IL QUADRO NORMATIVO

2.1 PREMESSA

Nel capitolo I è stato esaminato il fenomeno dell'*high frequency trading* sia nella sua versione "tradizionale"*,* sia in quella più recente basata su algoritmi di *machine learning.* In particolare, è stata condotta una analisi sostanziale delle tipologie, identificando i modelli e fornendo una disamina della normativa europea con cui il legislatore ha cercato di regolarne i fenomeni al fine di prevenire i rischi da esso derivanti, inclusi i cd. "*disruptive events".*[193]

L'analisi che verrà trattata nel presente capitolo si soffermerà su un tema centrale relativo al *trading* ad alta frequenza, vale a dire quello degli "abusi di mercato" realizzabili "tramite" sia, come si vedrà, "dalla" macchina stessa. L'argomento risulta di vitale importanza: con l'avvento dei sistemi algoritmici si ampliano, in positivo, non solo le opportunità di negoziazione ma si moltiplicano altresì, in negativo, le possibilità di realizzazione di illeciti nel mercato mobiliare.

---

[193] Il termine *disruption* è un termine che viene elaborato nell'ambito della strategia di impresa ma che può essere esteso anche al contesto dei mercati finanziari. Per un approfondimento si veda: CHRISTENSEN, C. M., RAYNOR, M. E., & MCDONALD, R. (2015). What is disruptive innovation? *Harvard Business Review (*finding that*:* "*disruption" describes a process whereby a smaller company with fewer resources is able to successfully challenge established incumbent businesses"*).

Le probabilità che la macchina venga coinvolta in manipolazioni di mercato sono molto elevate e, pertanto, si rende necessaria una trattazione specifica.[194] Nel prosieguo dei paragrafi verrà perciò analizzata la disciplina europea concernente gli abusi, esaminandone la *ratio*, le norme e i recepimenti a livello dell'ordinamento italiano.

Successivamente, sarà premura indagare quali siano le condotte più pericolose attuabili tramite i sistemi di HFT e che pongono rischi per la sicurezza e tenuta dei mercati. In tale contesto verrà attenzionato il rilevante contributo che le tecniche *machine learning* possono apportare alle suddette strategie, aprendo a scenari e situazioni sino a poco tempo fa inimmaginabili.

Infine, l'ultima parte del presente capitolo sarà dedicata all'analisi della adeguatezza dell'assetto normativo europeo in materia di abusi. In particolare, si esaminerà, in primo luogo, se la disciplina europea vigente sia effettivamente idonea a fronteggiare le manipolazioni realizzate mediante sistemi di *High-Frequency Trading* fondati su algoritmi di *machine learning*. In secondo luogo, ci si concentrerà sul profilo della responsabilità una volta che l'illecito venga concretamente realizzato. Più precisamente, verrà esaminato se l'impiego di algoritmi auto-apprendenti possa porre delle criticità in relazione all'assetto normativo vigente, tali da rendere necessario un ripensamento delle tradizionali categorie di imputazione, ovvero se tali criticità restino confinate prevalentemente sul piano probatorio ed applicativo.

---

[194] Nel presente capitolo l'analisi si soffermerà esclusivamente sulla condotta di"manipolazione di mercato". Come è risaputo, gli abusi di mercato comprendono anche la categoria dell'"abuso di informazioni privilegiate", tuttavia, dato che la forma di abuso più tipica realizzata dagli HFT consiste in condotte manipolative, quest' ultima fattispecie non verrà trattata. Ciò però non sottintende una minor importanza, sul tema si consulti in proposito: RAFFAELE, F., & MANNA, M. (2024). High Frequency Trading e informazioni privilegiate: Insider Trading "strutturale" o lecita superiorità informativa? *Orizzonti del Diritto Commerciale*, (1).
(Gli autori effettuano una interessante disamina della disciplina statunitense ed europea avente ad oggetto *l'insider trading,* concludendo che, se nell'ordinamento statunitense non è possibile ipotizzare il reato di sfruttamento abusivo delle informazioni privilegiate, in quello europeo la risposta non è così perentoria. Grazie alla co-ubicazione e ai *feed* privati, ossia flussi di informazioni provenienti dalla sede di negoziazione e diretti a clienti selezionati, rispetto ad altri HFT e ai cosiddetti *slow traders*, gli autori sono del parere che gli HFT possono essere considerati *insider traders* nell'ordinamento UE).

2.2 EVOLUZIONE E RATIO DELLA NORMATIVA

La legislazione sugli abusi di mercato costituisce un fondamentale caposaldo della disciplina europea del mercato dei capitali. Le norme sulla prevenzione e repressione di suddetti abusi sono da tempo un elemento distintivo del crescente *corpus* normativo del legislatore eurounitario.[195]

Le origini di tale normativa risalgono agli anni '80 del secolo scorso, con la direttiva sulla quotazione in borsa del 1979, [196] in cui il legislatore UE aveva stabilito l'obbligo di divulgare il prima possibile tutte quelle informazioni rilevanti concernenti l'emittente che potessero portare a variazioni sostanziali del prezzo delle azioni. Nel 1989 con la Direttiva *Insider Dealing*,[197] è stato inoltre stabilito il divieto di effettuare operazioni di *insider trading,* anche se*,* la portata di tale atto rimaneva circoscritta e limitata in quanto non affrontava i fenomeni di manipolazione di mercato.[198]

Il passaggio a un regime più completo è avvenuto nel 2003 con la Direttiva 89/592/CEE sugli abusi di mercato ("MAD I") [199] che ha rappresentato un pilastro fondamentale del *Financial Services Action Plan* (FSAP) [200]. Per la prima volta, le norme concernenti l'abuso di informazioni privilegiate e la manipolazione di mercato sono state riunite in un unico atto legislativo.

Tuttavia, la MAD I, essendo una direttiva, prevedeva solamente un'armonizzazione minima delle normative nazionali. Nel 2008 uno studio approfondito del CESR,[201] metteva in luce come la disciplina sugli abusi restava ancora frammentata tra gli Stati membri e le sanzioni, amministrative e penali, risultavano essere eterogenee e poco

[195] ANNUNZIATA, F. (2023). La disciplina del mercato dei capitali. Giappichelli, Torino, p. 469.
[196] Direttiva 5 marzo 1979, 79/279/CEE del Consiglio, recante "Direttiva concernente il coordinamento delle condizioni per l'ammissione di valori mobiliari alla quotazione ufficiale di una borsa valori" (Direttiva ammissione alla quotazione), in GUCE L 66 del 16 marzo 1979.
[197] Direttiva 5 marzo 1979, 79/279/CEE del Consiglio, recante "Direttiva concernente il coordinamento delle condizioni per l'ammissione di valori mobiliari alla quotazione ufficiale di una borsa valori" (Direttiva ammissione alla quotazione), in GUCE L 66 del 16 marzo 1979.
[198] Vedi nota 191, n. 191.
[199] Direttiva 28 gennaio 2003, 2003/6/CE del Parlamento europeo e del Consiglio, recante "Direttiva relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato (abusi di mercato)" (Direttiva MAD), in GUUE L 96 del 12 aprile 2003.
[200] MOLONEY, N. (2014). EU securities and financial markets regulation (3rd ed.). Oxford University Press, Oxford, p. 699.
[201] Committee of European Securities Regulators. (2008). Report on administrative measures and sanctions as well as criminal sanctions available in Member States under the Market Abuse Directive (MAD 2003) (CESR/07-693). CESR.

dissuasive. Il Gruppo di Alto Livello presieduto da Jacques de Larosière affrontò la questione dopo la crisi finanziaria, raccomandando l'adozione di un quadro regolatorio più coerente a livello europeo.[202]

In risposta a tali criticità, il legislatore ha adottato il Regolamento n. 596 del 2014 denominato *Market Abuse Regulation* (d'ora in poi MAR) [203] al fine di raggiungere una maggiore convergenza tra le legislazioni nazionali, onde ridurre così la frammentazione normativa. Parallelamente, è stata emanata anche una nuova direttiva, la n. 57 del 2014 *(*d'ora in poi, MAD II), [204] che richiede agli Stati membri di adottare sanzioni penali contro l'abuso di informazioni privilegiate e la manipolazione di mercato.

Con l'entrata in vigore del MAR, la repressione degli abusi è stata, pertanto, affidata al diritto uniforme dell'UE, attuato negli aspetti di dettaglio dai *technical standard*s dell'ESMA e dalle norme domestiche di adeguamento.[205] In capo al legislatore nazionale è rimasta invece la competenza sulla disciplina penale per le forme più gravi di abusi (Considerando n. 6 MAD II).

La *ratio* sottesa alla disciplina sugli abusi viene individuata dal legislatore UE al Considerando 1 del Reg. MAR in cui si afferma che il mercato interno dei servizi finanziari, debba essere "*efficiente, trasparente ed integrato"* al fine di *"assicurare la crescita economica e la creazione di posti di lavoro*". Il Considerando n. 2 esplicita poi che, al fine di garantire un mercato corrispondente a tali caratteristiche, sia necessario tutelare tanto il "*regolare funzionamento del medesimo*" quanto "*la fiducia del pubblico nei mercati*". Perciò, onde evitare che gli abusi di mercato ledano tali beni giuridici,[206] la disciplina in esame persegue lo "scopo mezzo" della tutela della fiducia degli investitori" e del "regolare funzionamento del mercato". [207] Solo proteggendo questi beni

---

[202] VEIL, R. (Ed.). (2017). European capital markets law (2nd ed.). Hart Publishing, Oxford, p. 184.
[203] Regolamento (UE) 16 aprile 2014, n. 596/2014 del Parlamento europeo e del Consiglio, recante "Regolamento relativo agli abusi di mercato (regolamento sugli abusi di mercato)" (MAR), in GUUE L 173 del 12 giugno 2014.
[204] Direttiva 16 aprile 2014, 2014/57/UE del Parlamento europeo e del Consiglio, recante "Direttiva relativa alle sanzioni penali in caso di abusi di mercato (direttiva sugli abusi di mercato)" (MAD II), in GUUE L 173 del 12 giugno 2014.
[205] PERRONE, A. (2024). Il diritto del mercato dei capitali. Giuffrè Francis Lefebvre, Milano, p. 321.
[206] ANNUNZIATA, F. (2024). The Market Abuse Regulation and the use of general clauses thereunder (Bocconi Legal Studies Research Paper Series)
[207] DI NOIA, C. (2012). Pending issues in the review of the European market abuse rules (ECMI Policy Brief No. 19). European Capital Markets Institute, p. 1.

da condotte abusive, si è in grado di garantire al meglio lo "scopo fine" di un mercato *integrato*, *trasparente* ed *efficiente,* presupposto necessario alla crescita economica interna e alla creazione dei posti di lavoro.

Assumendo infatti l'idea della *efficient capital market hipotesis* (ECMH) [208] secondo cui un mercato è efficiente quanto più i prezzi riflettono tutte le informazioni disponibili, così da garantire una corretta allocazione delle risorse, le pratiche abusive (nella fattispecie di abuso di informazioni privilegiate e manipolazioni di mercato) costituiscono un esempio di *market failure* in quanto, provocando distorsioni nel processo di formazione dei prezzi (*price-formation mechanism)*, causano, al contrario, una inefficiente allocazione delle risorse. [209]

In conclusione, nel contesto specifico del *trading* algoritmico, sembra corretto affermare come la disciplina contenuta nel pacchetto MAR-MAD II appaia un *corpus* normativo atto a garantire che la macchina algoritmica si rapporti "all'esterno" in modo tale che non vengano pregiudicati quei i beni giuridici sopra menzionati. In altre parole, la normativa in esame cerca di intercettare quella dimensione di comportamento "esterno" della macchina al fine di regolarlo e renderlo sicura.

2.3 LA NORMATIVA EUROPEA: MAR e MAD II

La norma fondamentale dalla quale la presente analisi deve partire è rappresentata dall'articolo 15 del *Market Abuse Regulation* (MAR) che, intitolato "Divieto di abusi di manipolazioni di mercato", proibisce tanto il tentativo quanto la realizzazione del fatto illecito.[210]

---

[208] FAMA, E. F. (1970). Efficient capital markets: A review of theory and empirical work. *The Journal of Finance*, 25(2), pp. 383–417 (finding that: "*In general terms, the ideal is a market in which prices provide accurate signals for resource allocation: that is, a market in which firms can make production-investment decisions, and investors can choose among the securities that represent ownership of firms' activities under the assumption that security prices at any time "fully reflect" all available information. A market in which prices always "fully reflect" available information is called "efficient.")*

[209] MOLONEY, N. (2014). EU securities and financial markets regulation (3rd ed.). Oxford University Press, Oxford, p. 705.

[210] L'art. 15 MAR recita in proposito: *"non è consentito effettuare manipolazioni di mercato o tentare di effettuare manipolazioni di mercato"*.

Al fine garantire una adeguata repressione di tali condotte, il legislatore UE ha creato un impianto normativo che assegna al singolo stato membro la facoltà di scegliere la risposta sanzionatoria ritenuta più efficace, fermo restando l'obbligo di criminalizzazione per le condotte più gravi (imposto dalla direttiva MAD II).

In particolare, dal combinato disposto del considerando n. 22 MAD II [211] e del considerando n. 72 MAR [212] emerge come scelta del legislatore eurounitario sia stata quella di prevedere un sistema a carattere flessibile in cui il singolo stato possa optare o per un sistema sanzionatorio duale, caratterizzato dalla duplice repressione e sul piano penale e sul piano amministrativo, ovvero punire la condotta illecita con il solo strumento del diritto penale.

Salvo i casi in cui il fatto venga commesso con "dolo" e nelle forme "più gravi" per i quali gli stati membri sono tenuti ad adottare le misure necessarie affinché la manipolazione di mercato costituisca reato (art. 5 MAD II), la condotta oggettiva di manipolazione viene descritta all' art. 12 MAR, in cui si elencano una serie di azioni che determinano una perturbazione nelle condizioni di fisiologico funzionamento del mercato.[213]

A un livello generale, si possono distinguere due tipologie di condotte: la manipolazione operativa (*trade based manipulation*) e la manipolazione informativa (*information based manipulation*).

La tipologia di "manipolazione operativa" si integra tutte le volte in cui venga avviata un'operazione, inoltrato un ordine di compravendita o qualsiasi altra condotta che "*invii, o è probabile che invii, segnali falsi o fuorvianti in merito all'offerta, alla domanda o al*

---

[211] "*Gli obblighi previsti nella presente direttiva di prevedere negli ordinamenti nazionali pene per le persone fisiche e sanzioni per le persone giuridiche non esonerano gli Stati membri dall'obbligo di contemplare in tali ordinamenti nazionali sanzioni amministrative e altre misure per le violazioni previste nel regolamento (UE) n. 596/2014, salvo che gli Stati membri non abbiano deciso, conformemente al regolamento (UE) n. 596/2014, di prevedere per tali violazioni unicamente sanzioni penali nel loro ordinamento nazionale"* (Considerando n. 22 MAD II).

[212] "*Anche se nulla osta a che gli Stati membri stabiliscano regole per sanzioni amministrative oltre che sanzioni penali per le stesse infrazioni, gli Stati membri non dovrebbero essere tenuti a stabilire regole in materia di sanzioni amministrative riguardanti violazioni del presente regolamento che sono già soggette al diritto penale nazionale, entro il 3 luglio 2016. Conformemente al diritto nazionale, gli Stati membri non sono tenuti a imporre sanzioni sia amministrative che penali per lo stesso reato, ma possono farlo se il loro diritto nazionale lo consente" (*Considerando *n.* 72 MAR*).*

[213] ANNUNZIATA, F. (2023). La disciplina del mercato dei capitali. Giappichelli, Torino, p. 493.

prezzo di uno strumento finanziario” (art. 12 lett. a, punto n.1 MAR) ovvero che “*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*” (art. 12 lett. a punto n. 2 MAR).

Entrambe le condotte in questione influiscono sul processo di formazione dei prezzi. Tuttavia, è necessario notare come nel primo caso, il successo della strategia faccia leva sulla reazione della condotta sugli altri partecipanti alle contrattazioni, i quali potrebbero essere ingannati dai segnali “falsi o fuorvianti” trasmessi dall'agire del manipolatore. Nel secondo caso, invece, il successo della strategia deriva direttamente dalla forza del manipolatore, il quale, indipendentemente dalla reazione degli altri partecipanti al mercato, “fissa” il prezzo a un livello anormale o artificiale.[214]

La manipolazione “operativa”, secondo la visione del legislatore, non si esaurisce solamente nelle fattispecie sopraindicate. Invero, esiste una terza tipologia che si integra ogniqualvolta vi sia una “*conclusione di un'operazione, immissione di un ordine di compravendita o il compimento di qualsiasi altra attività o condotta che, attraverso l'uso di artifizi o di ogni altro tipo di inganno o espediente, incide sul prezzo di uno o più strumenti finanziari o di un contratto a pronti su merci collegato*” (art. 12 lett. b MAR).

In tale ipotesi, a differenza delle precedenti, affinché sia configurato l'illecito è necessario un ulteriore elemento, consistente nella condotta attiva dell' “*artificio , raggiro o altro espediente*”.[215] La formulazione in questione, come è stato fatto notare, [216] non si distingue per la sua chiarezza e precisione in quanto non vi è alcuna chiarificazione circa il modo in cui i prezzi degli strumenti finanziari debbano essere effettivamente

[214] CONSULICH, F., MAUGERI, M., MILIA, C., POLI, T. N., & TROVATORE, G. (2023). AI and market abuse: Do the laws of robotics apply to financial trading? (CONSOB Legal Research Papers, *Quaderni Giuridici* No. 29), p. 54.
[215] Artifizi e raggiri sono condotte che portano il soggetto che li subisce a crearsi una falsa rappresentazione della realtà: l'artificio, più precisamente, opera sulla realtà esterna, e si ha quando viene fatta apparire come vera una situazione che non trova riscontro nei fatti; il raggiro, invece, agisce sulla psiche della vittima, che viene convinta mediante ragionamenti dalle false premesse che una situazione sia in un tal modo, quando ciò non è vero.
[216] Si veda nota 214, p. 55.

influenzati, il che porta a considerala come una norma di chiusura alla quale fare ricorso in casi eccezionali.[217]

Integra, altresì, manipolazione operativa anche la condotta consistente nell'*"invio 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"*(art. 12 par. 2 lett. c)).

Accanto all'ipotesi della manipolazione operativa, il MAR prevede una seconda tipologia di manipolazione, a carattere informativo (la c.d. "manipolazione informativa"). In questa ipotesi ad essere sanzionata è la condotta di chi "*diffonde informazioni, tramite i mezzi di informazione, compreso Internet, o tramite ogni altro mezzo, che forniscano, o siano idonei a fornire, segnali falsi o fuorvianti in merito all'offerta, alla domanda o al prezzo di uno strumento finanziario, o che consentano, o è probabile che consentano, di fissare il prezzo di mercato di uno o più strumenti finanziari a un livello anormale o artificiale, compresa la diffusione di voci, quando la persona che ha proceduto alla diffusione sapeva, o avrebbe dovuto sapere, che le informazioni erano false o fuorvianti"* (art. 12 par. 1 lett. c).

Occorre preliminarmente notare come, a differenza del MAR, la manipolazione informativa risulti essere diversa sotto il profilo penalistico. A tal riguardo, la MAD II richiede, come ulteriore elemento, che la condotta consegua un "*vantaggio o profitto per*

[217] La norma non è accompagnata da indicatori nell'allegato I del Reg. (UE) MAR e nell'allegato II del Reg. delegato (UE) 2016/522.

colui che ha divulgato le informazioni ovvero per altri" configurandosi così un reato punibile a titolo di dolo *specifico.*[218]

Per quanto riguarda la formulazione contenuta nel MAR, invece, tale elemento soggettivo non figura, ma si richiede la mera conoscenza o conoscibilità del soggetto manipolatore circa la falsità o il carattere fuorviante della notizia.

Nonostante la formulazione adottata dal legislatore in relazione alla definizione di "*information based manipulation",* contenuta nel MAR non sia delle più felici, la condotta ha come presupposto la "diffusione di informazioni"; tali informazioni (e non già i mezzi di informazione) devono avere, affinché si configuri l'illecito, l'effetto di fornire (o l' idoneità a fornire) segnali *falsi* o *fuorvianti* in merito alla domanda, offerta o prezzo strumento finanziario, ovvero consentano di fissare il prezzo di mercato a un livello anormale o artificiale.

L'assenza di un dolo specifico nella norma in esame permette, quindi, di assoggettare a sanzione tutte quelle condotte in cui la diffusione ha ad oggetto dichiarazioni non veritiere tali da produrre effetti distorsivi sui mercati, indipendentemente da una finalità specifica del soggetto agente e da una sua condotta successiva. [219]

In ultima analisi, è opportuno evidenziare come il legislatore europeo abbia individuato una zona di *safe harbour* all'art. 13 del Reg. UE n. 596/2014 (MAR) rubricato "prassi di mercato ammesse", in cui i *traders* possono ripararsi dall'accusa di aver realizzato condotte illecite. L'operatività di tale norma è tuttavia limitata alle condotte individuate all' art. 12 par. 1 lett *a);* in tali ipotesi il divieto di cui all'articolo 15 non trova applica "*a condizione che la persona che avvii un'operazione ovvero collochi un ordine di compravendita, stabilisca che tale operazione, ordine o condotta sono giustificati da legittimi motivi e sono conformi a una pratica di mercato ammessa".*

In linea con il Considerando 42 del presente regolamento,[220] affinché sia esclusa la fattispecie di manipolazione, il singolo dovrà dunque dimostrare i due requisiti cumulativi

[218] Art. 5 par. 2, lett. *c*, MAD II.
[219] In questo senso, anche la merà finalità *ioci causa* è passibile di sanzione amministrativa.
[220] Il considerando 42 MAR stabilisce che: "*Fatte salve la finalità del presente regolamento e le sue disposizioni direttamente applicabili, una persona che compie operazioni o inoltra ordini di compravendita che possano essere configurati come manipolazione del mercato può essere in grado di dimostrare che le*

consistenti nella presenza di motivazioni legittime (poste alla base della condotta) e nella conformità della medesima rispetto alle prassi ammesse, con queste ultime intendendosi l'insieme dei comportamenti preventivamente approvati dalla Autorità nazionale di settore competente in materia (per l' Italia la Consob).

2.4 LA NORMATIVA ITALIANA: TESTO UNICO FINANZIARIO

Il legislatore italiano con la legge 18 aprile 2005, n. 62, denominata Testo Unico Finanziario (d'ora innanzi TUF), [221] in attuazione della Direttiva 2003/6/CE (MAD I) ha introdotto la fattispecie di manipolazione di mercato agli articoli 185 e 187-*ter* TUF. Configurando la condotta sia come delitto (art. 185 TUF) sia come illecito amministrativo (art. 187-*ter* TUF) è stato deciso di adottare, sin dall'origine, un sistema a "doppio binario" entro cui perseguire tutte le condotte illecite. [222] In seguito, con il d.lgs. n. 107 del 2018, tali disposizioni sono state aggiornate ed adeguate al nuovo quadro europeo delineato dal MAR e dalla MAD II.

Da una parte l'art. 187-*ter* TUF punisce, salvo quando il fatto costituisca reato, con la sanzione amministrativa "*chiunque violi il divieto contenuto nell' art. 15 del Reg. UE 596/2014*" (divieto di manipolazione di mercato). Senza procedere a una definizione "autoctona", il legislatore rinvia dunque alla disciplina europea per l'identificazione delle condotte che integrano l'illecito amministrativo.

Dall'altra, con l'art. 185 TUF il legislatore definisce autonomamente una condotta che, se integrata nei suoi elementi oggettivi e soggettivi, costituisce un delitto e, quindi, punibile con la sanzione penale. La norma sancisce: "*Chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, è punito (…)*".

---

sue motivazioni per compiere tali operazioni o inoltrare tali ordini erano legittime, e che dette operazioni e ordini erano conformi alle prassi ammesse sul mercato in questione".

[221] Legge 18 aprile 2005, n. 62, recante "Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee – Legge comunitaria 2004". (GURI n. 96 del 27 aprile 2005).

[222] CUCCHIARA, M. F. (2017). Market abuse e doppio binario sanzionatorio: L'applicazione dei criteri elaborati dalla Grande Camera EDU al caso in cui il processo penale sia definito con sentenza di patteggiamento. *Giurisprudenza Penale*, 2017(5), p. 2.

Analizzando la norma si evincono i seguenti elementi che connotano la fattispecie. Innanzitutto, si identifica come bene protetto dall'articolo il "regolare funzionamento dei mercati"; soggetto attivo della condotta può essere "chiunque", configurandosi così un reato "comune". La condotta tipica consiste nella "*diffusione di notizie false*" (la c.d. manipolazione "informativa") ovvero "*operazioni simulate o altri artifizi*" (c.d. manipolazione operativa). In tal modo il legislatore nazionale si è in larga misura coordinato con le tipologie di condotte descritte dall'art. 12 MAR, creandosi così una sovrapponibilità delle fattispecie oggettive. [223] Per quanto attiene all'elemento soggettivo, non è richiesto il dolo specifico (la volontà di conseguire un profitto) ma solo un dolo generico, compreso quello eventuale, in tal modo ampliando il novero di condotte sanzionabili.

Esaminando le due condotte come sopra descritte, si evince altresì quanto segue. Per quanto concerne la manipolazione informativa, questa viene integrata quando la divulgazione ha ad oggetto, indipendentemente dai mezzi impiegati, una notizia contraddistinta come "falsa" per tale intendendosi una che contiene dati presentati come reali ma che sono difformi dal vero. [224] Inoltre, il legislatore non fornisce indicazioni sul contenuto della medesima, venendo così in rilevo ogni notizia, qualunque sia la sua fonte o contenuto, purché rivolta verso un pubblico indifferenziato. [225]

Per quanto attiene all'elemento soggettivo, come è stato poc' anzi sottolineato, non si richiede un fine specifico di profitto ma risulta sufficiente la sola rappresentazione e volizione del fatto tipico di reato.[226]

---

[223] SEMINARA, S. (2022). Diritto penale commerciale. Vol. 3: Il diritto penale del mercato mobiliare. Giappichelli, Torino, p. 119, il quale sul punto rileva che le condotte riportate nell'articolo 12 del MAR possono essere sovrapposte con la formula, più generale, dell'art. 185 "chiunque *diffonde notizie false o pone in essere operazioni simulate o altri artifizi"*.

[224] Sulla possibilità di ricondurre entro la previsione normativa anche le notizie "esagerate" e "tendenziose" toglie ogni dubbio la Corte costituzionale che ha ritenuto le "*notizie false, esagerate o tendenziose*" come una "*forma di endiadi con cui il legislatore si è proposto di abbracciare ogni specie di notizie che, in qualche modo rappresentano la realtà in modo alterato*" in proposito: Corte costituzionale, 8 marzo 1962, n. 19.

[225] Sul punto si veda AMATI, L. (2012). Abusi di mercato e sistema penale. Giappichelli, Torino, p. 183. *("Occorre innanzitutto precisare come per "diffusione" vada intesa qualsiasi genere di comunicazione scritta od orale trasmessa con qualsiasi mezzo (stampa, radio, televisione, internet), purché «rivolta a un numero indeterminato di persone o almeno ad una cerchia considerevole di persone").*

[226] Sul punto è opportuno rilevare come vi sia una idiosincrasia con l'art. 5 par. 2 della direttiva 2014/57/UE (MAD II) che richiede espressamente che ne derivi un "vantaggio o profitto per colui che ha divulgato le informazioni ovvero per altri".

In relazione alla manipolazione operativa, la caratteristica distintiva risiede in condotte finalizzate a creare movimenti fittizi di mercato che inducono effetti imitativi nel pubblico (operazioni simulate o altri artifizi). [227] Il disvalore è quindi incentrato sulle modalità o tempistiche dell'esecuzione, indipendentemente dal raggiungimento di un risultato o dalla condotta successiva del soggetto agente.

Sia la manipolazione informativa che operativa, affinché siano qualificate come fattispecie punibile penalmente devono essere "*concretamente idonee a provocare una sensibile alterazione del prezzo*". Con tale formulazione, si ritiene pacificamente che il legislatore abbia voluto identificare una fattispecie di reato a "pericolo concreto" in cui è compito del giudice accertare l'effettiva e concreta messa in pericolo del bene giuridico tutelato mediante un giudizio *ex ante* riconducibile alla prognosi postuma.[228]

È necessario sottolineare come ai fini della configurazione del reato non sia necessaria la realizzazione dell'evento (l'alterazione sensibile dei prezzi) ma basti che dalla condotta derivi il pericolo concreto che l'evento suddetto possa verificarsi: sotto questo punto di vista, il reato di cui all'art. 185 TUF è definibile allora come un reato di "mera condotta".

Infine, la condotta dolosa dell'agente deve essere idonea a provocare una alterazione "*sensibile*" dei prezzi degli strumenti finanziari. L'aggettivo "*sensibile*" assume qui una veste fondamentale, in quanto funge da "filtro" selettivo dei fatti penalmente rilevanti. [229] Tuttavia, tale elemento sembra apparire significativamente astratto e indeterminato dovendosi attendere l'apporto della giurisprudenza affinché siano configurati i relativi parametri.

In sintesi, alla luce dell'analisi sino ad ora delineata, si può ragionevolmente concludere che il legislatore abbia optato per un duplice ordine di sanzioni (penali o amministrative).

---

[227] SEMINARA, S. (2022). Diritto penale commerciale. Vol. 3: Il diritto penale del mercato mobiliare. Giappichelli, Torino, p. 104.

[228] Da ult. la Cass., sez. V, 1 febbraio 2022, n 3555, afferma che "*la concreta idoneità deve essere accertata sulla base del criterio della prognosi postuma, volto a verificare se – con riferimento all' intera platea degli investitori ed alla complessiva situazione di mercato, nonchè valutando le iniziative sollecitatorie della Consob a norma dell' art. 114 t.u.t. - gli effetti dei fatti comunicativi, prevedibili in concreto ed ex ante, quali conseguenza della condotta del soggetto agente, siano stati potenzialmente idonei a provocare una sensibile alterazione del prezzo di mercato del titolo, rispetto a quello determinato in un corretto processo di formazione dello stesso*".

[229] ANNUNZIATA, F. (2023). La disciplina del mercato dei capitali. Giappichelli, Torino, p. 492.

In particolare, qualora il singolo abbia agito con dolo [230] e la sua condotta (informativa o operativa) sia stata idonea a provocare una alterazione dei prezzi e qualora tale alterazione sia "sensibile", solo allora il soggetto potrebbe essere responsabile penalmente. In relazione invece all'art. 187 *ter* TUF, perché si configuri un illecito amministrativo accorre, sotto un punto di vista soggettivo anche la colpa del soggetto agente, mentre, da un punto di vista oggettivo, pur rimanendo l'esigenza di stabilire se la condotta sia stata concretamente idonea ad alterare i prezzi,[231] non si richiede la "sensibilità" di tale alterazione.

2.5 IL SISTEMA ATTUATIVO

In merito all'applicazione della disciplina dettata dal TUF, il legislatore italiano ha demandato la competenza alla repressione di eventuali illeciti all'autorità amministrativa (la Consob) e a quella giudiziaria. In particolare, alla Consob è attribuita la competenza in ordine all'accertamento e alla sanzione degli illeciti amministrativi, mentre al giudice penale spetta la cognizione delle fattispecie di reato, normalmente connotate dal dolo e da un più elevato disvalore.

Sul punto, l'articolo 187-*duodecies* TUF afferma che "*il procedimento amministrativo di accertamento e il procedimento di opposizione di cui all'articolo 187 septies non possono essere sospesi per la pendenza del procedimento penale avente ad oggetto i medesimi fatti o fatti dal cui accertamento dipende la relativa definizione*". In tale norma viene sancita l'autonomia dei procedimenti penale e amministrativo e, in tal modo, il principio del doppio binario trova un pieno riconoscimento.

È opportuno altresì ricordare la previsione di cui all'art. 187-decies TUF che pone in capo alle autorità competenti un obbligo di reciproca collaborazione: il pubblico ministero è tenuto a trasmettere senza ritardo la notizia di reato al Presidente della Consob. Allo stesso tempo, quest'ultimo è obbligato a trasmettere al p.m. la documentazione raccolta nello

[230] L'art. 185 TUF non richiede una particolare forma di dolo, potendo, pertanto, essere integrati sia i casi dolo intenzionale, diretto ed eventuale.
[231] SEMINARA, S. (2022). Diritto penale commerciale. Vol. 3: Il diritto penale del mercato mobiliare. Giappichelli, Torino, p. 121.

svolgimento delle indagini nel caso in cui emergano elementi che facciano presumere l'esistenza di un reato.

Infine, la Consob è titolare di una serie di poteri di indagine ex art. 187- *octies* TUF che possono essere esercitati in maniera autonoma (ad es. richiesta di notizie, dati, documenti e registrazioni relative a conversazioni telefoniche; audizioni personali; ispezioni) ovvero previa autorizzazione del pubblico ministero (ad es. sequestro beni a fini di confisca, perquisizioni, acquisizioni di tabulati telefonici). Inoltre, il comma 6 del 187- *octies* TUF investe la Consob di ulteriori poteri cautelari consistenti nella cessazione temporanea o permanente di qualunque pratica o condotta e nell'adozione di tutte le misure necessarie per la corretta informazione del pubblico.

2.6 IL DOPPIO BINARIO E IL NE BIS IN IDEM

L'analisi sino ad ora svolta mette in luce una caratteristica fondamentale connessa alla disciplina sugli abusi di mercato: quella del doppio binario sanzionatorio penale e amministrativo.

Di fronte alla sussistenza di un duplice impianto di sanzioni, sorge la questione circa il rispetto del principio del *ne bis in idem,* in base al quale *"nessuno può essere perseguito o condannato penalmente dalla giurisdizione dello Stato per un reato per il quale è già stato assolto o condannato a seguito di una sentenza definitiva conformemente alla legge e alla procedura penale di tale stato"* (art. 4 comma 1 del Protocollo n. 7 alla Convenzione per la salvaguardia dei diritti dell' uomo e delle libertà fondamentali).[232]

Nel sistema pre-MAR l'eventuale cumulo tra sanzioni penali e amministrative era regolato dall' art. 187-*terdecies* TUF*,* il quale limitava l'esazione della pena pecuniaria inflitta alla persona fisica o alla persona giuridica, alla parte eccedente quella già riscossa a seguito di condanna per illecito amministrativo.[233]

[232] L' art. 50 della Carta dei diritti fondamentali dell'UE estende la portata di tale principio a tutti gli stati UE.
[233] Si veda nt. 229.

Tale previsione, tuttavia, non è stata ritenuta sufficiente ad evitare la condanna per l'Italia, da parte della Corte Europea dei Diritti dell'Uomo (d'ora in poi CEDU) con la fondamentale sentenza del 4 marzo 2014 *Grande Stevens vs Italia.*[234] La CEDU ha infatti accertato la violazione dell'art. 4 protocollo n. 7 Convenzione EDU (rubricato "diritto di non essere giudicato o punito due volte"). La Corte, rinvenendo nelle sanzioni amministrative irrogabili dalla Consob in materia di abusi di mercato una natura penale, [235] aveva posto un divieto all'operatività del cumulo sancito dal TUF, operante nel caso in cui una medesima condotta venisse sanzionata sia dalla Consob, sia in sede penale. [236]

A distanza di pochi anni, la CEDU ha mutato il proprio orientamento e, pronunciandosi in materia tributaria, ha ammesso la duplicazione dei procedimenti laddove sussista tra essi una connessione "*in time and substance*".[237] In altre parole, la Corte ha ritenuto che ogniqualvolta i due procedimenti siano tra loro sufficientemente coordinati nel tempo e nella sostanza (ovvero perseguano fini complementari, risultino prevedibili per l'interessato, vengano integrati nella raccolta e valutazione della prova e risultino vicini temporalmente) essi debbano essere reputati come parti di un unico sistema sanzionatorio e non una duplicazione vietata del medesimo fatto.[238]

Nel 2018 è intervenuta la Corte di Giustizia Europea che nella sentenza *Garlsson* ha stabilito la non contrarietà del doppio binario con i principi del Trattato, purché le sanzioni complessivamente applicate risultino non sproporzionate. [239] In particolare, con tale pronuncia la Corte ha affermato infatti che *"l'art. 50 della Carta dei diritti fondamentali dell' UE deve essere interpretato nel senso che non osta a una normativa nazionale, che consente di celebrare un procedimento riguardante una sanzione amministrativa pecuniaria di natura penale nei confronti di una persona per condotte illecite che integrano una manipolazione di mercato, per le quali è già stata pronunciata una condanna penale definitiva a suo carico, nei limiti in cui tale condanna, tenuto conto del*

[234] Corte europea dei diritti dell'uomo, Grande Stevens e altri c. Italia, ricorsi nn. 18640/10, 18647/10, 18663/10 e 18698/10, sentenza 4 marzo 2014.
[235] Corte europea dei diritti dell'uomo, Engel e altri c. Paesi Bassi, ricorsi nn. 5100/71, 5101/71, 5102/71, 5354/72 e 5370/72, sentenza 8 giugno 1976.
[236] ANNUNZIATA, F. (2023). La disciplina del mercato dei capitali. Giappichelli, Torino, pp. 502–503.
[237] SEMINARA, S. (2022). Diritto penale commerciale. Vol. 3: Il diritto penale del mercato mobiliare. Giappichelli, Torino, p. 131.
[238] Corte europea dei diritti dell'uomo, A and B v. Norway, ricorsi nn. 24130/11 e 29758/11, sentenza 15 novembre 2016 (Grande Camera).
[239] ANNUNZIATA, F. (2023). La disciplina del mercato dei capitali. Giappichelli, Torino, p. 503.

danno causato alla società del reato commesso, sia idonea a reprimere tale reato in maniera efficace, proporzionata e dissuasiva". [240]

La Corte di Giustizia dell'Unione Europea ha quindi sostanzialmente avvallato l'interpretazione fatta dalla CEDU, non sposando l'idea di un *ne bis in idem* totale, ma ammettendo una risposta sanzionatoria combinata, con particolare risalto in particolare al principio della proporzionalità. Più precisamente, secondo la pronuncia adottata dalla Corte, è ammissibile, in presenza dei requisiti sopra indicati, un secondo giudizio in cui venga irrogata una sanzione amministrativa di natura sostanzialmente penale in relazione ad una medesima condotta, già giudicata nel corso di un precedente giudizio divenuto definitivo in sede penale.[241]

Sulla questione è intervenuta infine la Corte costituzionale con due sentenze: la prima è la pronuncia del 2 marzo 2018 n. 43 con cui la Corte si è adeguata ai principi enunciati dalla CEDU, stabilendo il divieto del *bis in idem* ogni volta in cui venga a mancare il legame temporale e materiale. [242]

La seconda è la sentenza n. 149 del 10 maggio 2022, [243] in materia di diritto di autore, in cui la Corte è intervenuta dichiarando incostituzionale l'art 649 c.p.p. (rubricato "Divieto di un secondo giudizio") [244] nella parte in cui non prevede che il giudice non pronunci il proscioglimento, o il non luogo a procedere verso un imputato per un delitto in materia di diritto di autore che, in relazione allo stesso fatto, sia già stato sottoposto a un procedimento amministrativo di natura punitiva, ormai definitivamente concluso.

La sentenza in questione assume una portata decisiva: il principio del *ne bis in idem* trova una sua concretizzazione non più solo nella prospettiva di una seconda pena (dimensione sostanziale), ma anche in quella antecedente, consistente nella possibilità di subire un secondo processo (dimensione processuale).

---

[240] Corte di giustizia dell'Unione europea, Garlsson Real Estate SA e a. c. Commissione Nazionale per le Società e la Borsa (CONSOB), causa C-537/16, sentenza 20 marzo 2018.
[241] ANNUNZIATA, F. (2023). La disciplina del mercato dei capitali. Giappichelli, Torino, p. 503.
[242] Corte costituzionale, sentenza 2 marzo 2018, n. 43.
[243] Corte costituzionale, sentenza 10 maggio 2022, n. 149.
[244] Codice di procedura penale, art. 649, recante "Divieto di un secondo giudizio".

LE CONDOTTE MANIPOLATIVE TRAMITE HIGH FREQUENCY TRADING

2.7 PREMESSA TECNICO GIURIDICA

Una volta illustrata la normativa nazionale ed eurounitaria in tema di manipolazioni di mercato, si rende necessario un approfondimento tecnico ed operativo tramite il quale analizzare le principali strategie di negoziazione realizzabili tramite *trading* ad alta frequenza e rispetto alle quali si sollevano dubbi di legittimità.

Più nel dettaglio, nella disamina a seguire verrà svolto un approfondimento su quali siano le principali condotte identificate come manipolazioni di mercato nel contesto dell'*high frequency trading*. In virtù di ciò, l'analisi si soffermerà su quelle fattispecie definibili come "tradizionali" in quanto perpetrate tramite modelli di *trading* deterministici, in cui la macchina agisce in base a regole predefinite e codificate all' interno dei programmi. [245] Si tratta, in questo ultimo caso, di forme di manipolazione tipicamente realizzate con modelli ad alta frequenza, che in ragione della loro velocità di esecuzione, consentono di realizzare in modo efficace tali strategie illecite.

Tuttavia, con lo sviluppo del *machine learning* i possibili scenari manipolatori si ampliano ed è quindi possibile ipotizzare nuove forme di rischi per la sicurezza e tenuta dei mercati. A tal riguardo, sarà effettuata una disamina che illustrerà in modo sistematico entro quali modi e forme i sistemi più avanzati si intersechino con l'ambito dei mercati finanziari.

2.8 HFT E FORME DI MANIPOLAZIONE TRADIZIONALI

Le principali forme di manipolazione di mercato realizzate tramite HFT sono *spoofing*, *layering*, *quote stuffing* e *momentum ignition* e nel prosieguo della disamina verranno dettagliatamente analizzate. Rispetto a tali forme, comune denominatore è la componente umana, la quale risulta essere predominante in ragione del fatto che la strategia abusiva è "iscritta" nel DNA della macchina stessa.

---

[245] DI MICHELE, M. (2024). Intelligenza artificiale. Etica, rischi e opportunità di una tecnologia rivoluzionaria. Diarkos, Roma, p. 22.

2.8.1 SPOOFING e LAYERING

Una delle tecniche di manipolazione più comuni perpetrata dai sistemi algoritmici ad alta frequenza è quella che prende il nome di *spoofing* (in italiano: "ordini civetta") e di cui il *layering* (o "stratificazione di ordini") costituisce una specifica sottocategoria.

Questa pratica è tutt'altro che inusuale sui mercati. Episodi di manipolazione di questo genere sono stati registrati sia durante il ben noto *Flash Crash* del 2010 [246] sia in momenti successivi [247] e il numero risulta essere in costante aumento.[248]

A livello operativo, le modalità di realizzazione dello *spoofing* e *layering* risultano piuttosto simili, pertanto non si rende necessaria una specifica distinzione tra le due condotte.[249] In entrambi i casi, infatti, il soggetto agente (tendenzialmente un algortimo HFT) inserisce una elevata quantità di ordini al limite [250] in uno dei due lati del *book* di negoziazione (lato acquisti ovvero lato vendite), con l'obiettivo di rimuoverli prima dell'esecuzione. [251]

---

[246] Il caso riguarda un *trader* londinese di nome Navinder Sarao che durante il Flash Crash aveva utilizzato un programma automatico per inserire ingenti ordini di vendita sui *futures*, modificarli e spostarli migliaia di volte e poi cancellarli prima dell'esecuzione, creando una fittizia pressione di vendita che ha contribuito agli squilibri di mercato. Sul punto si veda: WANG, X., & WELLMAN, M. P. (2017). Spoofing the limit order book: An agent-based model. In Das, S., Durfee, E. H., Larson, K., & Winikoff, M. (Eds.), Proceedings of the 16th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2017), p. 651.

[247] Un caso emblematico concernente lo *spoofing* ha coinvolto anche la nota banca statunitense JP Morgan che nel 2020 è stata obbligata a versare in virtù di un accordo transattivo record, 920,2 milioni di dollari per condotte di *spoofing* sui mercati dei metalli e dei futures sui Treasury. Sul punto: DO, B. L., & PUTNIŅŠ, T. J. (2023). Detecting layering and spoofing in markets (Working Paper), p. 1.; VALSANIA, M. (2020). JpMorgan, multa da 920 milioni $ per manipolazione dei futures su oro e argento. *Il Sole 24 Ore*. https://www.ilsole24ore.com/art/jpmorgan-multa-920-milioni-%24-manipolazione-futures-oro-e-argento-ADUskSs (Consultato il 22 settembre 2025).

[248] LADLEY, D., ORIOL, N., & VERYZHENKO, I. (2024). High-frequency spoofing, market fairness and regulation (Preprint submitted to Elsevier). p. 1 (finding that: "*most of the sanctions handed out in the period 2020-2022 were for insider trading and order-based manipulations. The same report observes that spoofing and layering are widespread types of market abuse, accounting for 38% of total fines all over the world.*").

[249] DO, B. L., & PUTNIŅŠ, T. J. (2023). Detecting layering and spoofing in markets (Working paper), p. 2 (finding that: "*some regulators use the two terms interchangeably as both refer to the use of non-bona-fide orders to deceive other traders about supply and demand*").

[250] Gli ordini al limite (o *limit orders*) permettono di aggiungere profondità al *book* di negoziazione, diversamente da un ordine al meglio (o *market order*) che aggredisce immediatamente la liquidità disponibile nei vari livelli del *book*.

[251] LIN, B. L. D., & PUTNIŅŠ, T. J. (2015). The new market manipulation. Charles Sturt University, School of Accounting and Finance, p. 1289 (finding that:" *allows the initiating party to distort the ordinary price discovery in the marketplace by placing orders with no intention of ever executing them and merely for the purpose of manipulating honest participants in the marketplace*").

Se l'inserimento avviene nel lato *bid* (il lato in cui figurano gli ordini al limite di acquisto), scopo dell'agente sarà quello di aumentare la profondità del *book* lato acquisti, spingendo gli altri investitori a inserire a loro volta ordini di acquisto, portati a credere ad una apparente spirale rialzista. In questo modo il prezzo subirà un incremento e, solo a questo punto, il manipolatore inserirà un ordine "reale" di vendita sull'altro lato del *book*, sfruttando un prezzo maggiorato e cancellando gli ordini "civetta" precedentemente inseriti.[252]

Al contrario, se l'inserimento degli ordini al limite dovesse avvenire sul lato *ask* (in cui sono presenti gli ordini al limite di vendita), l'agente inserirà numerosi ordini al limite di vendita con lo scopo di simulare una spirale ribassista e indurre così gli altri partecipanti a liquidare le proprie posizioni, per il timore di veder crollare il prezzo del titolo. Una volta che vi sia stato l'effettivo calo del prezzo, l'agente inserirà allora un ordine "reale" di acquisto sul lato *bid* con lo scopo di comprare lo strumento a un valore minore, cancellando allo stesso tempo gli ordini di vendita fittizi.[253]

Entrambe le condotte di *spoofing* e *layering,* come sopra analizzate, sembrano idonee a integrare una condotta manipolativa riconducibile alle due distinte fattispecie previste all'art. 12 MAR, par. 1 lett. *a)* sub. ii e par. 1 lett. *b),* per le motivazioni che seguono.

In particolare, il manipolatore, mediante l'immissione di ordini su uno dei lati del *book* e la loro successiva cancellazione fa credere erroneamente che il mercato stia assumendo una precisa direzione. Tale condotta risulta pertanto riconducibile alla fattispecie di cui all'art. 12, par. 1, lett. a), in quanto idonea a "*fornire indicazioni false o fuorvianti circa l'offerta, la domanda o il prezzo dello strumento finanziario"* (sub ii). Inoltre, ove la reazione degli investitori — tratti in inganno dall'apparente profondità del *book* — si traduca in un mutamento del prezzo, ipotesi verosimile, la medesima strategia

---

252 Sul punto anche*:* PUTNIŅŠ, T. J. (2020). An overview of market manipulation. In C. Alexander & D. Cumming (Eds.), Corruption and fraud in financial markets: Malpractice, misconduct and manipulation. John Wiley & Sons, p. 17 (finding that*:" typical layering cycle is as follows: (i) place a small sell order at or near the best ask price, (ii) layer the bid side of the order book until the market moves up and the small sell order executes, (iii) cancel the layering bid orders and repeat the above steps in the opposite direction").*

253 MARK, G. (2019). Spoofing and layering. *The Journal of Corporation Law*, 45(2), p. 104 (finding that: "*A basic spoofing scheme involves a trader entering a large order on one side of the market that the trader intends to cancel prior to execution and contemporaneously entering one or more small orders on the other side that the trader intends to fill. The large order creates an illusion of market depth and generates a response from other market participants that together benefit the trader's small positions").*

può essere riconducibile all'art. 12, par. 1, lett. b), in quanto consente di fissare il prezzo di mercato a un "*livello di prezzo anormale o artificiale*".

Le condotte di *spoofing* e *layering*, tenuto conto di quanto sino ad ora è stato precisato, sono assoggettabili, pertanto, nell'ordinamento italiano allo strumento della sanzione amministrativa in quanto violano il divieto di cui all'art. 187 *ter* TUF (rubricato "manipolazione di mercato") che rinvia, come noto, alle previsioni contenute nel regolamento 596/2014 (MAR).

Infine, per quanto attiene il trattamento sanzionatorio penale, sarà applicabile l'art. 185 TUF (rubricato "manipolazione di mercato") laddove venga accertato l'elemento soggettivo del dolo e la condotta sia concretamente idonea a provocare una sensibile alterazione del prezzo dello strumento finanziario.

2.8.2 QUOTE STUFFING

Una seconda tecnica impiegata in modo diffuso dagli HFT prende il nome di *quote stuffing* (sovraccarico di quotazioni). Tale strategia manipolatoria, per le modalità entro cui si svolge, presenta notevoli affinità con gli attacchi DoS e DDoS ai sistemi informatici, la cui trattazione approfondita sarà oggetto del capitolo 3 concernente la *cybersecurity*.

La suddetta pratica si verifica quando un HFT riversa sul mercato una quantità massiccia di "traffico", consistente nell'immissione e contestuale cancellazione di migliaia di ordini a limite di prezzo, in modo da determinare un duplice rallentamento: quello della sede di negoziazione e quello degli altri sistemi di *trading,* che a differenza dell'HFT sono tenuti a processare un elevatissimo numero di informazioni, perdendo un notevole vantaggio temporale.[254]

Una volta raggiunto il duplice scopo di rallentare la capacità di elaborazione del sistema di negoziazione e di innalzare, di conseguenza, barriere all'ingresso per gli altri

---

[254] PUORRO, A. (2013). High frequency trading: Una panoramica (Banca d'Italia, Occasional Paper n. 198), p.21.

investitori, [255] l'HFT procederà poi a condurre "arbitraggi da latenza" sfruttando i ritardi dei *market partecipants.* [256]

Il *quote stuffing* si presenta quindi come una pratica manipolativa in cui, a differenza dello *spoofing*, obiettivo principale non è tanto quello di alterare i livelli di domanda o di offerta, quanto, quello di congestionare, ritardare e rallentare le piattaforme in modo tale da poter creare i presupposti per successive operazioni opportunistiche. [257]

La condotta, date le sue caratteristiche, è idonea a essere ricompresa nell'art. 12, par. 2, lett. c) MAR che in proposito recita: "*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: <u>interrompe o ritarda, o è probabile che interrompa o ritardi, il funzionamento del sistema di negoziazione della sede di negoziazione</u>*".

Pertanto, qualora venga accertato in concreto che la strategia abbia interrotto o ritardato, o fosse verosimilmente idonea a interrompere o ritardare, il regolare funzionamento del sistema di negoziazione, la stessa risulta riconducibile all'art. 12, par. 2, lett. c) MAR. Ne consegue la potenziale applicazione della sanzione amministrativa prevista dall'art. 187-ter TUF.

Allo stesso tempo, potrà trovare applicazione anche la sanzione di cui all'art. 185 TUF, qualora l'invio massivo e la contestuale cancellazione degli ordini siano ricostruibili come "altro artifizio" e risultino concretamente idonei, alla luce di dati di mercato, a

---

[255] DALKO, V., & WANG, M. H. (2020). High-frequency trading: Order-based innovation or manipulation? *Journal of Banking Regulation*, 21, p. 292 (finding that: "*purpose is to slow down the processing of the exchange and lift the entry barrier to other traders*").

[256] Si veda nota 254 p. 21.

[257] DÍAZ, D., & THEODOULIDIS, B. (2013). Financial markets monitoring and surveillance: A quote stuffing case study. In Proceedings of the 17th Panhellenic Conference on Informatics (pp. 51–58). IEEE. p. 4. (Finding that: "*Quote stuffing not only has the potential to confuse other market participants but also puts real pressure on trading systems since all the orders are processed as valid orders, thereby adding a significant workload to already heavily used systems. Crucially, increased workloads could create delays and lags in processing times that affect the way valid orders are processed. These delays have some very important consequences, one of which relates to the way trading information is disseminated and consolidated*").

determinare una "sensibile" alterazione dei prezzi, a condizione che ovviamente sia riscontrata una condotta dolosa dell'agente.

2.8.3 MOMENTUM IGNITION

La *momentum ignition* (ossia, "avvio della tendenza") è una tra le tecniche manipolative caratterizzate da maggior aggressività.

In tale ipotesi, il *trader* HFT, dopo aver costruito una certa posizione [258] (*long*, se acquista con lo scopo di rivendere a un prezzo più alto ovvero *short,* se vende per poi riacquistare a un prezzo più basso, guadagnando sulla differenza), inserisce numerosi ordini di acquisto o vendita allo scopo di generare l'apparenza di una tendenza o di un movimento direzionale di mercato, così da indurre altri operatori a reagire nella stessa direzione.[259] Una volta che il valore (inizialmente stabile) dello strumento finanziario subisce la variazione desiderata, il *trader* ad alta frequenza chiude la propria posizione *long* o *short* ottenendo così un profitto.[260]

La tecnica in questione si presta a rientrare all'interno della fattispecie descritta dall'art. 12 del MAR. In particolare, la *momentum ignition* è astrattamente riconducibile alla previsione di cui al paragrafo 2 lett. c) in cui si allude a "*inoltro di ordini in una sede di negoziazione, comprese le relative cancellazioni o modifiche (…) che crea o è probabile che crei, un segnale falso o fuorviante in merito all' offerta, alla domanda o al prezzo di uno strumento finanziario <u>in particolare emettendo ordini per avviare o intensificare una tendenza</u>*". Ricorrendo tale ipotesi, e una volta accertata in concreto l'attitudine manipolativa della condotta, potrà trovare applicazione il binario amministrativo per violazione del divieto di manipolazione (o tentata manipolazione) di mercato, con conseguente irrogazione della sanzione amministrativa ex art. 187-ter (TUF).

Allo stesso tempo, sul piano penale, la condotta potrà rientrare nell'art. 185 TUF qualora sia ricostruibile come "altro artifizio", risulti concretamente idonea a determinare una

---

[258] DALKO, V., & WANG, M. H. (2020). High-frequency trading: Order-based innovation or manipulation? *Journal of Banking Regulation*, 21. p. 293.
[259] A differenza dello *spoofing*, non è necessario che all'inserimento di un ordine segua la cancellazione del medesimo.
[260] Vedi nota 258.

alterazione sensibile del prezzo (o del processo di formazione del prezzo) e, infine, ne sia accertato il dolo in capo al soggetto agente.

2.9 INTELLIGENZA ARTIFICIALE E MANIPOLAZIONI DI MERCATO

L'attuale scenario si completa esaminando forme ulteriori di manipolazione in cui un sistema di *trading* ad alta frequenza dovesse essere dotato di un algoritmo *machine learning* al fine di indagare quali siano i contributi che l'AI possa concretamente apportare alle strategie manipolative precedentemente descritte.

In primo luogo, le tecniche di intelligenza artificiale possono essere implementate all'interno del sistema HFT al fine di ottimizzare le condotte illecite precedentemente descritte. In questo senso, considerando la tecnica dello *spoofing,* è facile intuire come un algoritmo di autoapprendimento possa essere impiegato per migliorare nel complesso l'intera strategia operativa. In un sistema ottimizzato con AI*,* ad esempio*,* la macchina stessa potrebbe suggerire il miglior momento per effettuare lo *spoofing*, gestire il *timing* di inserimento e cancellazione di ordini, nonché effettuare, mediante un algoritmo non supervisionato, una *cluster analysis* per ricercare titoli poco liquidi e con *book* poco profondi che meglio si segnalano a una strategia manipolativa. Come è stato inoltre segnalato, un sistema di AT o HFT potenziato con *machine learning* potrebbe trovare poi modalità nuove per aggirare gli stessi limiti OTR, [261] posti dalle sedi di negoziazione, con lo scopo di ridurre l'invio di ordini poi successivamente cancellati (*non bona fide orders*).[262]

Allo stesso modo, l'AI potrebbe essere impiegata per migliorare il *quote stuffing.* Si pensi*,* ad esempio, all'individuazione del numero esatto di messaggi da inviare al sistema di abbinamento ordini di una piattaforma di negoziazione al fine di congestionarlo e farlo

---

[261] Un OTR (*order-to-trade ratio*) è un indicatore che misura il rapporto tra il numero di ordini immessi (inclusi quelli modificati/cancellati) e il numero di ordini effettivamente eseguiti su un determinato strumento o in un determinato arco temporale. Sul punto si rinvia al paragrafo 1.6.2.

[262] AZZUTTI, A., RINGE, W.-G., & STIEHL, H. S. (2021). Machine learning, market manipulation and collusion on capital markets: Why the "black box" matters. *University of Pennsylvania Journal of International Law*, 43(1). p. 99, (finding that: "*AI could optimize those strategies that seek to deceive other market participants through fast submission and cancellation of orders, such as "spoofing." Significantly, order-based algorithmic strategies are somehow constrained by venues' rules limiting the "orders to transactions ratio" (OTR), aimed at disadvantaging non bona fide trading orders*").

collassare ovvero alla individuazione dei momenti più adatti nell'arco di una giornata di *trading* che meglio si prestano a porre in essere la strategia in questione.

Un algoritmo "intelligente" potrebbe essere sfruttato per fini illeciti anche per condurre manipolazioni *cross markets* e *cross assets*.[263] Si pensi, ad esempio, a una AI in grado di monitorare lo stesso strumento finanziario negoziato contemporaneamente su più sedi ovvero più strumenti finanziari tra loro correlati o collegati a un medesimo sottostante. In tali ipotesi l'algoritmo sarebbe in grado di coordinare in modo sincrono l'inserimento e la cancellazione di ordini e di ottimizzare la durata e sequenza temporale delle operazioni, sfruttando disallineamenti di prezzo e asimmetrie informative fra sedi di negoziazione.

Tuttavia, le possibilità che una AI venga impiegata per manipolare un mercato non si limitano alle sole *order based manipulations* ma possono estendersi anche a quelle a carattere informativo. Invero, grazie all'elevatissime capacità degli algoritmi nonché alla enorme diffusione dei *media technologies,* è facile ipotizzare anche manipolazioni di mercato volte a creare una "*mass misinformation*".[264]

In questo senso, un sistema di intelligenza artificiale generativa [265] potrebbe essere impiegato per creare *ex nihilo* comunicati stampa o documenti societari falsi, idonei a condizionare le scelte di investimento. Si pensi, ad esempio, alla diffusione di notizie e report di analisi fuorvianti che, grazie a modelli avanzati (come i *large language models*, LLM),[266] siano in grado di riprodurre pressoché perfettamente strutture linguistiche umane complesse, ingenerando così un elevato grado di fiducia nei lettori.

---

[263] *Ibidem.*

[264] LIN, T. C. W. (2017). The new market manipulation. *Emory Law Journal*, 66. p. 1292. (Finding that: "*Unscrupulous parties can now leverage the mechanisms of new media technology and new financial technology to disrupt and distort financial markets on an unprecedented scale by disseminating bad data, fake news, and faulty information into a marketplace that thrives on accurate information. This Article terms this new method of cybernetic market manipulation, "mass misinformation". With mass misinformation schemes, parties can manipulate the marketplace through fake regulatory filings, fictitious news reports, erroneous data, and hacking").*

[265] L'intelligenza artificiale generativa (IA generativa) è un tipo di IA che crea contenuti nuovi e originali (testo, immagini, musica, codice, video) imparando dai modelli presenti in enormi quantità di dati, invece di limitarsi a eseguire compiti predefiniti.

[266] I *large language models* (LLM) sono una categoria di modelli di *deep learning* addestrati su quantità immense di dati, che li rendono capaci di comprendere e generare linguaggio naturale e altri tipi di contenuti per svolgere un'ampia gamma di compiti. STRYKER, C. (s.d.). What are LLMs? IBM Think. https://www.ibm.com/think/topics/large-language-models (Consultato 26 novembre 2025).

Una ulteriore ipotesi di applicazione di AI generativa a fini manipolativi può essere poi quella consistente nella creazione di *deepfakes* tramite GANs,[267] ossia modelli di intelligenza artificiale impiegati per la produzione di contenuti visivi, quali immagini e video. Si pensi, ad esempio, al caso di un video nel quale l'amministratore di una società annunci una fusione con un'altra impresa, senza che tale operazione trovi alcun riscontro nella realtà, ma sia artificiosamente creata al solo fine di influenzare le aspettative del mercato.[268]

Infine, ulteriori ipotesi di manipolazione a carattere informativo possono riguardare l'impiego di sistemi AI per la creazione e la gestione automatizzata di migliaia di account, profili e bot. Questi ultimi potrebbero essere impiegati per diffondere notizie finanziarie fuorvianti o suggerire scelte di investimento errate a un'ampia platea di investitori[269] ovvero essere utilizzati per generare forme di *micro-targeting* informativo su base strettamente individuale. Si pensi, ad esempio, a campagne comunicative personalizzate rivolte ai piccoli investitori, in cui si suggerisce loro – tramite messaggi *ad hoc* sui *social network*– idee o strategie di investimento particolarmente rischiose.

In tutte le ipotesi sopra richiamate si potrebbe configurare una vera e propria manipolazione informativa, astrattamente riconducibile al parametro normativo di cui all'art. 12, par. 1, lett. c), del Regolamento (UE) n. 596/2014 (MAR), nonché all'art. 185 TUF.

---

[267] Una *generative adversarial network* (GAN) è un modello di *machine learning* progettato per generare dati realistici apprendendo i pattern a partire da dataset di addestramento esistenti, JOBIT VARUGHESE, *What is a GAN?*, IBM Think, s.d., disponibile su: https://www.ibm.com/think/topics/generative-adversarial-networks (ultimo accesso: 26 Novembre 2025).

[268] Sulla pericolosità insita dei deepfake si rimanda alla nota vicenda in cui un'impiegata di una società di Hong Kong ha partecipato a una videochiamata in cui, grazie a deepfake realistici, i truffatori hanno impersonato il CFO e altri dirigenti della società, chiedendole di effettuare trasferimenti "riservati". Convinta di parlare con i superiori reali, la donna ha disposto bonifici verso cinque conti bancari per un totale di circa 200 milioni di dollari scoprendo solo dopo, tramite contatto con la sede centrale, di essere stata vittima di una frode basata su intelligenza artificiale. MILMO, D. (2024). Company worker in Hong Kong pays out £20m in deepfake video call scam. The Guardian. https://www.theguardian.com/world/2024/feb/05/hong-kong-company-deepfake-video-conference-call-scam (Consultato 26 novembre 2025).

[269] BATHAEE, Y. (2018). The Artificial Intelligence Black Box and the Failure of Intent and Causation. *Harvard Journal of Law & Technology*, 31(2). p. 912.

L' autore ipotizza come un algoritmo di *deep learning* impari a coordinare l'attività di *trading* con la diffusione di notizie (retweet) in quanto addestrato su innumerevoli dati, tra i quali anche i social network sfruttando così l'impatto informativo sui prezzi ("*Interestingly, the system has learned to "retweet" news articles on Twitter and often does so before and after trades*").

Nel presente paragrafo sono state esaminate ipotesi in cui l'intelligenza artificiale è impiegata come "mero strumento" per il perseguimento di scopi illeciti, svolgendo una funzione di "supporto" ad una precisa strategia decisa dall' uomo *ab initio* (si parla, in tal caso, di *manipulations AI enanched*). Tuttavia, come è stato esaminato, i modelli più avanzati di AI, in particolare quelli basati su *deep reinforcement learning*, sono idonei a dar luogo a veri e propri "agenti" in grado di operare in modo autonomo sui mercati finanziari. Tali modelli sono addestrati secondo meccanismi di *trial and error*, ricevendo una ricompensa (*reward*) ogniqualvolta una determinata azione contribuisce ad aumentare il valore della funzione-obiettivo che sono chiamati ad adempiere. In questa prospettiva, diversi studi scientifici – ivi compresi documenti di fonte istituzionale [270] – mettono in guardia rispetto alla possibilità che un algoritmo di *reinforcement learning* possa apprendere autonomamente una strategia manipolativa come soluzione "ottimale" per raggiungere al meglio l'obiettivo di massimizzazione del profitto (in tal caso si parlerebbe di *autonomous AI-driven manipulation*). [271]

L'ipotesi non è meramente teorica: qualora un algoritmo di *deep reinforcement learning* venisse addestrato su un ampio set di dati storici contenente milioni di transazioni, ordini e cancellazioni, esso potrebbe, quantomeno in astratto, individuare nello *spoofing* [272]– così come in altre strategie, ad esempio volte a manipolare un indice o un *benchmark*[273] – una condotta idonea a adempiere correttamente il compito di ottimizzare la funzione assegnata. [274] Un tale scenario potrebbe verificarsi qualora al sistema venisse attribuita

[270] DUTCH AUTHORITY FOR THE FINANCIAL MARKETS. (2023). Machine learning in algorithmic trading: Application by Dutch proprietary trading firms and possible risks. pp. 15–16.
(Finding that: "*If the objective of a machine learning based trading algorithm is to optimize some objective (e.g., profit or price impact), then – if other trading algorithms would be susceptible to manipulation and the reinforcement learning algorithm could profit from doing so – there is no reason a priori to assume the trading algorithm will not learn negative trading behavior, or even to manipulate. The AFM notes that trading algorithms could learn to manipulate the market even if its developers don't want them to*").

[271] MIZUTA, T. (2020). Does an artificial intelligence perform market manipulation with its own discretion? A genetic algorithm learns in an artificial market simulation (arXiv Preprint No. arXiv:2005.10488).

[272] BYRD, D. (2022). Learning not to spoof. In ICAIF '22: 3rd ACM International Conference on AI in Finance (pp. 1–9). Association for Computing Machinery.

[273] SHEARER, M., RAUTERBERG, G., & WELLMAN, M. P. (2023). Learning to manipulate a financial benchmark. In ICAIF '23: 4th ACM International Conference on AI in Finance. Association for Computing Machinery, pp. 592–600.

[274] MARTÍNEZ-MIRANDA, E., MCBURNEY, P., & HOWARD, M. J. W. (2015). Learning unfair trading: A market manipulation analysis from the reinforcement learning perspective (arXiv Preprint No. arXiv:1511.00740).

una funzione obiettivo formulata in termini generici (ad es. «massimizza il profitto»): in tal caso, infatti, l'algoritmo, orientando il proprio comportamento sulla base di ciò che viene premiato o scoraggiato, potrebbe apprendere che una determinata condotta manipolativa sia idonea a massimizzare l'obiettivo assegnato e, proprio perché "ricompensata", finirebbe per reiterarla durante la fase di impiego operativo.

Questa ultima ipotesi apre scenari tanto stimolanti per il giurista quanto, almeno in parte, distopici per la società. Se un sistema di intelligenza artificiale fosse oggi in grado di apprendere autonomamente una strategia illecita di tipo *order-based*, nulla escluderebbe che esso possa attuare, se non adeguatamente controllato, condotte di manipolazione a carattere informativo, imparando, ad esempio, che la divulgazione di alcune notizie false o fuorvianti (ad es. tramite la condivisione di determinati *tweet*), accompagnata da una successiva strategia di *trading* sia potenzialmente idonea ad incrementare i profitti.

TRADING ALGORITMICO, INTELLIGENZA ARTIFICIALE E IMPLICAZIONI GIURIDICHE

2.10 PREMESSA

Una volta individuate le condotte manipolative che pongono rischi per la sicurezza del mercato dei capitali, occorre procedere preliminarmente alla disamina dell'assetto normativo vigente allo scopo di comprendere se esso sia sufficientemente adeguato a fronteggiare e reprimere tutte quelle forme di manipolazioni perpetrate tramite l'ausilio di sistemi algoritmici avanzati.

In particolare, occorrerà *in primis* verificare se le norme contenute nel MAR siano sufficientemente idonee a regolare anche quelle condotte illecite perpetrabili tramite algoritmi "intelligenti" ovvero necessitino di aggiornamenti o ripensamenti al fine di contenere ed includere anche i più recenti sviluppi tecnologici.

In secundis, occorrerà esaminare il profilo concernente l'attribuzione delle responsabilità derivanti da fatto illecito. In particolare, alla luce della sempre maggior autonomia operativa dei sistemi AI, risulta lecito domandarsi se, con riguardo ai sistemi di *high frequency trading* più evoluti, si assista o meno a una crisi delle tradizionali categorie di ascrizione della responsabilità derivante dall'illecito commesso.

2.11 BLACK BOX, MARKET ABUSE REGULATION E PROBLEMI ATTUATIVI

Una distinzione molto importante che deve essere tracciata tra algoritmi deterministici e algoritmi avanzati di autoapprendimento (*machine learning*) concerne il grado di comprensione e spiegabilità del modello in concreto adottato.

Con riferimento ai primi modelli, vale a dire gli algoritmi basati su logiche statiche e deterministiche, l'agire della macchina è interamente riconducibile a regole predefinite e pre-codificate dall' uomo. Da ciò ne deriva che, in linea di principio, sia sempre possibile ricostruire e ripercorrere la catena logica che ha portato la macchina a produrre un determinato *output* o ad assumere una determinata decisione.

Nel caso degli algoritmi di *machine learning* – e, in particolare, quelli basati su reti neurali profonde (*deep learning*) – la ricostruzione del percorso attraverso cui la macchina, a partire da determinati *inputs*, riesce a generare uno specifico *output*, risulta spesso essere altamente opaca e complessa.

La ragione di ciò risiede nel fatto che la rete neurale elabora gli *input* esterni attraverso numerosissimi strati di neuroni artificiali, ognuno dei quali esegue calcoli interni e restituisce il risultato allo strato successivo, sottoforma di una funzione di attivazione.[275] Poiché in tale processo viene coinvolto un numero assai elevato di neuroni, la decisione finale non è riconducibile a poche regole chiare e lineari, ma al risultato congiunto di moltissimi passaggi numerici, difficilmente traducibili in una spiegazione semplice e intuitiva per l'essere umano.[276] Quando quindi ci si riferisce al termine "*black box*" si allude ad algoritmi che si presentano come vere e proprie scatole nere, in cui comprendere come si sia generato un certo *output* risulta essere inspiegabile tanto per gli *stakeholders* quanto per gli stessi *data scientists* più esperti.[277] In altre parole, l'uomo è in grado di conoscere un certo risultato, ma non è altrettanto in grado di comprendere fino in fondo come e perché la macchina sia arrivata ad esso, e di spiegarne il procedimento interno di ragionamento.

[275] A tal proposito sia consentito il rimando a quanto descritto nel par. 1.9 per il funzionamento di una rete neurale.
[276] LIPTON, Z. C. (2017). The mythos of model interpretability. *Communications of the ACM*, 61(10), pp. 36–43.
[277] KOSINSKI, M. (2024). Che cos'è la black box AI? IBM Think. https://www.ibm.com/it-it/think/topics/black-box-ai (Consultato 28 novembre 2025).

Una tale opacità pone evidenti problemi non solo di *trasparenza* [278] e *spiegabilità* [279] [280] ma anche di *affidabilità* per la presenza di possibili errori (o *bias)* nascosti negli algoritmi [281] e di conseguenza risulta inficiata la stessa *prevedibilità* dell'*output* atteso.

Il fatto che gli algoritmi più avanzati siano caratterizzati da un marcato grado di "opacità" acquista una rilevanza alla luce della formulazione di talune norme contenute all'interno del MAR, in quanto il tenore letterale di esse può condurre a significativi problemi di applicazione e attuazione.

Innanzitutto, un primo profilo di problematicità si pone in relazione alla fattispecie descritta all'interno dell'art. 12, par. 1, lett. a) MAR. Come è stato illustrato in precedenza, il legislatore europeo, tramite tale disposizione, ha deciso di creare una zona di "*safe harbour*" in cui escludere dall'ambito della manipolazione di mercato tutte quelle operazioni che, pur rientrando astrattamente nella descrizione oggettiva della fattispecie, risultino sorrette da ragioni legittime e siano conformi alle prassi di mercato ammesse.

In altre parole, qualora venisse dimostrato che alla base della strategia vi siano motivazioni legittime e che l'operazione realizzata rispecchi una prassi di mercato ammessa (n.d.r. dall' autorità nazionale), la condotta non verrà a qualificarsi come un "illecito di manipolazione". [282]

---

[278] "Trasparenza" può essere intesa come una conoscenza "oggettiva" della sequenza di tutti i passaggi svolti dall' algoritmo (conoscenza del "*quid"*).
[279] "Spiegabilità" può essere intesa come conoscenza "soggettiva" nel senso di conoscere i criteri che guidano tutti i passaggi svolti dall' algoritmo (conoscenza del "*quia*").
[280] AZZUTTI, A., RINGE, W.-G., & STIEHL, H. S. (2021). Machine learning, market manipulation, and collusion on capital markets: Why the "black box" matters. *University of Pennsylvania Journal of International Law*, 43(1). p. 90. (Finding that: "*The "black box" problem is where both the developers and users of AI may not fully understand and explain why and how their algorithms have generated a particular output given specific data input. The "black box" problem is often framed in terms of issues of AI "transparency," "explainability," and trustworthiness," especially for ML-based decision-making in critical domains related to human life, which underpins the problem of "auditability" and "accountability" in cases of AI wrongdoing*.").
[281] PEDRESCHI, D., GIANNOTTI, F., GUIDOTTI, R., MONREALE, A., RUGGIERI, S., & TURINI, F. (2019). Meaningful explanations of black box ai decision systems. Proceedings of the AAAI conference on artificial intelligence, 33(01), pp. 9780.
(finding that: "*This is problematic not only for lack of transparency, but also for possible biases inherited by the algorithms from human prejudices and collection artifacts hidden in the training data*").
[282] Sul punto anche il considerando n. 8 del Reg. del. 522/2016 afferma: "*alcuni esempi di prassi possono essere considerati legittimi se, ad esempio, una persona che compie operazioni o inoltra ordini di compravendita che possono configurarsi come una manipolazione del mercato è in grado di dimostrare che le motivazioni alla base di tali operazioni o tali ordini erano legittime, e che le operazioni e gli ordini in questione erano conformi alle prassi ammesse sul mercato considerato".*

Una simile disposizione risulta, tuttavia, essere difficilmente applicabile in tutti quei casi in cui venisse applicato un algoritmo di *machine learning* (ML) opaco in quanto l'assenza di una chiara ricostruibilità del processo decisionale della macchina inibirebbe la possibilità di dimostrare che tale condotta sia stata giustificata da legittimi motivi. [283]

Una ulteriore disposizione che potrebbe presentare limiti alla sua concreta applicazione è quella contenuta nell'art. 12, par. 1, lett. c) MAR, in cui si viene a definire la condotta di manipolazione informativa. Affinché sia configurato l'illecito, il legislatore richiede che «*la persona che ha proceduto alla diffusione sapeva, o avrebbe dovuto sapere, che le informazioni erano false o fuorvianti*».

Una simile formulazione è chiaramente costruita avendo in mente un autore umano, rispetto al quale è astrattamente possibile accertare l'elemento soggettivo. Tuttavia, laddove si sia in presenza di un sistema di intelligenza artificiale che abbia autonomamente appreso durante l'addestramento che la diffusione di notizie sui *social media* o il *retweet* di determinati contenuti, accompagnata ad una successiva strategia di *trading,* sia idonea ad incrementare la funzione di massimizzazione del profitto, l'opacità e la non chiarezza del processo decisionale della macchina renderebbero estremamente difficile dimostrare che l'uomo sapesse o potesse sapere che le notizie diffuse dall'algoritmo erano in realtà false o fuorvianti. In altre parole, dato che la norma richiede la conoscenza o almeno la conoscibilità *ex ante* del carattere falso o fuorviante delle informazioni diffuse, l'impiego di sistemi di AI, dotati di elevata autonomia e opacità, rende particolarmente complesso muovere un rimprovero soggettivo: il fatto che l'operatore umano non conosca fino in fondo come il sistema ragioni internamente *(c.d. black box)* rende assai difficile prevedere *ex ante* il comportamento dell'algoritmo in una specifica situazione e, di conseguenza, dimostrare che l'essere umano sapesse o avrebbe dovuto prevedere la condotta illecita generata dalla macchina.

---

[283] CONSULICH, F., MAUGERI, M., MILIA, C., POLI, T. N., & TROVATORE, G. (2023). AI and market abuse: Do the laws of robotics apply to financial trading? (CONSOB Legal Research Papers, *Quaderni Giuridici* No. 29), pp. 55-56.

Una tale problematica non si limiterebbe ai soli casi di manipolazione informativa. Invero, essa si estenderebbe anche ai casi di manipolazione operativa, in quanto, sebbene non espresso testualmente, si richiede sempre la dimostrazione dell'elemento soggettivo in capo all'agente.

Come è agevole notare, l'impianto normativo contenuto all' interno del MAR sembra non tenere adeguatamente in considerazione le problematiche che emergono dall'impiego di algoritmi di *machine learning.* Se le fattispecie descritte all'art. 12 (MAR) sono idonee a far fronte a sistemi deterministici o statici, rimane in parte irrisolta la questione concernente le eventuali manipolazioni perpetrate dagli algoritmi più evoluti, posto che, a mio avviso, le formulazioni in questione non devono essere interpretate in senso letterale come un divieto all' impiego di strumenti "intelligenti" nelle strategie di *trading*.[284]

In conclusione, sebbene l'impiego dell'AI nel settore del *trading* ad alta frequenza non crei, almeno per il momento, il rischio di nuove forme di manipolazione tali da ricadere al di fuori del perimetro normativo, la legislazione contenuta nel MAR potrebbe affrontare un deficit di attuazione (*enforcement)* in relazione a tutte quelle manipolazioni che dovessero essere attuate mediante sistemi basati sul *machine learning*.

Da ciò ne consegue che il MAR è un insieme di norme che è stato concepito ed elaborato per fronteggiare fenomeni manipolativi prettamente umani, secondo schemi decisionali lineari e prevedibili, e che, pur mantenendo una struttura tecnologicamente neutra, mostra possibili limiti sul piano dell'attuazione. La forte opacità algoritmica dei modelli avanzati può, pertanto, rappresentare un ostacolo effettivo all'attuazione delle norme del regolamento ed un incentivo a compiere strategie opportunistiche illecite, mettendo a dura prova la "adeguatezza" della normativa.

---

[284] Sul punto si rimanda alla medesima considerazione effettuata nel par. 1.10 a proposito dell'ammissibilità di sistemi intelligenti nei mercati finanziari.

2.11.1 IL REG. EU n. 1689/2024: AI ACT

Il Regolamento EU n. 1689/2024 denominato *Artificial Intelligence Act* (d'ora in avanti AI ACT) [285] costituisce il primo esempio di normativa sull'intelligenza artificiale a livello globale. In questa sede, il medesimo sarà esaminato per verificare se le norme in esso contenute possano costituire un *corpus* normativo di riferimento anche per l'ipotesi di *trading* basato su algoritmi avanzati.

Nello specifico, il regolamento si pone come obiettivo quello di "*promuovere la diffusione di una AI antropocentrica e affidabile, garantendo un livello elevato della salute, della sicurezza e dei diritti fondamentali compresi dalla Carta dei diritti fondamentali dell'Unione Europea, compresi la democrazia, lo stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi IA nell' Unione, e promuovendo l'innovazione*" (Art. 1 AI act).

L'intento alla base del regolamento è quello di garantire un'intelligenza artificiale *affidabile* e *sicura*, attraverso una regolazione generale e non distinta per settori regolamentati. [286] A ciò si aggiunge, come fine ultimo, quello della protezione dei *diritti fondamentali dell'individuo,* così da definire un modello di riferimento per un utilizzo responsabile a livello globale. [287]

A tale scopo, il legislatore ha adottato un approccio basato sul rischio (*risk based approach*) in ragione del quale i sistemi AI vengono classificati in base al loro livello di pericolosità e al loro effetto negativo sulla società.

Le categorie individuate dal regolamento sono rispettivamente: sistemi AI che presentano rischi "inaccettabili" e che pertanto non potranno mai essere immessi nel mercato europeo

[285] Regolamento (UE) 13 giugno 2024, 2024/1689 del Parlamento europeo e del Consiglio, recante "Regolamento che stabilisce norme armonizzate sull'intelligenza artificiale e recante modifica dei regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e delle direttive 2014/90/UE e (UE) 2016/797" (AI Act), in GUUE L 202 del 12 luglio 2024, pp. 1–278.
[286] CORASANITI, G. (2025). Sicurezza informatica e intelligenza artificiale: Rischio e resilienza nello spazio giuridico europeo. Giappichelli, Torino. p. 59.
[287] ZICCARDI, G. (2025). Una lettura dell'Artificial Intelligence Act: norme, etica, adempimenti, attuazione. In F. Basile et al. (a cura di), Intelligenza artificiale. Diritto, giustizia, economia ed etica. Giappichelli, Torino. p. 24.

(art. 5 Reg. denominato "pratiche AI vietate");[288] sistemi "ad alto rischio" (artt. 6 e 7 Reg.) che sono sottoposti a stringenti obblighi (artt. 8-15 Reg.) e sistemi a rischio "limitato" per i quali sono previsti solamente taluni obblighi di trasparenza (art. 50 Reg.). Ulteriori disposizioni sono inoltre previste in riferimento ai modelli di AI *per finalità generali*, le c.d. GPAI (art 51 ss. Reg.).[289]

Per la configurazione giuridica dell'AI, fondamentale è la definizione che viene fornita dal regolamento all' art. 3, punto n. 1, che recita: "con *sistema AI si intende un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*". [290]

Dalla citata disposizione si ricava come la definizione di "sistema AI" poggi su quattro elementi chiave: il primo è quello della "automatizzazione", con cui si intende che il funzionamento del sistema debba avvenire per il mezzo di una macchina. [291] Il secondo elemento consiste nel fatto che macchina deve possedere una "capacità inferenziale", [292] ovvero una capacità di dedurre *input* ed elaborare *output* (ad es. previsioni, contenuti, decisioni) che possono influenzare ambienti fisici e virtuali. Il terzo elemento è la presenza di "diversi livelli di autonomia", che vanno dal mero supporto alle decisioni fino alla totale automazione, con una variabile presenza dell'intervento umano. [293] Infine, il quarto elemento risiede nella "continua adattabilità del sistema" che permette ad esso di evolversi e mutare il proprio comportamento. [294]

---

[288] L'art. 5 del Regolamento (UE) 2024/1689 individua un nucleo di pratiche di IA vietate, tra cui sistemi manipolativi, forme di social scoring e applicazioni intrusive di identificazione e categorizzazione biometrica.
[289] I modelli di IA per finalità generali sono tutti quei modelli "in grado di svolgere con competenza un'ampia gamma di compiti distinti" (art. 3, n. 63). Un esempio è quello rappresentato oggi da Chatgpt.
[290] Art. 3 AI ACT.
[291] Considerando 12 AI ACT.
[292] A questo proposito, vale la pena citare il considerando n. 12 nella parte in cui afferma "*Una caratteristica fondamentale dei sistemi di IA è la loro capacità inferenziale. Tale capacità inferenziale si riferisce al processo di ottenimento degli output, quali previsioni, contenuti, raccomandazioni o decisioni, che possono influenzare gli ambienti fisici e virtuali e alla capacità dei sistemi di IA di ricavare modelli o algoritmi, o entrambi, da input o dati*".
[293] Considerando 12 AI ACT.
[294] Considerando 12 AI ACT.

In base a quanto sopra esplicitato si può ragionevolmente concludere che non possano essere ricondotti alla definizione di cui all'art. 3 Reg. tutti quei sistemi AT o HFT "tradizionali" [295] ovvero fondati su algoritmi statico-meccanici, *rule based*, in cui la componente di autonomia è praticamente assente. [296]

Nelle suddette ipotesi, infatti, l*'output* discende dall'esecuzione di regole predefinite senza che vi sia una capacità inferenziale né un significativo margine di autonomia operativa o di adattamento della macchina.

Tuttavia, laddove il sistema di AT/HFT faccia ricorso a tecniche di *machine learning*, esso può rientrare perfettamente nella nozione di 'sistema di IA', poiché in tal caso esso integrerebbe le quattro le caratteristiche necessarie di cui all'art. 3, punto n. 1 AI ACT.

L'AI ACT trova, pertanto, una applicazione nel caso di AT o HFT basati su algoritmi di *machine learning*, ma contrariamente a quanto si potrebbe attendere, un simile sistema non rientra nella categoria "*high risk system*".

All'interno di tale categoria rientrano tutti quei sistemi individuati all'art. 6 par. 1 dell'AI ACT per i quali il legislatore ha predisposto numerosi e specifici requisiti onde garantirne un uso sicuro ed affidabile. In particolare, secondo il legislatore si considera "ad alto rischio" un sistema che è destinato ad essere utilizzato come "componente di sicurezza di un prodotto" (ovvero è esso stesso un "prodotto") disciplinato da una direttiva di armonizzazione dell'UE indicata nell'allegato n. I del presente regolamento e il medesimo è soggetto a una valutazione di conformità da parte di terzi, ai fini dell'immissione sul mercato o della messa in servizio.

All'art. 6 par. 2 del regolamento si aggiunge che sono inoltre considerati "ad alto rischio" tutti quei sistemi rientranti nelle categorie elencate nell' allegato III dell'AI ACT. In tale elenco figurano tutti quei settori ("critici") in cui il legislatore presume che l'impiego di un sistema AI arrechi un pregiudizio significativo di danno per la salute, la sicurezza o i

---

[295] ANNUNZIATA, F. (2023). Artificial intelligence and the regulation of market abuse: A European perspective. Edward Elgar Publishing, Cheltenham (UK)–Northampton, MA (USA). p. 75.

[296] A tal proposito si rinvia al considerando n. 12 dell'AI ACT che espressamente afferma: "*Inoltre, la definizione* (di "sistema AI", n.d.r.) *dovrebbe essere basata sulle principali caratteristiche dei sistemi di IA, che la distinguono dai tradizionali sistemi software o dagli approcci di programmazione più semplici, e non dovrebbe riguardare i sistemi basati sulle regole definite unicamente da persone fisiche per eseguire operazioni in modo automatico".*

diritti fondamentali. Ne consegue che, se il sistema, pur formalmente incluso all'interno dell'allegato III, non presenti in concreto un livello di rischio significativo, non verrà a considerato ad "alto rischio".[297]

Alla luce di queste considerazioni, è possibile concludere come, laddove un sistema di *trading* algoritmico faccia ricorso a tecniche di *machine learning*, esso non rientri in alcuna delle due categorie "ad alto rischio" delineate dall'art. 6 del reg. AI ACT per i seguenti motivi. In primo luogo, esso non integrerebbe l'ipotesi di cui all' art. 6 par. 1, poiché non è un componente di sicurezza ovvero un prodotto disciplinato dalla normativa di armonizzazione UE. In secondo luogo, la categoria del *trading* algoritmico non si figura nemmeno tra quelle elencate nell'Allegato n. III. [298]

Le ragioni di questa esclusione risiedono, come è stato motivato, [299] nel fatto che una applicazione finanziaria di intelligenza artificiale comporta un rischio puramente economico e, pertanto, esso è tale da ricadere al di fuori del perimetro regolatorio dell'AI ACT (incentrato, come noto, sulla tutela dei diritti fondamentali).[300]

L'impossibilità di ricondurre il *trading* algoritmico (o ad alta frequenza) svolto per il tramite di algoritmi avanzati di *machine learning* nella sfera dei "sistemi ad alto rischio" impedisce quindi l'applicazione del regime giuridico speciale previsto per sistemi *high risk*, in cui sono contenuti diversi obblighi in tema di AI *transparency*. [301] Di seguito verranno analizzate le principali disposizioni contenenti obblighi previsti dal legislatore all'interno del regolamento.

---

[297] Art. 6, par. 3 AI ACT.

[298] Cfr. EUROPEAN COMMISSION. (2021). Commission staff working document impact assessment accompanying the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts (SWD (2021) 84 final). European Commission, Brussels. n. 237, p. 51. (In tale atto si afferma come il *trading* algoritmico risulti essere già estensivamente regolato dal pacchetto MiFID II).

[299] SCIARRONE ALIBRANDI, A., RABITTI, M., & SCHNEIDER, G. (2023). The European AI Act's impact on financial markets: From governance to co-regulation (Working paper). p. 18. (finding that: "*a third category of financial AI systems do not, as such, appear to have any impact onto customers' fundamental rights, but involve only purely economic interests of either customers or financial operators*").

[300] AZZUTTI, A. (2024). AI governance and algorithmic trading: Some regulatory insights from the EU AI Act. *Banking & Finance Law Review*, 41(1), p. 27.

[301] Considerando n. 72 AI ACT "*Per rispondere alle preoccupazioni relative all'opacità e alla complessità di determinati sistemi di IA e aiutare i deployer ad adempiere ai loro obblighi a norma del presente regolamento, è opportuno imporre la trasparenza per i sistemi di IA ad alto rischio prima che siano immessi sul mercato o messi in servizio*."

In primo luogo, una serie di obblighi è prevista all'art. 10 dell'AI ACT (denominato "Dati e governance dei dati") nei confronti del "fornitore dei sistemi AI", quest'ultimo definito come "*qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che sviluppa un sistema AI (o che fa sviluppare un sistema AI) e immette tale sistema sul mercato o lo mette in servizio, con il proprio nome o marchio, a titolo oneroso o gratuito*".[302]

In tale articolo il legislatore ha inteso stabilire come i set di dati di addestramento, convalida e prova per i modelli di IA debbano soddisfare appositi criteri e standard di qualità, ogniqualvolta questi vengano utilizzati. [303]

A tal proposito, si prevede come tali *set* di dati debbano essere soggetti a pratiche di *governance* e gestione dei dati calibrate sulla "finalità prevista" del sistema ad alto rischio. [304] Inoltre, viene stabilito come i *dataset* debbano essere *pertinenti*, *sufficientemente rappresentativi*, e nella misura possibile, *privi da errori* e *completi* in relazione alla finalità prevista.[305] Essi devono altresì tenere conto delle caratteristiche e degli elementi particolari dello specifico ambiente geografico, contestuale, comportamentale o funzionale all'interno del quale il sistema verrà utilizzato. [306]

Sul punto occorre ricordare che non manchino considerazioni critiche in merito, [307] soprattutto in relazione al fatto che non essendo possibile stabilire aprioristicamente la quantità di dati necessaria per addestrare un modello, le clausole di "completezza" e "rappresentatività" risultano essere non verificabili in concreto. Inoltre, altrettanto vaga è la formula "*esenti da errori*": posto che un sistema AI può sbagliare anche con dati corretti, come distinguere gli errori "nei dati" dagli errori "del modello" ai fini di una successiva rimproverabilità?

Ulteriori obblighi sono previsti all'art. 11 Reg. tale disposizione prevede che i fornitori siano tenuti a redigere una documentazione tecnica prima dell'immissione sul mercato o

[302] Art. 3 punto n. 3 AI ACT.
[303] Art 10 par. 1. AI ACT.
[304] Art. 10 par. 2 AI ACT.
[305] Art. 10 par. 3 AI ACT.
[306] Art. 10 par. 4 AI ACT.
[307] LIZA, F. F. (2022). Challenges of enforcing regulations in Artificial Intelligence Act — Analyzing quantity requirement in data and data governance. CEUR Workshop Proceedings, 3221, pp. 1–10.

della messa in servizio del sistema. [308] In tale documentazione, l'allegato IV del presente regolamento prescrive che siano riportate una serie di informazioni, tra cui: le specifiche di progettazione del sistema, la logica generale del sistema di IA e degli algoritmi, la descrizione dell'*output* atteso e la qualità dell'*output* del sistema (par. 2 lett. *b*); una descrizione dell'architettura del sistema, che illustri come i componenti *software* dipendano tra loro, si alimentino reciprocamente e si integrino nel processo complessivo, nonché le risorse computazionali impiegate per sviluppo, addestramento, test e convalida del sistema di IA (par. 2, lett. *c*); i requisiti sui dati, documentati tramite schede tecniche che descrivano metodologie e tecniche di addestramento e i dataset impiegati, con indicazione di origine, ambito e caratteristiche principali, nonché delle modalità di acquisizione e selezione dei dati, delle procedure di etichettatura (es. apprendimento supervisionato) e delle tecniche di pulizia (es. rilevamento di *outlier*) (par. 2 lett. *d*).

Ulteriori obblighi sono poi quelli previsti all'art. 12 dell'AI ACT in cui si stabilisce che i sistemi AI devono consentire la registrazione automatica degli eventi (altresì detta "*log*") per l'intera durata del ciclo di vita del sistema, onde poterne garantire un livello di tracciabilità del funzionamento. [309] In tal modo il "log" potrebbe rendersi utile a ricostruire *ex post* come e perché il sistema abbia operato rispetto alla finalità prevista.

Obblighi aggiuntivi discendono inoltre dall'art. 13 dell'AI ACT (denominato "Trasparenza e fornitura di informazioni ai *deployers"*). In particolare, i fornitori sono tenuti a progettare e sviluppare i sistemi *high risk* in modo tale da garantire che il funzionamento sia sufficientemente trasparente in modo da permettere ai *deployers* [310] di interpretare *l'output* del sistema (la c.d. "trasparenza *by design*").[311] A tale proposito, i suddetti sistemi sono accompagnati da istruzioni tecniche per l'uso contenenti una serie di informazioni riguardanti le caratteristiche, le capacità e i limiti delle prestazioni, tra cui: le capacità e caratteristiche del sistema onde spiegarne l'*output* (art. 13 AI ACT par. 3, lett. *b*, *iv)*); le opportune specifiche per i dati di *input* o qualsiasi altra informazione pertinente in termini di set di dati di addestramento, convalida e prova (art 13 AI ACT

[308] Art. 11 par. 1 e par. 2 AI ACT.
[309] Art. 12, par. 2 AI ACT.
[310] «Deployer»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale. (Art. 3 AI ACT).
[311] Art. 13 par. 1 AI ACT.

par. 3, lett. *b*, *vi)*); le informazioni che consentano al *deployer* di interpretare l'*output* del sistema IA ad alto rischio e di usarlo in modo opportuno (art 13 AI ACT par. 2, lett. *b*, *vii)*).

E' opportuno sottolineare come la differenza tra l'art. 11 reg. (documentazione tecnica), prima menzionato, e l'art. 13 reg. del medesimo regolamento (trasparenza e fornitura di informazioni ai *deployers*) riguardi principalmente il destinatario dell' informazione: le autorità nazionali competenti affinché queste valutino la conformità dei sistemi rispetto ai requisiti del regolamento, nel primo caso, e i *deployers*, nel secondo, affinché questi ultimi siano messi nelle condizioni di "comprendere" come e perché sia stato generato un certo *output*.

Infine, una ultima serie di previsioni è contenuta nell' art. 14 dell'AI ACT (denominato "Sorveglianza umana") in cui si afferma come i sistemi ad alto rischio debbano essere progettati e sviluppati al fine di poter essere efficacemente "supervisionati" da persone fisiche durante il periodo in cui essi sono in uso. In ragione di ciò, si prevede che il sistema debba essere fornito ai *deployers* in modo tale che le persone fisiche alle quali è affidata la sorveglianza abbiano la possibilità di comprendere le capacità e i limiti del sistema ovvero di essere in grado di monitorare debitamente il funzionamento (art. 14 par. 4, lett. *a)* e di interpretare correttamente l'output (art. 14 par. 4, lett. *c)*).[312]

2.11.2 LA LEGGE n. 132/2025: LEGGE AI

Il Governo italiano ha dedicato da tempo grande attenzione allo sviluppo dell'Intelligenza Artificiale e nel novembre 2021 ha pubblicato il "Programma Strategico Intelligenza Artificiale 2022-2024"; [313] tuttavia, a causa dell'incredibile e dirompente sviluppo dei sistemi AI, tale programma si è dimostrato presto obsoleto ed inadeguato. A fronte di questa circostanza, nel luglio del 2024, il Dipartimento per la trasformazione digitale, di

[312] Art. 14, par. 4 AI ACT.
[313] GOVERNO ITALIANO. (2021). Programma strategico per l'intelligenza artificiale 2022–2024. Ministero dell'Università e della Ricerca; Ministero dello Sviluppo Economico; Ministro per l'Innovazione tecnologica e la Transizione Digitale.

concerto con l'Agenzia per l'Italia Digitale (AGID) ha adottato un nuovo piano strategico, aggiornato e denominato "Strategia Italiana per l'Intelligenza Artificiale 2024-2026". [314]

Sulla base di tale atto di indirizzo politico-strategico, che definisce obiettivi**,** priorità e principi della politica nazionale sull'IA, il 10 ottobre 2025 è entrata in vigore la legge 23 settembre 2025, n. 132 recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale" (di seguito denominata Legge AI),[315] con l'obiettivo di introdurre un quadro normativo che, nel rispetto dei principi dell'AI ACT*,* tenga conto delle specificità del sistema giuridico italiano e delle esigenze del tessuto produttivo. [316]

La legge in parola si compone di 28 articoli distribuiti in sei Capi.

Fondamentale è l'articolo 1, in cui si enunciano l'"oggetto" che la legge intende disciplinare (ovvero la ricerca, la sperimentazione, lo sviluppo, l'adozione e l'applicazione di sistemi e modelli di IA)[317] nonché gli "obiettivi" che il legislatore intende perseguire (ovvero la *promozione di un uso corretto, trasparente e responsabile, in una dimensione antropocentrica dell'AI*, ma anche la *vigilanza sui rischi economici, sociali e giuridici* nonché *l'impatto sui diritti fondamentali* che da questa ne derivano).

Al fine di evitare problemi di coordinamento, la legge specifica testualmente che le disposizioni in essa contenute *si interpretano e si applicano conformemente al Reg. UE 2024/1689* (AI ACT).[318] In tal modo viene quindi ribadita la preminenza della normativa europea sulla legge italiana, confermando altresì l'intenzione del legislatore di disciplinare i tratti tipici della realtà economico-sociale nazionale.

Un riferimento merita anche l'articolo 3 della Legge AI, che esplicita i principi che devono essere seguiti in tutte le attività che hanno ad oggetto l'intelligenza artificiale. In particolare, viene affermato come "tutte le attività relative all'IA" [319] debbano rispettare,

---

[314] AGENZIA PER L'ITALIA DIGITALE (AgID). (2024). Strategia italiana per l'intelligenza artificiale 2024–2026.

[315] Legge 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale". (GURI n. 223 del 25 settembre 2025).

[316] TADDEI ELMI, G., CONTALDO, A., CAVACEPPI, C., & MARCHIAFAVA, S. (Eds.). (2025). Intelligenza artificiale: Legge 23 settembre 2025, n. 132. Il nuovo scenario giuridico italiano. Pacini Giuridica, xvii.

[317] L'art. 2 lett. A) rinvia all' art. 3, punto 1) dell'AI Act per la definizione di sistema AI.

[318] Art. 1 co. 2 Legge IA.

[319] Le "attività relative all'IA" comprendono le fasi di: ricerca, sperimentazione, sviluppo, adozione, applicazione ed utilizzo.

in primo luogo, *i diritti fondamentali e le libertà previste dalla costituzione e dal diritto UE*, e, in secondo luogo, i principi quali *trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità*. [320] Viene inoltre specificato come la fase di "sviluppo" dei sistemi e modelli di intelligenza artificiale debba avvenire su dati e tramite processi in cui devono essere garantite e vigilate la *correttezza, l'attendibilità, la sicurezza, la qualità, l'appropriatezza e la trasparenza, secondo il principio di proporzionalità*.[321]

In relazione all' oggetto del presente studio, l'articolo 16 della legge 132 è tra le disposizioni più rilevanti. In particolare, la norma affida al Governo il compito di *disciplinare dati, algoritmi e metodi matematici utilizzati per addestrare i sistemi di intelligenza artificiale.* La delega, senza duplicare o riscrivere l'AI ACT, riempie di contenuto nazionale gli spazi che l'ordinamento dell'Unione lascia aperti al fine di rafforzare la tutela dei diritti individuali. [322] In questa prospettiva, l'articolo consente al Governo, in primo luogo, di *selezionare i casi* in cui si ritiene "necessaria" una disciplina specifica per dati, algoritmi e metodi usati per l'addestramento, e in secondo luogo, *di definire obblighi e diritti* secondo un approccio basato sui processi (di addestramento, n.d.r.) e sul rischio, al fine di incrementare i livelli di trasparenza, tracciabilità e controllabilità. [323] In altre parole, la norma è di fondamentale importanza in quanto anziché guardare agli "outputs" del sistema AI, mira a regolare i presupposti del suo funzionamento, ossia dati, algoritmi e metodi matematici. Nell'esercizio di questa delega, il Governo sarà tenuto a recepire la classificazione europea per livelli di rischio (allineandosi così alla tassonomia dell'AI ACT dei sistemi) intensificando la disciplina laddove l'incidenza sui diritti fondamentali e sicurezza sia maggiore, in una logica di "attuazione verticale" del Reg. UE 1689/2024.[324]

[320] Art. 3 comma 1.
[321] Art. 3 comma 2.
[322] TADDEI ELMI, G., CONTALDO, A., CAVACEPPI, C., & MARCHIAFAVA, S. (Eds.). (2025). Intelligenza artificiale: Legge 23 settembre 2025, n. 132. Il nuovo scenario giuridico italiano. Pacini Giuridica. p. 132.
[323] *Ibidem.*
[324] Dato che il *trading* algoritmico non viene considerato come categoria ad alto rischio, è logico dedurre che i decreti legislativi che il Governo sarà chiamato ad adottare non potranno intervenire nell'ottica di aumentare la trasparenza e spiegabili di sistemi IA impiegati per le negoziazioni finanziarie.

Un'altra disposizione rilevante all'interno della Legge AI è quella contenuta all'art. 24, rubricato "Deleghe al Governo in materia di intelligenza artificiale". Nello specifico, il Legislatore, ha previsto una ulteriore delega, rispetto a quella già contenuta nel precedente art. 20, con la quale esorta il Governo *ad adottare entro 12 mesi uno o più decreti legislativi per l'adeguamento della normativa nazionale al regolamento (UE) 2024/1689 (AI ACT)* allo scopo di garantire la conformità ai requisiti europei e colmare eventuali lacune.

Il contenuto della delega è molto ampio e, per quello che interessa l'oggetto della presente analisi, è centrale l'art. 24 comma 3 che delega il governo "*ad adottare uno o più decreti legislativi per adeguare e specificare la disciplina dei casi di realizzazione e di impiego di illeciti di sistemi di intelligenza artificiale"*. Al fine di realizzare ciò, il Governo dovrà attenersi a una serie di principi e criteri direttivi, quali, ad esempio, l'introduzione di misure di prevenzione ed inibizione, e la precisazione dei criteri di responsabilità civile e penale.[325]

Sul solco tracciato dall'articolo 24 Legge AI, si inserisce il fondamentale articolo 26 che modifica alcune disposizioni al Codice penale al fine di sanzionare usi distorti dell'AI in una logica *ex post* e non già di regolazione *ex ante,* tipica dell'AI ACT.[326] Per quanto attiene il presente studio, l'articolo 26 modifica anche l'art. 185 TUF (rubricato "manipolazione di mercato") introducendo al comma 1 una circostanza aggravante speciale che trova applicazione in tutti quei casi in cui *il fatto dovesse essere commesso mediante l'impiego di sistemi di intelligenza artificiale.*

L' intervento normativo si giustifica per la maggior capacità di manipolazione dell'IA sia nella dimensione "operativa" che "informativa" e può considerarsi un riconoscimento da parte del legislatore della pericolosità tecnologica e dell'effetto sistemico che l'AI può avere nei mercati finanziari.[327]

---

[325] Art. 3 comma 5 Legge IA.

[326] Il Codice penale è stato innovato nel seguente modo: due nuove circostanze aggravanti previste una all'art. 61 c.p. numero 11-*undecies)*, e l'altra all'art. 294 c.p. e un nuovo reato all' articolo 612-*quater* (Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale).

[327] Si veda nota 322, p. 254.

2.11.3 DE IURE CONDENDO

Dalla disamina dell'AI ACT e della Legge AI, è possibile comprendere come premura del legislatore sia stata quella di incrementare i livelli di AI *transparency* e AI *expleinability* introducendo obblighi per i fornitori di sistemi IA ad alto rischio nella fase a monte di progettazione e sviluppo del sistema. Tuttavia, come è stato approfondito in questo studio, tali requisiti non vedono applicazione per tutti quei casi di *trading* ad alta frequenza implementati con algoritmi avanzati di *machine learning.*

Come evidenziato, uno dei principali limiti applicativi delle norme europee in materia di abusi – e, per riflesso, di quelle nazionali, considerato il rinvio operato dall'art. 187-ter TUF alla disciplina europea – risiede nell'intrinseca opacità dei sistemi algoritmici avanzati, che rende assai complesso dimostrare l'elemento soggettivo in capo a colui che si serve della macchina.[328] Tale opacità può, in concreto, trasformarsi in un meccanismo di elusione idoneo a schermare condotte illecite, rendendone più difficile l'accertamento e la sanzione.

Alla luce di ciò, e considerato che l'AI Act introduce obblighi di trasparenza e qualità degli algoritmi, dei dati e dei modelli matematici un concreto adottati, [329] proprio al fine di fronteggiare le criticità legate alla complessità e all'opacità dei sistemi di intelligenza artificiale, il legislatore europeo – ovvero le autorità di regolazione dei mercati finanziari – potrebbero considerare l'opportunità di formulare obblighi simili anche nel settore del *trading* algoritmico dato l' impatto e gli enormi rischi che da questo possono discendere.

Attraverso la previsione di mirati obblighi di trasparenza, documentazione e qualità posti in capo ai *providers* di sistemi algoritmici destinati ad essere impiegati nelle attività di *trading*, [330] sarebbe possibile attenuare il problema dell'opacità algoritmica e, forse, rafforzare anche l'effettività delle norme in materia di manipolazione del mercato. Tale

---

[328] Si specifica che la dimostrazione dell'elemento soggettivo è richiesta non solo nelle manipolazioni a carattere informativo ma anche in quelle a carattere operativo.
[329] Il riferimento è qui in particolare agli articoli 10, 11 e 13 dell'AI ACT.
[330] Nel contesto del *trading* algoritmico possono darsi due tipologie di fornitori: i *providers* "esterni" ossia tutti coloro dai quali la banca o l'impresa di investimento algoritmica (*HFT firm*) acquista il modello che poi verrà dalla medesima impiegata, ovvero *providers* "interni", in tal caso il modello algoritmico viene progettato, creato o sviluppato "internamente" dalla banca o HFT *firm* stessa che poi in concreto lo utilizzerà (*in house*). In questo ultimo caso la banca o la HFT *firm* assumerà sia la veste di *provider* (fornitore) quanto quella di *deployer* (utilizzatore).

soluzione potrebbe essere perseguita non tanto tramite un aggiornamento sostanziale della direttiva MiFID II, che, come è già stato illustrato nel cap. 1 risulta essere tecnologicamente neutra, [331] quanto intervenendo sui Regolamenti delegati (RTS).

2.12 ADEGUATEZZA E RESPONSABILITA'

L'analisi sino ad ora condotta ha consentito di verificare se rispetto a potenziali condotte illecite realizzabili tramite sistemi di *high-frequency trading*, l'impianto predisposto dal legislatore risulti sufficientemente solido e adeguato onde garantire un livello apprezzabile di "sicurezza esterna". Tuttavia, tale ricostruzione ha lasciato aperta una questione cruciale: quella del *quis respondeat* nel momento in cui l'abuso venga effettivamente realizzato. Posto che i modelli di intelligenza artificiale più avanzati sono caratterizzati da crescente autonomia decisionale ed operativa appare quindi lecito domandarsi se emergano delle criticità in relazione all'individuazione di un soggetto imputabile.

2.12.1 MACHINA DELINQUERE NON POTEST*?*

Per quanto concerne i sistemi di *trading* basati su algoritmi statici, chiedersi chi sia il soggetto responsabile, una volta che l'illecito di manipolazione dovesse essere compiuto, risulta essere piuttosto semplice. Essendo il sistema espressamente deterministico, è pacifico che il reato "*sia imputabile direttamente all'uomo, quando l'intelligenza artificiale è utilizzata come strumento per la consumazione mediante una serie di istruzioni da colui che, impartendole, l'abbia determinato a commettere materialmente l'illecito*". [332]

[331] Si pensi, in proposito alla definizione di "*trading algoritmico*" contenuta nell'art. 4(39)(40) che è sufficientemente ampia da ricomprendere anche i casi di *trading* algoritmico basato su *machine learning*, sul punto si rinvia al par. 1.10.
[332] CONSULICH, F., MAUGERI, M., MILIA, C., POLI, T. N., & TROVATORE, G. (2023). AI and market abuse: Do the laws of robotics apply to financial trading? (CONSOB Legal Research Papers, *Quaderni Giuridici* No. 29), p. 28.

In tale ipotesi, la lesione del bene giuridico rimane nel pieno controllo di chi impiega la macchina stessa, con la conseguenza che, il fatto, non è dell'algoritmo ma dell'uomo che ha incorporato nel codice di programmazione la strategia abusiva. A questo si può aggiungere che in presenza di un *input* umano alla commissione di un illecito il compimento di un evento diverso (ma pur sempre illecito) dovuto a una deviazione imprevedibile del sistema, non scinde il collegamento causale ma si risolve in una mera *aberratio causae* [333] che non sottrae l'uomo ad alcuna responsabilità.[334]

Nel caso quindi di un algoritmo statico impiegato per una strategia abusiva, la responsabilità dell'illecito ricadrà sempre sull' uomo; in tal caso vale, quindi, il brocardo di *machina delinquere (et puniri) non potest* [335] con la conseguenza di una responsabilità vicaria dell'essere umano che se ne è servito. [336]

La riflessione, tuttavia, si viene a complicare notevolmente in riferimento ai modelli auto apprendenti basati sul *machine learning*. Qualora infatti ci si trovi in presenza di un algoritmo di ultima generazione, capace di auto apprendere e di autonomia decisionale viene da chiedersi se, in tale ipotesi, il brocardo latino *machina delinquere non potest* sia ancora valido. Se la macchina (supponiamo un modello di *deep reinforcement elarning*) dovesse infatti apprendere in sede di addestramento che, al fine di massimizzare la funzione assegnata, la soluzione ottimale sia quella di porre in essere una strategia tale da integrare tutti gli elementi della fattispecie di manipolazione di mercato, l'AI si trasformerebbe da "*mero strumento*" ad "*autore del reato*", con discutibili conseguenze in tema di responsabilità.[337]

---

[333] L'*aberratio causae* consiste nella divergenza tra il decorso causale prefigurato dall'agente e quello che si realizza in concreto, fermo restando che l'evento tipico voluto si verifica comunque.
[334] CONSULICH, F. (2018). Il nastro di Möbius: Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato. *Banca, Borsa e Titoli di Credito*, 71(2), pp. 196–216.
[335] CAPPELLINI, A. (2018). Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale. *Criminalia*, 2018, p. 501.
[336] Nonostante la macchina costituisca in questo caso un mero strumento, taluni autori sottolineano una serie di difficoltà pratiche nell' imputare concretamente il fatto illecito in capo al *trader* umano, in proposito si veda: CONSULICH, F. (2018). Il nastro di Möbius: Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato. *Banca, Borsa e Titoli di Credito*, 71(2), pp. 196–216; PALMISANO, M. (2019). L'abuso di mercato nell'era delle nuove tecnologie: Trading algoritmico e principio di personalità dell'illecito penale. *Diritto penale contemporaneo – Rivista trimestrale*, 2/2019, pp. 129–159.
[337] BASILE, F. (2019). Intelligenza artificiale e diritto penale: Quattro possibili percorsi di indagine. *Diritto penale e uomo*, 10/2019, p. 27.

Con riferimento a questa seconda tipologia di sistemi, si pone quindi il problema di individuare chi sia il soggetto a cui rimproverare gli illeciti.

Una parte della dottrina sostiene l'idea che l'opacità e inspiegabilità dei modelli più avanzati (*black box*) determini un vuoto di tutela per il diritto penale, dovuto ad una impossibilità di applicare i tradizionali criteri di imputazione della responsabilità.

I fautori di questa teoria sostengono quindi la necessità di attribuire uno specifico *status* giuridico all'intelligenza artificiale, onde poter configurare una responsabilità diretta della macchina per gli illeciti da essa commessi. [338] Le giustificazioni a sostegno di tale tesi si basano principalmente su tre ordini di ragioni. La prima si fonda sull'assunto per cui le macchine sono capaci di un "*actus reus*" [339] inteso come la capacità di compiere azioni penalmente rilevanti (si pensi al movimento di un braccio robotico). La seconda si basa sul fatto che i sistemi AI, agendo sulla base della loro esperienza,[340] sarebbero in grado di intendere e di volere [341] in tal modo integrandosi il requisito della "*mens rea*". [342] Infine, l'ultimo argomento a favore di una responsabilità diretta della macchina fa leva sul fatto che, così come in passato sono state superate le ragioni ostative al riconoscimento di una responsabilità amministrativa dell'ente in conseguenza di un reato, allo stesso modo ciò potrebbe accadere per una AI. [343] In merito viene infatti sottolineato che l'ente non possieda "*a body to kick, and a soul to be damned*" [344] mentre un sistema AI avrebbe certamente "*a body to kick, but still no soul to damn*".[345]

---

[338] HALLEVY, G. (2015). Liability for crimes involving artificial intelligence systems. Springer; Si consulti anche la Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), il punto 59, lett. f) (sezione sulla responsabilità) in cui si chiedeva alla Commissione di riflettere sulla possibilità di: "*creare uno status giuridico specifico per i robot, in modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di rimediare ai danni che causano, ed eventualmente applicare tale "personalità elettronica" ai casi in cui i robot prendono decisioni autonome o interagiscono in modo indipendente con terzi".*

[339] HALLEVY, G. (2015). Liability for crimes involving artificial intelligence systems. Springer, p. 61.

[340] Il riferimento è qui ai sistemi di *reinforcement learning.*

[341] PIERGALLINI, C. (2020). Intelligenza artificiale: da "mezzo" a "autore" del reato? *Rivista italiana di diritto e procedura penale*, 63(4), p. 1745.

[342] HALLEVY, G. (2015). Liability for crimes involving artificial intelligence systems. Springer, p. 61 e p. 82.

[343] HALLEVY, G. (2015). Liability for crimes involving artificial intelligence systems. Springer p. 199

[344] COFFEE, J. C., Jr. (1981). "No Soul to Damn: No Body to Kick": An unscandalized inquiry into the problem of corporate punishment. *Michigan Law Review*, 79(3), pp. 386–459.

[345] ASARO, P. M. (2011). A body to kick, but still no soul to damn: Legal perspectives on robotics. In P. Lin, K. Abney, & G. A. Bekey (Eds.), *Robot ethics: The ethical and social implications of robotics* MIT Press pp. 169–186.

La ricostruzione che porta alla riconduzione di uno *status* giuridico della macchina, seppur per certi versi suggestiva, risulta sottovalutare alcuni aspetti di fondamentale rilevanza del diritto penale.

In primis, la macchina, anche nel sistema di AI più evoluto, difetta di un elemento essenziale e che è propriamente umano: quello della coscienza, [346] intesa come capacità di essere consapevoli di sé stessi: la macchina non sa di essere ne sa ciò che fa ma "*esegue in modo statico, logico, macchinico, mancando di intenzione e genialità*. [347] Difettando di questo elemento, le intelligenze artificiali, seppur possano agire con "tipicità dolosa" non sono in grado di autodeterminarsi e perseguire scopi "egoistici" se non quelli che l'uomo impone loro di fare. In virtù quindi del fatto che le macchine non hanno la capacità di comprendere il significato del loro agito e del valore delle loro azioni, allora non è possibile muovere nei loro confronti un rimprovero e, pertanto, difettano di "colpevolezza". [348]

In secundis, risulta essere fallace anche il parallelismo con la responsabilità amministrativa dell'ente dipendente da reato. In questo caso, infatti, l'ente come persona giuridica non è che una "*maschera, uno schermo che viene colpito dalla sanzione al fine di orientare quei burattinai umani che la manovrano*".[349] Posta in questi termini, allora, una sanzione che viene inflitta contro la macchina non farebbe che ripercuotersi sulla macchina stessa, senza orientare la condotta di alcuno. Sarebbe quindi, in definitiva, un diritto penale che dovrebbe rinunciare a se stesso, con il risultato che con l'ammettere una responsabilità della macchina, si finirebbe, per converso, per deresponsabilizzare l'uomo.[350]

Negare quindi uno *status* giuridico alla macchina sottintende da una parte riaffermare, anche nei sistemi AI più evoluti, il dogma del "*machina delinquere (et puniri) non potest*"

---

[346] MAGRO, M. B. (2020). Decisione umana e decisione robotica: Un'ipotesi di responsabilità da procreazione robotica. In *Giustizia penale e nuove tecnologie* Giappichelli, p. 16.
[347] BOVASSI, G. (2025). Attrazione digitale. Il lato oscuro del transumano e dell'intelligenza artificiale. Il Timone, pp. 90–91.
[348] CAPPELLINI, A. (2018). Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale. *Criminalia*, 2018, p. 15.
[349] *Ibidem,* pp. 17 e 18.
[350] BASILE, F. (2019). Intelligenza artificiale e diritto penale: Quattro possibili percorsi di indagine. *Diritto penale e uomo*, 10/2019, p. 28.

e dall'altro, la necessità di trovare un responsabile nell'essere umano che si colloca alle spalle di essa.

A sostegno della tesi umano-centrica è lo stesso AI ACT che all'art. 1 afferma: "*scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile".* In una medesima direzione si muove anche il legislatore italiano che, con la legge n. 132 del 23 settembre 2025 ha sancito all' art. 3, rubricato "principi generali", come *"i sistemi e modelli di A.I. per finalità generali devono essere sviluppati e applicati nel rispetto dell'autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità, della trasparenza, assicurando in ogni caso la sorveglianza e l'intervento umano".* Una tale impostazione assume una rilevanza importantissima nel diritto penale, laddove la centralità del controllo umano diventa elemento essenziale per l'imputazione della responsabilità, in tal modo evitando il rischio di una "*deriva tecnologica che potrebbe svuotare di significato i criteri tradizionali della responsabilità penale medesima*". [351]

2.12.2 QUOMODO HOMINEM PUNIRE?

Una volta sciolto ogni dubbio su "chi" sia tenuto a rispondere degli illeciti commessi mediante o da sistemi di intelligenza artificiale, occorre verificare "come" l'ordinamento possa concretamente imputare tali condotte al soggetto umano, in riferimento alle condotte di manipolazione.

A tal proposito, la teoria del "rischio consentito" offre una chiave di lettura molto utile. Come è stato già esaminato nel paragrafo 2.11.1, l'impianto dell'AI ACT è fondato su un approccio basato sul rischio. L' idea alla base della normativa europea, nonostante cerchi di tutelare nel modo più ampio possibile i diritti individuali, si basa sull'assunto per cui non si possa impedire, in assoluto, che i sistemi AI, pur conformi alla normativa di sicurezza, cagionino offese ai beni giuridici.[352] In altre parole, l'ordinamento delimita

[351] TRITTO, N. M. (2025). Verso il c.d. diritto digitale: prime riflessioni sulla riforma in materia di intelligenza artificiale. *Internet & Diritto*, 9/2025.
[352] FRAGASSO, B. (2024). Intelligenza artificiale e crisi del diritto penale d'evento: Profili di responsabilità penale del produttore di sistemi di I.A. In F. Basile, M. Biasi, L. Camaldo, G. Caneschi, B.

un'area di rischio "consentito" entro la quale "determinate aggressioni ai beni giuridici sono oggettivamente permesse".[353] [354]

Quella del rischio consentito [355] è quindi una teoria che permette, tramite regole cautelari, di perimetrare un'area entro la quale talune condotte lesive di beni giuridici vengono ammesse, in virtù di un bilanciamento di interessi effettuato *ex ante* e che, pertanto, non determinano una responsabilità penale nei confronti del soggetto agente. Ne consegue che, se una determinata attività dovesse oltrepassare i limiti stabiliti dal legislatore, la medesima sarà soggetta ad un rimprovero penale, qualora ne ricorrano i presupposti.[356] Il rischio consentito è una teoria che trova un forte appiglio nel settore degli illeciti aventi ad oggetto l'AI e una parte significativa della dottrina ha rimodulato infatti la nozione di "rischio consentito" riguardo alla responsabilità penale connessa all'impiego di sistemi di intelligenza artificiale. [357]

Seguendo tale impostazione, si potrebbe considerare come un'aerea di rischio ammissibile quella delineata a proposito del *trading* algoritmico e ad alta frequenza dalla normativa europea rappresentata dalla MiFID II e dai reg. delegati [358]. Invero, il legislatore, pur riconoscendo la pericolosità insita di questi strumenti tramite la regolazione, delimita uno spazio entro cui l'esercizio dell'attività debba considerarsi

---

Fragasso, & D. Milani (a cura di), *Intelligenza artificiale: Diritto, giustizia, economia ed etica* Giappichelli, p. 46.

353 ZIRULIA, S. (2018). Esposizione a sostanze tossiche e responsabilità penale. Giuffrè, p. 339.

354 Sul punto si veda l'art. 9 par. 5 AI ACT che afferma: "*Le misure di gestione dei rischi di cui al paragrafo 2, lettera d), sono tali che i pertinenti rischi residui associati a ciascun pericolo nonché il rischio residuo complessivo dei sistemi di IA ad alto rischio sono considerati accettabili*".

355 La letteratura sul tema è molto ampia: FORTI, G. (1990). Colpa ed evento nel diritto penale. Giuffrè, p. 250 ss.; CONSULICH, F. (2020). Rischio consentito. In M. Donini (Dir.), *Reato colposo* (Enciclopedia del diritto – I Tematici, p. 1102 ss.). Giuffrè; PIERGALLINI, C. (1995). Danno da prodotto e responsabilità penale. Giuffrè.

356 FRAGASSO, B. (2024). Intelligenza artificiale e crisi del diritto penale d'evento: Profili di responsabilità penale del produttore di sistemi di I.A. In F. Basile, M. Biasi, L. Camaldo, G. Caneschi, B. Fragasso, & D. Milani (a cura di), *Intelligenza artificiale: Diritto, giustizia, economia ed etica*, Giappichelli, p. 51.

357 PICOTTI, L. (Ed.). (2023). Resolution on traditional criminal law categories and AI. AIDP – International Association of Penal Law; GLESS, S., SILVERMAN, E., & WEIGEND, T. (2016). If robots cause harm, who is to blame? *New Criminal Law Review*, 19(3), pp. 412–431; MANES, V. (2020). L'oracolo algoritmico e la giustizia penale: Al bivio tra tecnologia e tecnocrazia. In U. Ruffolo (a cura di), *Intelligenza artificiale: Il diritto, i diritti, l'etica* (p. 5). Giuffrè; CAPPELLINI, A. (2018). Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale. *Criminalia*, 2018, p. 19; PIVA, D. (2022). Machina discere, (deinde) delinquere et puniri potest. *Rivista italiana di diritto e procedura penale*, 65(4), p. 681 ss.; CONSULICH, F. (2023). Il diritto penale al tempo dell'intelligenza artificiale: Prospettive punitive nazionali dopo l'AI Act. *Diritto e Difesa*, 3–4, p. 721 ss.

358 Per l'elenco dei regolamenti delegati (RTS) si rinvia al par. 1.6.

lecito e pienamente ammissibile ed in cui non sia possibile rimproverare al soggetto agente un evento dannoso, qualora quest'ultimo abbia rispettato tutte le regole cautelari. In questa prospettiva, la conseguenza è quella di un rimprovero che sorge solo nella misura in cui l'agente dovesse aver superato, con la sua condotta dolosa o colposa, tale "zona di sicurezza protetta".[359]

Da un punto di vista empirico è possibile porre l'attenzione a tre diverse possibili situazioni in astratto realizzabili.[360]

La prima ipotesi si viene a delineare ogniqualvolta un sistema di *trading* tradizionale o basato su *machine learning* venga utilizzato intenzionalmente dall'uomo con lo scopo materiale di compiere una manipolazione di mercato. In tale situazione, il dolo (intenzionale)[361] dell'uomo potrebbe essere dimostrato sulla base del fatto che la strategia illecita sia stata "iscritta" nel programma della macchina, la quale viene espressamente progettata per manipolare ovvero la medesima, nei modelli di *machine learning*, venga volutamente addestrata su set di dati in cui *ictu oculi* sia ravvisabile una certa condotta illecita (si pensi al caso di un *audit trail* in cui sono registrati tutti gli ordini immessi, cancellati e modificati).[362] In tale ipotesi, il soggetto ha agito dolosamente, collocandosi volutamente al di fuori di un perimetro di rischio consentito, usando (o istruendo) la macchina allo scopo precipuo di compiere un illecito e, pertanto, risulta azionabile il rimprovero penale ex art. 185 TUF, laddove ve ne ricorrano i presupposti.

La seconda ipotesi che può verificarsi concerne quella in cui non vi sia un finalismo illecito tale per cui il *trader* si ponga come obiettivo specifico quello di realizzare il fatto di reato, quanto, semmai, quest' ultimo non adotti le cautele necessarie affinché sia scongiurata la condotta di manipolazione da parte della macchina algoritmica. In altre parole, il singolo individuo non rispetta le regole cautelari poste come condizione per lo

---

[359] In tal caso troverebbero applicazione le disposizioni sanzionatorie previste dal pacchetto MAR-MAD II.
[360] DELLAGIACOMA, M. (2025). Negoziazione algoritmica, intelligenza artificiale e market abuse oltre l'high frequency trading: I profili di rilevanza penale (Tesi di dottorato, Università Commerciale Luigi Bocconi), p. 160 ss.
[361] Il dolo intenzionale si configura quando il soggetto agisce allo scopo di realizzare il fatto. Per una disamina approfondita si consulti: MARINUCCI, G., DOLCINI, E., & GATTA, G. L. (2023). Manuale di diritto penale. Parte generale (12ª ed.). Giuffrè Francis Lefebvre, p. 399.
[362] Per *audit trail* si intende la traccia completa e cronologica di tutte le operazioni compiute su un sistema, registrata in modo tale da poter ricostruire chi ha fatto cosa, quando e come.

svolgimento dell'attività, e sviluppa o utilizza un modello "programmaticamente inadeguato" rispetto agli standard normativi. Come nel caso precedente, siamo qui oltre l'area di rischio consentito. In questo caso, occorre indagare l'*animus* del soggetto, in quanto, a seconda delle circostanze, possono aprirsi due diversi scenari: se il *trader* si è rappresentato come possibile l'evento illecito, ma ciononostante ha deciso comunque di proseguire, costi quel che costi, aderendo volontaristicamente all'evento, all'esito di un bilanciamento consapevole degli interessi in gioco, ricorrerà il dolo eventuale, e quindi, nulla escluderebbe la possibilità di muovere un rimprovero penale ai sensi dell'art 185 TUF.[363] Oggetto del rimprovero in questo caso sarebbe la conoscenza, da parte del soggetto, che l' infrastruttura di *trading* non era stata adeguatamente predisposta per evitare condotte potenzialmente abusive, ma ciononostante, lui la ha comunque utilizzata.[364]

Se invece, il *trader* non avesse aderito volontaristicamente all' evento, ma fosse stato, negligente imperito o imprudente nel rispettare le regole cautelari sia nella dimensione di colpa grave sia in quella di colpa incosciente, allora in questa ipotesi il rimprovero ex art. 185 TUF non potrebbe essere mosso (si ricorda che l'art. 185 TUF richiede come elemento soggettivo il dolo).[365] Tuttavia, la condotta non rimarrebbe "scoperta" in quanto sarebbe comunque possibile azionare il 187 *ter* TUF che ammette la possibilità di sanzionare condotte colpose come illeciti amministrativi.

[363] Il dolo eventuale si ha quando il soggetto non persegue la realizzazione del fatto (la manipolazione) ma si rappresenta come possibile il verificarsi dell'evento, come conseguenza dell'azione e, pur di non rinunciare all' azione e ai vantaggi che né se ne ripromette, accetta il fatto che possa verificarsi: il soggetto decide di agire "costi quel che costi", mettendo in conto la realizzazione del fatto. Sul punto si rinvia nuovamente a MARINUCCI, G., DOLCINI, E., & GATTA, G. L. (2023). Manuale di diritto penale. Parte generale (12ª ed.). Giuffrè Francis Lefebvre, p. 401.

[364] La Corte di cassazione, nella nota sentenza *Sentenza n. 38343 (caso ThyssenKrupp)* ha elaborato una serie di indici sintomatici funzionali alla ricostruzione della sfera interiore del soggetto agente, tra cui si riportano: il grado di rischio, le capacità tecniche del soggetto agente, la reiterazione della condotta, le conseguenze lesive del soggetto agente.

[365] In diritto penale esistono due dimensioni della colpa. La prima viene definita "colpa cosciente" o "colpa con previsione" che ricorre ogniqualvolta il soggetto si rappresenta come possibile il verificarsi dell'evento, ma ciononostante si astiene dall'agire doveroso per "trascuratezza, irragionevolezza o altro biasimevole motivo" (si veda, in prop. sentenza *n. 38343 (caso ThyssenKrupp).* La seconda dimensione della colpa è quella descritta all'articolo 43 co. 1 c.p. in cui si stabilisce che "*il delitto è colposo, o contro l'intenzione, quando l'evento, anche se preveduto non è voluto dall' agente e si verifica a causa di negligenza imperizia o imprudenza, ovvero per inosservanza di leggi regolamenti, ordini o discipline*". Dunque, è possibile concludere che in questa seconda dimensione della colpa la "previsione dell'evento" non sussiste in quanto elemento caratterizzante la fattispecie di "colpa cosciente".

Infine, come ultimo scenario, vi è quello in cui il *trader*, pur avendo adottato tutte le misure cautelari rinvenibili nell'ordinamento e non mirando in alcun modo al compimento di strategie illecite, né accettandone il rischio, non riesca a impedire il verificarsi del fenomeno manipolativo. Si immagini un algoritmo di *machine learning* addestrato su *dataset* "puliti", privi cioè di qualsiasi collegamento teleologico con condotte abusive, e reso il meno possibile opaco nel suo funzionamento interno, che ciononostante, per ragioni in larga parte incomprensibili (*black box effect*), "apprenda" ad attuare sequenze di ordini idonee a integrare una manipolazione di mercato ai sensi dell'art. 12 MAR. In una situazione di questo genere, non pare possibile muovere alcun rimprovero al soggetto "dietro la macchina": difetterebbero, infatti, tanto gli elementi del dolo quanto quelli della colpa, entrambi imprescindibili ai fini dell'accertamento della colpevolezza dell'agente.

L'evento lesivo rientra, quindi, in quel residuo di rischio intrinseco non eliminabile, che l'ordinamento è chiamato a tollerare, a condizione che l'operatore abbia effettivamente rispettato le regole cautelari. [366]

L' analisi sino ad ora delineata, seppur con ampie semplificazioni, mette in luce come l'utilizzo dell'AI nel contesto specifico del *trading* algoritmico, non sembri mettere in discussione le classiche categorie di ascrizione della responsabilità per un fatto illecito fondate sul dolo e sulla colpa. Questo è dovuto, in parte, anche al fatto che il delitto di manipolazione di mercato descritta dall'art. 185 TUF risulti essere un reato di "mera condotta" e, pertanto, non è necessaria la dimostrazione del nesso causale tra la condotta e l'evento, semplificando così notevolmente gli oneri probatori.

In conclusione, pare ragionevole affermare come, a differenza di altre condotte offensive aventi ad oggetto l'AI in cui si assiste a una "crisi del diritto penale", [367] non pare potersi ravvisare un vuoto di tutela nel caso di manipolazioni di mercato realizzate tramite

---

[366] In questa ipotesi si accetterebbe "*un rischio normale nell' utilizzazione dei sistemi AI equiparabile al rischio ambientale oppure al caso fortuito e alla forza maggiore (artt. 45-46 cp), come tale imponderabile ma distribuito e condiviso su tutta collettività"* si veda CONSULICH, F., MAUGERI, M., MILIA, C., POLI, T. N., & TROVATORE, G. (2023). AI and market abuse: Do the laws of robotics apply to financial trading? (CONSOB Legal Research Papers, *Quaderni Giuridici* No. 29), p. 33.

[367] FRAGASSO, B. (2024). Intelligenza artificiale e crisi del diritto penale d'evento: Profili di responsabilità penale del produttore di sistemi di I.A. In F. Basile, M. Biasi, L. Camaldo, G. Caneschi, B. Fragasso, & D. Milani (a cura di), *Intelligenza artificiale: Diritto, giustizia, economia ed etica*, Giappichelli

algoritmi tradizionali ovvero basati sul *machine learning,* in riferimento alle tradizionali categorie di imputazione della responsabilità penale. [368]

A fronte della disamina sino ad ora svolta, occorre prendere atto che permangono talune questioni di non facile soluzione. Infatti, non sempre "dietro la macchina" esiste un unico individuo facilmente identificabile (il *trader*) bensì una pluralità di soggetti astrattamente responsabili. Si pensi, ad esempio, ad una banca o impresa di investimento che progetti e sviluppi internamente un algoritmo di *machine learning* senza affidarsi a fornitori esterni. In tale ipotesi, i soggetti potenzialmente responsabili potrebbero essere gli sviluppatori, i *designer*, i *trader*-operatori, i dirigenti ovvero lo stesso Consiglio di amministrazione, dando luogo a quello che in dottrina viene definito come un "*many hands problem*". [369] Con tale termine si intende la difficoltà di attribuire in modo chiaro la responsabilità per un danno o un illecito quando l'esito è il prodotto del concorso di molte persone non facilmente individuabili. [370]

Tuttavia, può segnalarsi come tale impedimento potrebbe essere in parte superato ricorrendo al d.lgs. 231/2001 che disciplina la "responsabilità dell'ente per gli illeciti amministrativi dipendenti da reato", [371] attraverso l'applicazione del contenuto di cui all'art. 8 del medesimo decreto. [372]

Affinché l'ente possa essere ritenuto responsabile ai sensi del d.lgs 231, è necessario che ricorrano i seguenti elementi. In primo luogo, deve essere stato commesso un reato specificatamente individuato dal legislatore nel d.lgs. 231, da parte di un soggetto apicale

---

[368] Alla conclusione giunge: DELLAGIACOMA, M. (2025). Negoziazione algoritmica, intelligenza artificiale e market abuse oltre l'high frequency trading: I profili di rilevanza penale (Tesi di dottorato, Università Commerciale Luigi Bocconi).

[369] CONSULICH, F. (2023). Il diritto penale al tempo dell'intelligenza artificiale: Prospettive punitive nazionali dopo l'AI Act. *Diritto e Difesa*, 3–4, p. 721 ss.

[370] TADDEO, M., & FLORIDI, L. (2018). How AI can be a force for good. *Science*, 361(6404), pp. 751–752. (Finding that: "*The effects of decisions or actions based on AI are often the result of countless interactions among many actors, including designers, developers, users, software, and hardware. This is known as distributed agency. With distributed agency comes distributed responsibility. Existing ethical frameworks address individual, human responsibility, with the goal of allocating punishment or reward based on the actions and intentions of an individual. They were not developed to deal with distributed responsibility*").

[371] Decreto legislativo 8 giugno 2001, n. 231, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300" (d.lgs. 231/2001). (GURI n. 140 del 19 giugno 2001).

[372] CONSULICH, F. (2018). Il nastro di Möbius: Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato. *Banca, Borsa e Titoli di Credito*, 71(2), p. 219.

o di una persona sottoposta alla direzione o vigilanza di un soggetto apicale. [373] In secondo luogo, la commissione del reato deve essere avvenuta *nell'interesse* o *a vantaggio* dell'ente. Infine, non devono essere state adottate le misure necessarie volte a prevenirne la realizzazione.

Nell'ipotesi di responsabilità degli enti, pertanto, il cuore del rimprovero si fonda sull'assenza di un'organizzazione adeguata, consistente in procedure e controlli volti a prevenire la commissione di un illecito. In sostanza, ad essere rimproverato è il *deficit* organizzativo presente all'interno della struttura aziendale, senza che sia necessario accertare in capo all'ente un elemento soggettivo in senso psicologico, come avviene per le persone fisiche.

Per quello che interessa il presente studio, l'art. 8 del d.lgs. 231/2001 consente, in particolare, di ricondurre una responsabilità in capo all'ente laddove l'autore del reato *non sia stato identificato*. In questo caso, si è in presenza di un indice inequivocabile di disorganizzazione in quanto l'anonimato dell'autore rivela l'assenza di regole, controlli e sistemi di tracciamento adeguati. [374] L'articolo risulta essere particolarmente utile nei casi in cui, per la frammentazione dei compiti e il coinvolgimento di più soggetti, sia difficile individuare uno o più autori materiali dell'illecito.

Alla luce della formulazione contenuta nel già menzionato art. 8 del d.lgs. 231 è quindi possibile ritenere responsabile del reato presupposto di manipolazione di mercato, realizzato mediante un algoritmo, l'ente medesimo, laddove sia dimostrato un deficit organizzativo che impedisca l'esatta identificazione del responsabile e venga provato che tale reato sia stato compiuto *nell'interesse* o *a vantaggio* dell'ente stesso.

Un'altra questione di non facile soluzione risiede nella difficoltà di individuare e dimostrare in concreto l'elemento soggettivo in capo all'autore dell'illecito di

[373] Il catalogo dei reati presupposto è contenuto agli art. 24 e ss. del decreto 231/2001 in cui si ricomprende anche la manipolazione di mercato.

[374] Laddove invece sorgano dubbi circa l'appartenenza dell'autore del reato alla struttura aziendale, è impossibile attribuire all'ente il fatto della persona fisica in quanto difetterebbe la prova del nesso imputativo di cui all' art. 5 del medesimo decreto legislativo. In particolare, tale disposizione richiede che "*L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a)*".

manipolazione, qualora quest'ultimo sia stato effettivamente identificato. Al riguardo, se nell'ipotesi di algoritmi tradizionali ciò non sembra porre particolari problemi, [375] è nei sistemi basati su ML che si palesano maggiori difficoltà.[376]

Invero, essendo questi sistemi caratterizzati da una ampia autonomia e, spesso, da una intrinseca opacità algoritmica, il pieno accertamento del dolo e della colpa risulta essere una operazione di difficile attuazione.

Come è stato enunciato nei paragrafi che precedono, una prima soluzione potrebbe essere quella di applicare ai fornitori di modelli algoritmici avanzati destinati ad essere impiegati nel settore del *trading* ad alta frequenza, il contenuto degli obblighi stabiliti per i *providers* di sistemi AI ad alto rischio, al fine di aumentare i livelli di AI *transparency* e AI *expleinability*.

Una seconda soluzione potrebbe essere quella di adottare nuovi criteri di accertamento dell'elemento soggettivo (dolo o colpa) che potrebbero consistere, ad esempio, nell' aver impiegato funzioni obiettivo estremamente generiche. Al riguardo si pensi alle seguenti funzioni assegnabili alla macchina: "*massimizza il profitto nel più breve tempo possibile*"; "*privilegia strategie che generano micro-profitti costanti anche se comportano un'elevata attività di cancellazione ordini*"; o infine "*apprendi e replica le strategie che storicamente hanno generato i maggiori profitti in finestre di pochi millisecondi, indipendentemente dal rapporto ordini eseguiti/cancellati*".

In considerazione della rilevanza che la funzione-obiettivo detiene, pare ragionevole, infine, sottoporre tali funzioni a un preventivo controllo da parte delle autorità competenti (Consob).

[375] In tale ipotesi, infatti, l'accertamento del dolo e della colpa potrebbero risiedere, invero, nel primo caso, nel fatto che il *trader* abbia incorporato nel codice di programmazione della macchina la strategia manipolativa, nel secondo caso, abbia omesso colposamente una opportuna programmazione onde scongiurare una strategia abusiva.
[376] Sul punto si rinvia a quanto già enunciato nel paragrafo 2.11.

CAPITOLO III

CYBERSECURITY E TRADING AD ALTA FREQUENZA

LA CYBERSECURITY: IL QUADRO NORMATIVO.

3.1 PREMESSA

Il presente capitolo si sofferma su un tema attuale e al tempo stesso rilevante, vale a dire quello della sicurezza informatica inerente i sistemi di negoziazione algoritmica. La trattazione dell'argomento in esame può far sorgere dubbi e perplessità circa il motivo per cui si intenda procedere a tale approfondimento; i dubbi sono legittimi e, pertanto, si rende necessaria una breve premessa introduttiva.

Nel capitolo che precede è stato illustrato come l'assetto normativo concernente gli abusi di mercato, vietando condotte illecite di manipolazione, sia atto a regolare il comportamento "esterno" della macchina algoritmica, allo scopo di garantirne un funzionamento controllato, corretto e sicuro.

A tal proposito, si può argomentare come anche la normativa concernente la sicurezza informatica (o *cybersecurity*) delle imprese di investimento algoritmiche miri a un fine simile, ma da una diversa prospettiva ossia quella "interna".

In particolare, dato che al giorno d'oggi risultano essere sempre più numerosi e frequenti i casi di minacce ed incidenti informatici, si rende necessario predisporre adeguati presidi normativi che si pongano come scudo rispetto a possibili fenomeni perturbativi esterni. Un eventuale attacco informatico perpetrato, ad esempio, da una impresa rivale a danno dei sistemi *hardware* o *software* della macchina algoritmica potrebbe non solo impattare economicamente sull'impresa che ne è vittima ma essere tale da poter innescare comportamenti non voluti e/o imprevisti dello stesso algoritmo di negoziazione, con effetti distorsivi sui mercati e con potenziali ricadute sistemiche.

In questa prospettiva, la normativa *cybersecurity* nel settore del *trading* algoritmico e ad alta frequenza costituisce la “cassetta degli attrezzi” [377] che permette alle imprese di proteggersi e tutelarsi meglio rispetto ad eventuali minacce o incidenti informatici.

Posto quindi che la trattazione della normativa sulla sicurezza informatica in connessione al *trading* algoritmico costituisce un approfondimento di indubbia rilevanza, nel presente capitolo si procederà, in primo luogo, ad analizzare il quadro normativo europeo ed italiano di riferimento in materia di *cybersecurity*, allo scopo di comprenderne i principi fondanti, le fonti e i soggetti destinatari; in secondo luogo, l’analisi si sposterà sulle normative in materia di sicurezza informatica che interessano, in particolare, le imprese di investimento algoritmiche; in terzo luogo, la disamina procederà poi ad inquadrare quali tra le tipologie di minacce informatiche possano in concreto verificarsi all’interno dell’infrastruttura tecnologica che permette il funzionamento dell’attività algoritmica e, in tale sede, un approfondimento sarà dedicato in particolare all’intelligenza artificiale.

In analogia al capitolo che precede, l’obiettivo della presente ricerca sarà quello di indagare e valutare l’adeguatezza della normativa e, per tale ragione, il presente capitolo si concluderà con una valutazione *de iure condito* e *de iure condendo*.

3.2 QUADRO TERMINOLOGICO DI RIFERIMENTO

La disamina concernete la *cybersecurity* nei sistemi di *trading algoritmico* e *ad alta frequenza* presuppone la conoscenza e la comprensione dei termini tecnici che sono formulati nell’ambito della sicurezza informatica la quale, come è noto, si distingue per un elevato impiego di vocaboli strettamente legati al settore tecnologico e digitale.

Un termine che risulta centrale nella presente analisi e dal quale è necessario partire è quello di *cyber space* (o spazio cibernetico).

---

[377] MELE, S. (22 gennaio 2026). Intervento alla tavola rotonda del convegno *Sicurezza dei dati nelle PMI: strumenti di compliance tra GDPR, NIS 2 e AI Act* (Camera dei Deputati, Sala Matteotti, Roma).

In dottrina, il *cyber space* [378] viene definito come quella dimensione caratterizzata dalla combinazione di diversi elementi fisici (i sistemi *hardware*) e logici (chiamati *software*) che vengono scambiati nel mercato secondo le leggi della domanda e dell'offerta.[379] In questa prospettiva lo spazio cibernetico viene a delinearsi come un agglomerato di prodotti, processi e servizi che attengono alle tecnologie dell'informazione e della comunicazione. [380]

A tal proposito, si precisa, [381] come le "merci" o gli elementi che compongono tale spazio ricomprendano, *in primis,* le "reti" e "i sistemi informativi" (*Information and Communication Technology* o ITC*).*

Nel caso di "reti" si intende l'insieme dei sistemi che consentono l'instradamento e la trasmissione di segnali[382] tra nodi presenti all'interno della rete stessa. [383] Al riguardo si pensi, a titolo esemplificativo, al WI-FI di casa che collegando più dispostivi a un *router,* consente a questi ultimi di comunicare tra loro nonché di accedere ad una rete ulteriore, ossia Internet. Nel caso di "sistema informativo", si allude, invece, a un dispositivo o a un gruppo di dispositivi tra loro interconnessi che eseguono, in base a un programma, una elaborazione dati in formato digitale. Per tale ipotesi si rinvia, ad esempio, al funzionamento di un *computer* che riceve *input* esterni sotto forma di dati digitali e che, secondo istruzioni specifiche, i c.d. programmi o *software*, li elabora al fine di produrre un determinato risultato. [384]

---

[378] Il prefisso '*cyber*' deriva dalla parola 'cibernetica', che, a sua volta, deriva dal termine greco antico κυβερνήτης col significato di timone o timoniere, pilota, governatore.
[379] RIZZI, M. A., & SERINI, F. (2024). Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano. *Rivista Italiana Di Informatica E Diritto*, 6(2), p. 118.
[380] *Ibidem*.
[381] SERINI, F. (2024). La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana. *Rivista Italiana Di Informatica E Diritto*, 5(2), p. 44.
[382] I segnali possono essere di natura elettrica, ottica o elettromagnetica e costituiscono il mezzo fisico attraverso cui le informazioni vengono trasmesse all'interno delle reti.
[383] Direttiva (UE) 11 dicembre 2018, 2018/1972 del Parlamento europeo e del Consiglio, recante "Direttiva che istituisce il codice europeo delle comunicazioni elettroniche (rifusione)" (European Electronic Communications Code), in GUUE L 321, pp. 36–214, art. 2(1).
[384] Direttiva (UE) 14 dicembre 2022, 2022/2555 del Parlamento europeo e del Consiglio, recante "Direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione" (Direttiva NIS 2), in GUUE L 333, pp. 80–152, art. 6(1).

In secundis, sono altresì considerati elementi del *cyber* spazio le "risorse ITC", queste ultime intese come "elementi presenti all'interno dei sistemi informativi e di rete".[385] A titolo esemplificativo sono considerate "risorse ITC" le componenti *hardware* di un *computer* come la *random access memory* (RAM) oppure la *central processing unit* o processore (CPU) che svolge la funzione essenziale di dare esecuzione alle istruzioni contenute nei programmi (*software*).

Volendo quindi ricorrere ad una immagine descrittiva, è possibile considerare i "sistemi informativi e di rete" (ITC) come una cornice composta, al suo interno, dalle diverse "risorse ITC" ossia i singoli prodotti *hardware* e *software* che rendono in concreto possibile il funzionamento dei sistemi stessi.

In conclusione, sembra corretto poter affermare che il termine *cyberspazio* si riferisca ad un luogo [386] o, secondo alcuni,[387] a un vero e proprio dominio da proteggere (in aggiunta ai quattro domini tradizionali: terrestre, marittimo, aereo e spaziale) caratterizzato da una specifica infrastruttura (ossia le reti e i sistemi informativi) e dall'interazione di questa con le singole persone fisiche e che, pertanto, data la sua rilevanza, risulta essere sottoposto a regole e controlli.[388]

Data l'enorme importanza che il cyberspazio riveste al giorno d'oggi, risulta fondamentale assicurare una adeguata protezione contro le "minacce informatiche" queste ultime intese come *qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone* (Art. 2 Reg. UE 881 del 2019, denominato *Cybersecurity Act*). [389]

---

[385] Regolamento (UE) 17 aprile 2019, 2019/881 del Parlamento europeo e del Consiglio, recante "Regolamento relativo all'ENISA (Agenzia dell'Unione europea per la cibersicurezza) e alla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione, e recante abrogazione del regolamento (UE) n. 526/2013" (Cybersecurity Act), in GUUE L 151 del 7 giugno 2019, pp. 15–69.
[386] MICHIELI, N. (2024). Cybersecurity e gestione del rischio ICT: l'impatto sulla corporate governance. *Banca Impresa Società*, 2, p. 244.
[387] MARZIALI, A. (2020). Cybersecurity: come la NATO si adatta alle nuove sfide. ISPI.
[388] Si parla in dottrina di "sovranità digitale" per riferirsi al processo di regolazione del cyberspazio da parte degli stati. Sul concetto di "Sovranità Digitale": MANGIAMELI, S. (2023). La sovranità digitale. *Diritti fondamentali*, (3), pp. 279–297.
[389] Regolamento (UE) 17 aprile 2019, 2019/881 del Parlamento europeo e del Consiglio, recante "Regolamento relativo all'ENISA (Agenzia dell'Unione europea per la cibersicurezza) e alla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione, e recante abrogazione del regolamento (UE) n. 526/2013" (Cybersecurity Act), in GUUE L 151 del 7 giugno 2019, pp. 15–69.

La pretesa di sicurezza all'interno dello spazio cibernetico ha interessato lo stesso legislatore europeo che nel corso degli ultimi decenni ha elaborato e adottato un quadro normativo a supporto della strategia di *cybersecurity.*

Rinviando al paragrafo successivo la disamina della normativa di riferimento, si anticipa qui come, dall'analisi complessiva della legislazione, scopo del legislatore eurounitario sia stato quello di promuovere al contempo tanto la "*cyber* sicurezza" quanto la "*cyber* resilenza".

Con il termine *cyber*sicurezza il legislatore europeo ha inteso riferirsi all' *"insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche"* (Art. 2 Reg. UE 881 del 2019, denominato *Cybersecurity Act*).[390]

Da tale definizione si ricavano alcune considerazioni di fondamentale importanza. Innanzitutto, si desume che il fine primario del legislatore sia la protezione delle "reti" e dei "sistemi informativi" vale a dire l' infrastruttura sulla quale sono conservate, trattate e trasmesse le informazioni in formato digitale.[391] La protezione di tali sistemi è quindi funzionale a garantire che i dati ivi contenuti mantengano le tre proprietà fondamentali della sicurezza (R.I.D.): la riservatezza (*confidentiality*) intesa come prevenzione dall'accesso o dall'uso da parte di soggetti non autorizzati; l'integrità (*integrity*) intesa come preservazione dell'accuratezza e completezza delle informazioni e, in particolare, come impedimento da alterazioni non autorizzate; e la disponibilità (*availability*) intesa come possibilità per i soggetti legittimati di accedere ai dati e ai servizi ogniqualvolta questi lo richiedano.[392] Pertanto, una eventuale minaccia informatica, qualora si concretizzasse (il c.d. incidente), andrebbe ad impattare almeno su una di queste tre proprietà.[393]

---

[390] *Ibidem.*
[391] Per "digitale" si intende la rappresentazione e il trattamento di informazioni mediante codifica numerica (tipicamente binaria), che consente la memorizzazione, l'elaborazione e la trasmissione dei dati tramite dispositivi elettronici.
[392] BATTELLI, E., & D'IPPOLITO, G. (2025). Compendio di normativa sulla privacy e cybersicurezza 2025. Nel diritto Editore, p. 311.
[393] Si pensi, ad esempio, ad un attacco DoS o DDoS che mediante l'invio massiccio di traffico nella rete, ne impedisca il regolare funzionamento, compromettendone la disponibilità ovvero si pensi a un *malware* che sottraendo o modificando informazioni, incida sulla riservatezza e sull'integrità dei dati.

In secondo luogo, nella medesima definizione si deduce anche il riferimento alla "sicurezza dell'umano"[394] inteso non solo come "utente" ossia la persona fisica che in concreto utilizza le risorse informatiche, ma anche come un qualsiasi soggetto che, pur non facendone uso, venga impattato negativamente dall'informatica o da minacce veicolate attraverso di essa. Pertanto, è possibile concludere che la scelta del legislatore europeo sia stata anche quella di indirizzare la *cybersicurezza* verso un fine pubblico, consistente nella protezione delle singole persone fisiche.

Tuttavia, raggiungere un livello adeguato di sicurezza affidandosi solo a misure tecnico-organizzative di protezione è ad oggi particolarmente arduo: la complessità dei sistemi e l'imprevedibilità dei rischi tecnologici impediscono di eliminare le incertezze e di mantenere il rischio entro soglie accettabili.[395]

A fronte di questa quasi insormontabile difficoltà, all'interno del *corpus* normativo europeo è stato avanzato più volte il concetto di "*cyber* resilienza". Sebbene non vi sia alcuna definizione nei documenti ufficiali, con tale termine si intende generalmente la "*capacità delle infrastrutture, delle reti e dei sistemi informativi di resistere, di adattarsi e di recuperare l'operatività dopo possibili eventi critici, siano essi attacchi informatici ma anche eventi critici che possano insorgere sul piano tecnico*".[396] La *cyber* resilenza implica quindi una concretizzazione della "minaccia informatica" (il c.d "incidente") sia nella dimensione dolosa dell'"attacco informatico" sia in quella non dolosa riconducibile, ad esempio, ad un errore di sistema, *bug*, guasto o malfunzionamenti dei prodotti ITC.

A differenza di una sicurezza "tradizionale", che risponde alla logica per cui la lesione del bene rappresenta un fallimento per le politiche di sicurezza,[397] la "*cyber* resilenza" si sviluppa su modelli di accettazione del rischio sul presupposto che, nonostante le robuste misure di sicurezza messe in atto, gli incidenti possano comunque verificarsi. Pertanto,

[394] RIZZI, M. A., & SERINI, F. (2024). Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano. *Rivista Italiana Di Informatica E Diritto*, 6(2), p. 123.
[395] CHIARA, P. G., & BRIGHI, R. (2024). La dimensione della "resilienza" nel diritto UE della cybersicurezza. *Ragion Pratica*, 2, p. 408.
[396] CORASANITI, G. (2025). Sicurezza informatica e intelligenza artificiale: Rischio e resilienza nello spazio giuridico europeo. Giappichelli, Torino, p. 30.
[397] RIZZI, M. A., & SERINI, F. (2024). Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano. *Rivista Italiana Di Informatica E Diritto*, 6(2) p. 126.

cyber sicurezza e *cyber* resilenza possono essere considerate come facce di una stessa medaglia: la prima, intesa come la capacità di proteggere i sistemi attraverso controlli preventivi di minimizzazione dei rischi;[398] la seconda, come la capacità di resistere a minacce informatiche preservando la funzionalità ovvero, in caso di soccombenza, di essere in grado di ripristinare le proprie funzionalità nel più breve tempo possibile.[399]

Assumendo questa prospettiva e concretizzando tali osservazioni rispetto all'oggetto del presente elaborato, il tema della *cyber* sicurezza e della *cyber* resilenza acquisiscono una portata determinante in relazione ai sistemi algoritmici di negoziazione ad alta frequenza.

In particolare, volgendo l'attenzione all'infrastruttura che supporta il funzionamento dei modelli HFT, sembra ragionevole poter teorizzare come la macchina algoritmica non sia altro che un complesso "ecosistema" caratterizzato da "reti" e "sistemi informativi". Si pensi, invero, ai complessi *server* che gestiscono il meccanismo di ricezione ed elaborazione dei *market data* al fine di generare un ordine di borsa (sistema informativo) ovvero ai sistemi che consentono l'instradamento e la trasmissione dei messaggi dai *server* dell'impresa di investimento ai sistemi di abbinamento presenti presso la piattaforma di negoziazione (reti).

Di fronte a una siffatta complessa rappresentazione, pare opportuno qualificare l'ambiente in cui si collocano le infrastrutture di *trading* ad alta frequenza come un vero e proprio "spazio cibernetico" (o *cyberspace*), contraddistinto da innumerevoli prodotti ITC tra loro interconnessi e rispetto al quale è necessario applicare misure che garantiscano la *cyber* sicurezza e la *cyber* resilenza in ragione della pericolosità che discende dalla modalità di negoziazione in commento. Invero, un "incidente informatico" si potrebbe ripercuotere non solo sulla singola HFT *firm* "vittima" ma, data l'interdipendenza dei soggetti che operano sui mercati finanziari, potrebbe estendersi anche ad altri attori economici, generando, in tal modo, un vero e proprio rischio "sistemico"[400] con pesanti ripercussioni sull' economia reale.

---

[398] CHIARA, P. G., & BRIGHI, R. (2024). La dimensione della "resilienza" nel diritto UE della cybersicurezza. *Ragion Pratica*, 2, p. 423.
[399] CASTALDO, F. (2019). Dalla cyber defense alla cyber resilience dell'infrastruttura critica. Alcune implicazioni strategiche e organizzative. *Rivista di economia e politica dei trasporti*, (3), Articolo 2, p. 7.
[400] BEVIVINO, V., & GIMIGLIANO, G. (2024). Il rischio sistemico ESG delle attività della FinTech. *Mercato Concorrenza Regole: Rivista quadrimestrale*, 1–2, pp. 175–224.

3.3 LA NORMATIVA EUROPEA

L'Unione Europea ha, nel corso degli ultimi decenni, ideato e adottato un quadro normativo a supporto della *cybersecurity* e *cyber-resilienza*, finalizzato alla protezione dei cittadini, delle imprese e delle istituzioni dalle minacce informatiche, promuovendo al contempo una costante cooperazione internazionale.[401] Di seguito verranno analizzate le principali fonti normative in materia "*cyber*".

Si premette che tale impianto normativo si snoda attraverso due macro-filoni tra loro complementari:[402] Il primo, normativo-strategico, è volto alla protezione e alla resilienza delle reti e dei sistemi informativi ed include, come vedremo, la Direttiva (UE) del 2022 n. 2555 denominata NIS II; la Direttiva (UE) del 2022 n. 2557 denominata CER (direttiva sulla resilienza sei soggetti critici); ed infine il Regolamento del 2022 n. 2554 (detto Reg. DORA), *lex specialis* della Direttiva NIS II, sulla resilienza operativa del settore finanziario. Il secondo macro-filone riguarda invece le normative che si occupano di certificazione e di standardizzazione della *cybersecurity* di determinati prodotti, servizi e processi ITC. Esse mirano a stabilire un livello uniforme di sicurezza ed interoperabilità nel mercato digitale europeo attraverso la creazione di schemi armonizzati di valutazione.[403] Tra queste ultime si annoverano il Reg. (UE) del 2019 n. 881 noto come *Cybersecurity Act* e il più recente Reg. (UE) del 2024 n. 2847 (*Cyber Resilience Act, CRA*).

Pietra miliare della normativa *cyber* eurounitaria è stata la Direttiva (UE) n. 1148 del 2016 recante misure per un livello comune ed elevato di sicurezza delle reti e dei sistemi informativi (c.d. NIS I – *Network and Information Security*). [404]

Con tale direttiva il legislatore UE aveva inteso, da una parte, individuare taluni soggetti privati e pubblici (identificati come operatori di servizi essenziali, detti "OSE" e fornitori

---

[401] BARBARA, G. (2022). La cybersecurity: minacce, evoluzione normativa, corporate governance e nuove prospettive. *Corporate Governance*, (4), p. 505.
[402] ARDITO, S. (2025). Tutela della cybersecurity e dell'intelligenza artificiale. In G. Cassano & E. Prosperetti (a cura di), *Le regole dei dati e dell'intelligenza artificiale: Dal GDPR alla Legge 132/2025* Maggioli Editore, p. 349.
[403] *Ibidem*, p. 350
[404] Direttiva (UE) 6 luglio 2016, 2016/1148 del Parlamento europeo e del Consiglio, recante "Direttiva concernente misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione" (Direttiva NIS), in GUUE L 194 del 19 luglio 2016, pp. 1–30.

di servizi digitali, detti “FSD”) tenuti a rispettare obblighi in tema di innalzamento delle misure di sicurezza per i propri sistemi informatici e di notifica nel caso di incidenti rilevanti subiti.[405]

Dall’altra, il legislatore aveva affidato agli Stati membri una serie di compiti, tra i quali: a) l’ adozione di una strategia nazionale di cybersicurezza, al fine di individuare priorità di intervento, piani di valutazione dei rischi, misure di risposta agli attacchi nonché di attivare programmi di formazione e sensibilizzazione collettiva sulle tematiche concernenti la sicurezza informatica; b) la designazione di una o più autorità nazionali competenti in materia di sicurezza informatica (la c.d. Autorità NIS); c) l’ istituzione di un gruppo unico di intervento in caso di incidenti informatici (*Computer Security Incident Response Team*, chiamato CSIRT); e, da ultimo d) l’ individuazione di un punto di contatto unico nazionale, al fine di assicurare un’effettiva cooperazione in materia tra le autorità europee e gli Stati membri. [406]

Tuttavia, la presenza di taluni profili di inadeguatezza della suddetta normativa [407] assieme a fattori economici, sociali e geopolitici, [408] ha condotto all’emanazione di una nuova Direttiva, la n. 2555 del 2022 (c.d. NIS II) [409] che ha abrogato la precedente e che ha cercato di armonizzare le criticità registrate fra gli Stati membri nel recepimento del precedente impianto.

---

[405] POLETTI, S. (2023). La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica. *MediaLaws – Rivista di diritto dei media*, 2, p. 402.
[406] PREVITI, L. (2022). Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico. *Federalismi.it*, (25), p. 71.
[407] *Ibidem*, in cui si evidenziano, quali difetti, l’assenza di termini specifici entro cui provvedere alle notifiche, l’elevata discrezionalità rimessa in capo agli stati membri sia nell’ individuazione delle autorità competenti sia nella possibilità di comminare sanzioni ai soggetti che non hanno ottemperato alle previsioni della direttiva ed infine’ eccessiva autonomia conferita agli stati membri nell’ identificazione degli operatori di servizi essenziali.
[408] Si veda: BUFFA, M. (2023). La direttiva NIS II cybersecurity in Europa: tra innovazione, formazione e diritto vivente. *Democrazia e Diritti Sociali*, 2023(1), p. 52.
In esso l’ autore individua, quali fattori che hanno determinato la necessità di una revisione normativa rispettivamente: 1) crescenti attacchi informatici; 2) le nuove sfide per il mercato interno dell’ UE dettate dalla crescente digitalizzazione; 3) ruolo sempre più importante della *supply chain;* 4) consapevolezza della necessità di armonizzazione di requisiti, controlli, sanzioni sui territori e negli ordinamenti degli stati membri; 5) nuova tecnologia 5g; 6) crisi pandemica dovuta alla diffusione del virus Covid-19; 7) conflitto tra Russia e Ucraina.
[409] Direttiva (UE) 14 dicembre 2022, 2022/2555 del Parlamento europeo e del Consiglio, recante “Direttiva relativa a misure per un livello comune elevato di cibersicurezza nell’Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972, e recante abrogazione della direttiva (UE) 2016/1148” (Direttiva NIS 2), in GUUE L 333 del 27 dicembre 2022, pp. 80–152.

In particolare, la Direttiva 2555 del 2022 (d'ora innanzi NIS II) pur mantenendo inalterato il fine perseguito dal legislatore UE, ossia la predisposizione di *misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno* (art. 1 par. 1 NIS II), amplia notevolmente il proprio ambito di applicazione rispetto alla precedente.

In primo luogo, viene superata la distinzione tra soggetti OSE e FSD proponendosi, invece, le categorie di soggetti "essenziali" [410] o "importanti"[411] ai quali si aggiungono poi una serie di entità definite come "critiche" dalla Direttiva UE del 2022 n. 2557 (CER). [412] Ciascuna delle suddette categorie di soggetti è destinataria di specifici obblighi al fine di innalzare "l'asticella" di cybersicurezza.

In secondo luogo, la NIS II ha il merito di collocare la sicurezza informatica tra le competenze dell'organo di amministrazione della società [413] in tal modo attribuendo espressamente agli amministratori la responsabilità per la gestione della sicurezza digitale. [414]

In terzo luogo, la NIS II, in continuità con la NIS I, impone agli Stati membri di adottare una strategia nazionale di cybersicurezza, di individuare uno o più CSIRT nazionali e la designazione di una Autorità nazionale competente in materia (la già nota Autorità NIS). Elemento di novità rispetto alla NIS I è poi l'istituzione della rete EU-CyCLONe per la gestione coordinata di incidenti e crisi cibernetiche.[415]

---

[410] Tali soggetti operano nei settori elencati nell'Allegato I NIS 2.
[411] Tali soggetti operano nei settori elencati nell'Allegato II NIS 2.
[412] Direttiva (UE) 14 dicembre 2022, 2022/2557 del Parlamento europeo e del Consiglio, recante "Direttiva relativa alla resilienza dei soggetti critici e recante abrogazione della direttiva 2008/114/CE del Consiglio" (Direttiva CER), in GUUE L 333 del 27 dicembre 2022, pp. 164–198.
[413] PÉREZ CARRILLO, E. F. (2023). Cybersecurity in European financial institutions: New grounds for corporate governance reform. *European Business Law Review*, 34(7), p. 1137.
(Finding that: *"The NIS Directives and especially DNIS2 have been instrumental in the acknowledgement that responsibility for the management of digital security, as well as liabilities arising from mismanagement, should be attributed to the Directors. This link had already been suggested by academics and experts, but it is only recently that it has been fully identified in written positive law: DNIS2 expressly places cybersecurity within the remit and under the responsibility of the entity's highest governance body (under the control of the Board of Directors where such Organisations are Corporations)")*.
[414] CULMONE, M. (2025). Rischi IT nelle entità finanziarie: riflessioni sul regolamento DORA. *Il Nuovo Diritto delle Società*, (8), p. 1514.
[415] BUFFA, M. (2023). La direttiva NIS II cybersecurity in Europa: tra innovazione, formazione e diritto vivente. *Democrazia e Diritti Sociali*, 2023(1), pp. 57-58.

Da ultimo, la NIS II rafforza anche gli obblighi concernenti le misure di sicurezza secondo un approccio multi-rischio e razionalizza altresì il processo di notifica allo CSIRT nazionale degli incidenti *significativi* che dovessero colpire i soggetti *essenziali* o *importanti.* [416] Nello specifico, si prevede che sia effettuata una *pre-notifica* senza ingiustificato ritardo e comunque entro 24 ore dalla venuta a conoscenza dell'incidente, a cui deve seguire, entro 72 ore dalla scoperta dell'incidente, una *notifica* di aggiornamento con annessa valutazione ed, infine, una *relazione finale* da inviare entro un mese.

A livello eurounitario, oltre alla Direttiva NIS II merita poi essere citato il Regolamento UE del 2019 n. 881 denominato *Cybersecurity Act* [417] con cui il legislatore UE ha inteso rafforzare il mandato dell'Agenzia dell'Unione Europea per la Cybersicurezza (ENISA) [418] e al tempo stesso, istituire un quadro europeo di certificazione della *cybersicurezza* per i prodotti, servizi e processi ITC. In tal modo, con il regolamento il legislatore mira a ottenere una *security by design,* ossia la creazione di *software* e *hardware* sicuri e affidabili sin dalla loro progettazione. [419]

Il quadro europeo *cyber* si completa, infine, con tre ultimi interventi di grande importanza.

Il primo è il Regolamento (UE) del 2022 n. 2554, noto come *Digital Operation Resilence Act* (Reg. DORA)[420] volto a promuovere una "*resilienza operativa digitale*" nel settore finanziario e per la cui trattazione specifica si rinvia al titolo II del presente elaborato.

---

[416] Ai sensi dell'art. 23 della direttiva NIS 2, un "incidente significativo" ricorre quando l'evento ha causato o può causare (a) una perturbazione operativa o perdite finanziarie sostanziali per il soggetto interessato, oppure (b) si è ripercosso o può ripercuotersi su terzi causando perdite materiali o immateriali considerevoli.

[417] Regolamento (UE) 17 aprile 2019, 2019/881 del Parlamento europeo e del Consiglio, recante "Regolamento relativo all'ENISA (Agenzia dell'Unione europea per la cibersicurezza) e alla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione, e recante abrogazione del regolamento (UE) n. 526/2013" (Cybersecurity Act), in GUUE L 151 del 7 giugno 2019, pp. 15–69.

[418] L' agenzia è stata istituita nel 2004 dal reg. UE 460/2004 e persegue la missione di migliorare la sicurezza informatica e delle reti di telecomunicazione dell'Unione Europea.

[419] POLETTI, S. (2023). La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica. *MediaLaws – Rivista di diritto dei media*, 2, p. 403.

[420] Regolamento (UE) 14 dicembre 2022, 2022/2554 del Parlamento europeo e del Consiglio, recante "Regolamento relativo alla resilienza operativa digitale per il settore finanziario e recante modifica dei regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011" (DORA), in GUUE L 333 del 27 dicembre 2022, pp. 1–79.

Il secondo è il Reg. (UE) del 2024 n. 2847 (*Cyber Resilience Act, CRA*)[421] relativo a misure orizzontali di cybersicurezza per i prodotti "*con elementi digitali*". [422] In particolare, il suddetto regolamento impone ai fabbricanti specifici obblighi nella fase di progettazione, sviluppo e manutenzione, al fine di garantire che tali prodotti da immettere sul mercato interno siano sicuri, secondo il già noto approccio di *security by design*. [423] Ne consegue che una volta immessi sul mercato i prodotti conformi potranno essere considerati *cyber-safe.* [424]

La cornice normativa si completa, da ultimo, con il Reg. (UE) del 2025 n. 38 denominato *Cyber Solidarity Act* [425] che prevede l'istituzione di un meccanismo europeo di collaborazione tra gli Stati membri per affrontare gli attacchi informatici su larga scala.[426]

Il tema della sicurezza informatica trova un riferimento valido anche al di fuori di quella che è stata propriamente definita con il termine "normativa *cyber*". Invero, lo stesso Reg. (UE) del 2024 n. 1689 (AI Act) riconosce come *la cibersicurezza svolga un ruolo cruciale nel garantire che i sistemi di IA siano resilienti ai tentativi compiuti da terzi con intenzioni malevole che, sfruttando le vulnerabilità del sistema, mirano ad alterarne l'uso, il comportamento, le prestazioni o a comprometterne le proprietà di sicurezza*.[427]

In linea generale, i sistemi AI sono anche sistemi informatici e per quanto concerne i profili di sicurezza, bisogna tener conto anche di questa loro secondo natura. [428] Pertanto,

---

[421] Regolamento (UE) 23 ottobre 2024, 2024/2847 del Parlamento europeo e del Consiglio, recante "Regolamento relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e recante modifica dei regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e della direttiva (UE) 2020/1828" (Cyber Resilience Act), in GUUE L, 2024/2847 del 20 novembre 2024.

[422] Per prodotti con elementi digitali si intende qualsiasi prodotto *hardware* o *software* e le relative soluzioni di elaborazione dati da remoto. Compresi i componenti software o hardware da immettere sul mercato separatamente. (Art 3 par. 1 CRA).

[423] CHIARA, P. G. (2023). Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali. *Rivista Italiana Di Informatica E Diritto*, 5(1), p. 145.

[424] BAGNI, F. (2023). La sandbox regolamentare e la sfida a tema cybersecurity: dall'Artificial Intelligence Act al Cyber Resilience Act. *Rivista Italiana Di Informatica E Diritto*, 5(2), p. 212.

[425] Regolamento (UE) 19 dicembre 2024, 2025/38 del Parlamento europeo e del Consiglio, recante "Regolamento che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e recante modifica del regolamento (UE) 2021/694" (Cyber Solidarity Act), in GUUE L 2025/38 del 15 gennaio 2025.

[426] BATTELLI, E., & D'IPPOLITO, G. (2025). Compendio di normativa sulla privacy e cybersicurezza 2025. Nel diritto Editore, p. 330.

[427] Considerando 76 AI ACT.

[428] FIORIGLIO, G. (2025). Intelligenza artificiale e cibersicurezza: profili informatico-giuridici, fra vulnerabilità delle macchine e delle persone. *I-lex*, 18(2), pp. 5-7.

posto che AI e cibersicurezza sono sempre più interconnesse con ruoli sempre più rilevanti, il Reg. AI ACT impone che i fornitori di sistemi di IA "ad alto rischio" adottino misure adeguate anche nella gestione dei rischi informatici.[429] [430]

A tal riguardo, l'art. 9 (AI ACT) rubricato "sistema di gestione dei rischi" prescrive ai *providers* l'obbligo di realizzare ed implementare un sistema completo di gestione del rischio in modo continuo ed iterativo, riferito *all' intero ciclo di vita del sistema.* [431] Ciò presuppone una preventiva identificazione ed analisi non solo dei rischi che derivano dall'utilizzo del sistema IA (i c.d. rischi legati all' "uso") ma anche dei rischi insiti "nel sistema stesso" ed indipendenti da un effettivo utilizzo.[432]

In altre parole, attacchi alla sicurezza informatica ovvero accessi non autorizzati ai sistemi di intelligenza artificiale, secondo la visione del legislatore UE contenuta nell'AI ACT, rappresentano una fonte di pericolo, in quanto, causando un malfunzionamento del sistema IA, possono in concreto provocare danni e mettere a rischio la stessa sicurezza delle persone fisiche (incidendo quindi sui diritti fondamentali).[433]

In questa prospettiva, risulta altresì essere di centrale rilevanza l'art. 15 (AI ACT) rubricato *accuratezza, robustezza e cibersicurezza* [434] che mira a garantire un funzionamento sicuro del sistema IA ad alto rischio durante l'intero ciclo di vita.

La disposizione in esame, recuperando un approccio di sicurezza sin dalla progettazione (*cybersecurity by design)* impone ai fornitori di progettare e sviluppare i modelli in maniera tale che essi siano *il più resilienti possibile* sia rispetto eventuali errori, guasti o incongruenze della macchina,[435] sia rispetto ai tentativi di terzi non autorizzati volti a

---

[429] Considerando 76 AI ACT.
[430] Si specifica che le misure di cibersicurezza contente nell'AI ACT non riguardano solamente i sistemi a rischio elevato ma sono previste, ad esempio, anche per i modelli di IA per finalità generali. Nella presente analisi, tuttavia, ci si soffermerà sulle misure di sicurezza informatica concernenti i sistemi ad alto rischio.
[431] Art. 9 par. 1 e 2 AI ACT.
[432] CORASANITI, G. (2025). Sicurezza informatica e intelligenza artificiale: Rischio e resilienza nello spazio giuridico europeo. Giappichelli, Torino, p. 108.
[433] *Ibidem.*
[434] Per "robustezza" si intende la capacità del sistema di mantenere le prestazioni sotto diverse condizioni operative, per "accuratezza" si intende invece l' assicurazione di prestazioni conformi alle specifiche dichiarate.
[435] Art. 15 par. 4 AI ACT.

modificarne l'uso, gli *output* e le prestazioni, sfruttando le vulnerabilità del sistema (i c.d. attacchi informatici).[436]

La medesima norma prevede poi, a livello operativo, alcune misure che in concreto possono essere adottate, quali, ad esempio soluzioni tecniche di ridondanza che includono *backup* o *fail-safe* [437] [438]ovvero misure volte a prevenire, accertare, rispondere, risolvere e controllare attacchi che cercano di manipolare il set di dati di addestramento (*data poisoning* o "avvelenamento dei dati") o i componenti pre-addestrati utilizzati nell'addestramento (*model poisoning* o "avvelenamento dei modelli"), gli input progettati in modo da far sì che il modello di IA commetta un errore (*adversarial examples* – "esempi antagonistici", o *model evasion*, o "evasione dal modello"), gli attacchi alla riservatezza o i difetti del modello.[439] Tali misure, si specifica, dovranno essere adeguate alle circostanze e ai rischi pertinenti, secondo il ben noto principio di proporzionalità.[440]

In conclusione, operando un confronto tra la normativa *cyber,* prima analizzata, e le disposizioni concernenti la cybersicurezza dei sistemi IA contenute nell'AI ACT, è possibile evidenziare quanto segue.

Nel contesto della normativa *cyber* la responsabilità circa l'identificazione e valutazione dei rischi è attribuita direttamente ai soggetti obbligati, ossia le imprese pubbliche e private. Queste ultime, in quanto esperte del loro assetto, sono chiamate a effettuare una mappatura completa delle attività e dei servizi suscettibili di incidere negativamente sulle reti e sui sistemi informativi e ad adottare misure di sicurezza proporzionate alla gravità del rischio rilevato.[441] In altre parole, l'impresa deve comprendere il proprio livello di esposizione al rischio ed adottare misure adeguate.

L'approccio adottato dall'AI ACT, invece, mantiene il medesimo paradigma regolatorio *risk based,* ma sembra divergere a livello operativo. Come noto, il Reg. (UE) del 2024 n.

---

[436] Art. 15 par. 5 AI ACT.
[437] Il *backup* consiste in una duplicazione del file o insieme di dati al fine di disporre di una copia di riserva. Il *fail-safe* permette invece di proteggere il sistema perché, in caso di guasto, lo porta automaticamente in una condizione sicura evitando effetti dannosi.
[438] Art. 15 par. 4 AI ACT.
[439] Art. 15 par. 5 AI ACT.
[440] *Ibidem*.
[441] ARDITO, S. (2025). Tutela della cybersecurity e dell'intelligenza artificiale. In G. Cassano & E. Prosperetti (a cura di), *Le regole dei dati e dell'intelligenza artificiale: Dal GDPR alla Legge 132/2025*, Maggioli Editore, p. 354.

1689 adotta uno schema piramidale basato su livelli di rischio differenti associati all'utilizzo del sistema AI. In questa prospettiva, il legislatore classifica già *ex ante* i sistemi IA in fasce di rischio con obblighi, vincoli o divieti differenziati.

Ne consegue che è la classificazione normativa stessa a stabilire *a priori* quale sia il regime che un sistema IA debba rispettare e, quindi, anche le disposizioni concernenti la sicurezza informatica, indipendentemente da una valutazione dei rischi del singolo operatore.[442]

3.4 NORMATIVA ITALIANA

Alla luce della esponenziale crescita del numero dei dispositivi e delle persone collegate alla rete, anche la legislazione italiana in tema di *cybersecurity* è stata oggetto, nel corso degli anni, di una costante e profonda implementazione.

Occorre innanzitutto rilevare che per il legislatore italiano il concetto di *cybersecurity* assuma una portata più specifica rispetto alla definizione elaborata in sede europea. Il decreto legge n. 82 del 2021 recante "*Disposizioni urgenti in materia di cyber sicurezza, definizione dell'architettura nazionale di cyber sicurezza e istituzione dell'Agenzia per la cybersicurezza Nazionale"*,[443] ha introdotto infatti, per la prima volta, la nozione di "Cyber Sicurezza Nazionale" all'art. 1, co.1 lett. *a*), definendola come: "*l'insieme delle attività, (...) necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico*".

Come per la formulazione di cybersicurezza fornita dal legislatore UE, anche all'interno della definizione di "cybersicurezza nazionale" è possibile distinguere "due anime".[444]

---

[442] *Ibidem*, p. 362.

[443] Decreto-legge 14 giugno 2021, n. 82, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale" (d.l. 82/2021). (GURI, Serie generale, n. 140).

[444] RIZZI, M. A., & SERINI, F. (2024). Una proposta di studio dei concetti di cybersicurezza e cyber resilienza in senso giuridico tra ordinamento europeo e italiano. *Rivista Italiana Di Informatica E Diritto*, 6(2), p. 124.

In primis, quella relativa alla protezione delle "reti e dei sistemi informativi" al fine di garantire le tre proprietà dei dati (R.I.D.), quali, la confidenzialità, l'integrità e la disponibilità.

In secundis, vi è anche quella relativa alla tutela della "*sicurezza nazionale e dell'interesse nazionale allo spazio cibernetico*", ancorando così la disciplina entro un confine dal tratto giuridico-politico. E' opportuno specificare che la nozione di "cybersicurezza nazionale" costituisce un concetto non completamente coincidente con quello di "sicurezza nazionale" ma ne è certamente ricompreso, posto che è oggettivamente impossibile tutelare l'interesse nazionale in assenza di misure volte a salvaguardare l'integrità dei processi e dei sistemi informativi che strutturalmente ne sono una parte integrante.[445]

In linea generale, la normativa *cyber* italiana si rivolge a due gruppi di soggetti destinatari: i soggetti individuati dal d.l. 21 settembre 2019 n. 105 e denominati "Soggetti Perimetro"; e i soggetti individuati dal d.lgs. 4 settembre 2024, n.138 in recepimento della NIS 2, denominati "Soggetti NIS".

Tenuto conto di quanto sopra enunciato è necessario attenzionare il decreto-legge 21 settembre 2019 n. 105,[446] convertito dalla legge n. 133 del 2019 [447] istitutivo del "*Perimetro di Sicurezza Nazionale Cibernetica"* (PSNC).

La *ratio* della normativa in commento viene espressa dall'art. 1 co. 1 d.l 105 del 2019 che testualmente recita: "*Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero*

---

[445] PANSA, A. (2019). La sicurezza nazionale: innovazione e nuovi limiti. *Gnosis*, 25(1), p. 27.
[446] Decreto-legge 21 settembre 2019, n. 105, recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica" (d.l. 105/2019). (GURI, Serie generale, n. 222).
[447] Legge 18 novembre 2019, n. 133, recante "Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica" (l. 133/2019). (GURI, Serie generale, n. 272).

utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è istituito il perimetro di sicurezza nazionale cibernetica".

Dalla lettura della norma in esame si comprende come il legislatore abbia inteso offrire una tutela specifica a tutte le amministrazioni pubbliche, enti e operatori nazionali pubblici e privati rientranti nel c.d. "Perimetro".

Tali soggetti sono individuati secondo due criteri: il primo consiste nel fatto che l'operatore *eserciti una funzione essenziale* dello Stato ovvero *assicuri un servizio essenziale* per il mantenimento delle attività civili, sociali o economiche fondamentali per gli interessi dello Stato. A tale requisito se ne aggiunge un secondo, consistente nel fatto che l'esercizio della funzione ovvero la prestazione del servizio è resa possibile tramite l'uso di *reti, sistemi informativi e servizi informatici dal cui malfunzionamento, interruzione, anche parziali, ovvero dall' utilizzo improprio può derivarne un pregiudizio per la sicurezza nazionale*.[448]

Dalla formulazione del sopracitato art. 1 (d.l 105 del 2019) rimangono esclusi gli incidenti minori che riguardano la c.d. "criminalità comune" ossia quegli incidenti che coinvolgono soggetti dai quali non possano scaturire lesioni alla già citata sicurezza nazionale. [449]

La determinazione delle "categorie" di soggetti che sono ricompresi all'interno del Perimetro viene demandata ad un apposito d.p.c.m. mentre l'indicazione puntuale dei "soggetti" che rientrano in esso viene effettuata mediante l'adozione di uno specifico provvedimento amministrativo "secretato" da parte del Presidente del Consiglio dei Ministri. [450]

I soggetti facenti parte del Perimetro (i c.d. "Soggetti Perimetro") sono tenuti al rispetto di una serie di obblighi.

In particolare, oltre all'adozione di apposite misure di sicurezza,[451] i Soggetti Perimetro sono tenuti a predisporre e a aggiornare annualmente un elenco delle reti, sistemi

---

[448] Art. 1 comma 2 lett *a)* d.l. 21 settembre 2019, n. 105.
[449] POLETTI, S. (2023). La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica. *MediaLaws – Rivista di diritto dei media*, 2, p. 404.
[450] GIUPPONI, T. F. (2024). Il governo nazionale della cybersicurezza. *Quaderni Costituzionali*, 2/2024, p. 285.
[451] Art. 1 comma 3 lett. *b)* d.l. 21 settembre 2019, n. 105.

informativi e servizi informatici nonché della componentistica ITC di rispettiva pertinenza.[452] E' previsto, inoltre, che tali soggetti notifichino gli *incidenti aventi impatto su reti, sistemi informativi e servizi informatici* allo CSIRT Italia: [453] entro un'ora per gli incidenti gravi ed entro sei ore per quelli meno gravi. [454]

Infine, ogniqualvolta i Soggetti Perimetro intendano procedere all' affidamento di forniture, beni e servizi ITC essi hanno l'obbligo di comunicarlo al Centro di Valutazione e Certificazione Nazionale (CVCN)[455] affinché tale componentistica sia sottoposta a controlli preventivi di sicurezza e di affidabilità. [456]

Il decreto prevede, inoltre, l'attribuzione al Presidente del Consiglio dei Ministri del potere di disporre la disattivazione, totale o parziale, di reti, sistemi informativi, servizi e prodotti ICT, in caso *di rischio grave e imminente per la sicurezza nazionale*.[457]

La normativa in esame appare dunque, nel suo complesso, un *corpus* di norme che sembra in parte replicare il modello già delineato in sede europea dalla direttiva NIS II volto ad innalzare il livello di sicurezza cibernetica in riferimento a taluni soggetti specifici, [458] tuttavia adattandolo allo specifico contesto della difesa nazionale.

Accanto al decreto legge n. 105 del 2019 (PSNC), vi è poi il già menzionato d.lgs. 4 settembre 2024 n.138 che recepisce la NIS 2 e che individua tutti quei "soggetti NIS" tenuti a conformarsi agli obblighi posti dal legislatore europeo e italiano.[459] Tale decreto conferma altresì il ruolo dell'Agenzia per la cybersicurezza nazionale come "Autorità nazionale competente NIS" e come "Punto di contatto unico".

In conclusione, il decreto PSNC e il decreto NIS, nel loro complesso, si rivolgono parallelamente a due categorie di soggetti, prevedendo per ciascuna di esse, un apposito

---

[452] Art. 1 comma 2 lett. *b)* d.l. 21 settembre 2019, n. 105.
[453] Tale organo opera in seno all' Agenzia per la cybersicurezza nazionale (ACN).
[454] A tal proposito è stato affermato dagli esperti del settore come questo limite temporale sia eccessivamente limitato per comprendere la tipologia di attacco, redigere il rapporto e notificarlo allo CSIRT nazionale mentre contestualmente si opera per delimitare e contrastare la minaccia. S. Mele, Convegno: "Le nuove reti per l'industria italiana e per i consumatori", 8 aprile 2021, in cybersecitalia.It.
[455] Tale organo, come per il CSIRT Italia è istituito presso l'ACN.
[456] Art. 1, comma 6, lettera a), del D.L. 21 settembre 2019, n. 105.
[457] Art. 5 d.l. 21 settembre 2019, n. 105
[458] GIUPPONI, T. F. (2024). Il governo nazionale della cybersicurezza. *Quaderni Costituzionali*, 2/2024, p. 286.
[459] Si pensi ad es. alla procedura sancita dalla NIS 2 per quanto concerne gli obblighi di notifica in caso di incidenti significativi nonché alle misure in tema di *corporate governance*.

regime giuridico. Al riguardo, occorre precisare che tali categorie non siano alternative tra di loro, potendo un soggetto rientrare in entrambe.

All'interno dell'impianto cyber nazionale, un ruolo centrale viene poi svolto dalla già citata Agenzia per la cybersicurezza nazionale (ACN). Tale Autorità è stata istituita con il decreto legge n. 82 del 2021, convertito dalla legge n. 109 del 2021,[460] e si colloca come una terza entità tra le categorie di soggetti precedentemente individuati. L'autorità ha assorbito talune delle competenze che erano precedentemente ripartite tra un'ampia pletora di soggetti [461] assumendo, pertanto, una veste fondamentale nell'attuale assetto normativo: per quanto concerne il versante NIS 2, essa è "Autorità nazionale competente NIS" nonché "Punto di contatto unico" e presso di essa ha la sede il già ricordato CSIRT Italia [462]; per quanto attiene invece al "Perimetro di sicurezza nazionale cibernetica" l'ACN è la sede del Centro di valutazione e certificazione nazionale (CVCN) e snodo di notifica degli incidenti per i "Soggetti Perimetro" (funzione svolta tramite lo CSIRT Italia).

---

[460] Legge 4 agosto 2021, n. 109, recante "Conversione in legge, con modificazioni, del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale" (l. 109/2021). (GURI, Serie generale, n. 185).

[461] In particolare, le prime disposizioni concernenti la sicurezza informatica risalgono al periodo 2012-2013, in tale periodo il legislatore aveva predisposto una complessa macchina amministrativa volta a risolvere, mediante tre distinti livelli di intervento, le criticità legate allo sviluppo delle moderne tecnologie. In primo luogo, un ruolo di cruciale importanza veniva affidato al Presidente del Consiglio dei ministri, al quale era attribuita la definizione degli indirizzi e degli obiettivi generali della politica di sicurezza cibernetica (primo livello). In secondo luogo, l' attuazione degli indirizzi e degli obiettivi era devoluta a una pluralità di organismi di supporto e coordinamento operativo (secondo livello) tra i quali: il Comitato interministeriale per la sicurezza della Repubblica (CISR), con funzione di consulenza; il Dipartimento delle informazioni per la sicurezza della repubblica (DIS), con il compito di presiedere tutte le attività di ricerca, analisi e di elaborazione informativa relative alle minacce e attacchi cibernetici; e il Nucleo per la Sicurezza Cibernetica, volto a a coordinare l' azione di tutti i soggetti coinvolti nella preparazione e nella gestione di crisi; l' Agenzia per l' Italia Digitale, alla quale spettava l' individuazione delle tecniche idonee a garantire la disponibilità, l' accessibilità, l' integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture digitali delle P.A. nonché il coordinamento delle attività svolte dal CERT-PA (*Computer Emergy Response Team*), istituito nel 2014, per supportare il settore pubblico nelle iniziative di reazione e ripristino (terzo livello). L'impianto descritto si è rivelato, tuttavia, alquanto complesso e inefficiente a causa della insufficiente attenzione rivolta alle problematiche connesse alla gestione delle situazioni di crisi, sia per il limitato coinvolgimento degli operatori economici del settore.
Sul punto: PREVITI, L. (2022). Pubblici poteri e cybersicurezza: Il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico. *Federalismi.it*, (25), pp. 75–76.

[462] Si ricorda che in origine tale organo era prima incardinato presso il Dipartimento delle informazioni per la sicurezza della repubblica, DIS.

Nel complesso, l'ACN rappresenta il fulcro dell'attuale architettura istituzionale in materia di cybersicurezza [463]e, in ragione di ciò, è chiamata a sviluppare e attuare la "Strategia nazionale di cybersicurezza" predisposta dal Presidente del Consiglio.[464]

Da ultimo, completa la normativa *cyber* italiana la legge 25 giugno 2024 n. 90[465] in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

Come è stato illustrato nel paragrafo 3.3, l'intelligenza artificiale e la sicurezza informatica costituiscono un nucleo inscindibile. A ragione di ciò, anche il legislatore italiano, sulla scia di quello eurounitario, ha formulato disposizioni specifiche in tema di sicurezza informatica all'interno della legge 23 settembre 2025 n. 132 (c.d. Legge IA).

In primo luogo, l'art. 3 (Legge IA) rubricato "Principi generali" eleva la cybersicurezza a principio generale, riconoscendo che *deve essere assicurata, quale precondizione essenziale, la cybersicurezza lungo tutto il ciclo di vita dei sistemi e dei modelli di intelligenza artificiale per finalità generali, secondo un approccio proporzionale e basato sul rischio, nonché l'adozione di specifici controlli di sicurezza, anche al fine di assi curarne la resilienza contro tentativi di alterarne l'utilizzo, il comportamento previsto, le prestazioni o le impostazioni di sicurezza.*[466]

In secondo luogo, l'art. 18 (Legge IA) rubricato "Uso dell'intelligenza artificiale per il rafforzamento della cybersicurezza nazionale" che aggiunge all' articolo 7 comma 1 del decreto-legge n. 82 del 2021, la lettera *m-quater)* con cui viene attribuito all'ACN il compito di *promuovere e sviluppare ogni iniziativa, anche attraverso la conclusione di accordi di collaborazione con i privati, comunque denominati, nonché di partenariato pubblico-privato, volta a valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale*".

La presente norma risulta di vitale importanza per due ordini di motivi. *In primis*, il legislatore riconosce che l'IA costituisce una risorsa innovativa e uno strumento

[463] GIUPPONI, T. F. (2024). Il governo nazionale della cybersicurezza. *Quaderni Costituzionali*, 2/2024, p. 289.
[464] SANCHINI, F. (2025). Sicurezza cibernetica e architettura istituzionale: verso una governance costituzionalmente orientata? *Federalismi.it*, (26), p. 180.
[465] Legge 28 giugno 2024, n. 90, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (l. 90/2024). (GURI, Serie generale, n. 153, pubblicata il 2 luglio 2024).
[466] Art. 3 comma 6 legge 132 del 2025 (Legge IA).

strategico per rafforzare la cybersicurezza nazionale. In altri termini, grazie alle capacità computazionali, predittive e di analisi di questa tecnologia, i sistemi IA possono essere validamente impiegati per la prevenzione e difesa delle infrastrutture nazionali. *In secondis,* si riconosce l'importanza del partenariato pubblico-privato (PPP) come pilastro fondamentale per l'attuazione delle politiche di cibersicurezza. Invero, grazie ad accordi di collaborazione nonché di partenariato pubblico-privati promossi dall'ACN con soggetti privati, dotati di risorse economiche, tecniche e organizzative superiori, si è in grado di perseguire al meglio gli obiettivi di sicurezza cibernetica nazionale.

In terzo luogo, all'interno della Legge IA degna di nota è anche la disposizione contenuta all'art. 19 comma 4 che attribuisce espressamente all'Agenzia per la cybersicurezza nazionale (ACN) il compito di garantire che gli aspetti di sicurezza informatica siano integrati nella pianificazione e nell'attuazione della "Strategia Nazionale per l'Intelligenza Artificiale 2024-2026" predisposta e aggiornata dalla Presidenza del Consiglio dei ministri.[467]

Infine, sempre con riferimento ai poteri e attribuzioni dell'ACN, merita essere ricordato il rilevantissimo articolo 20 (Legge IA) che designa l'Agenzia per l' Italia digitale (AgiD) e l'Agenzia per la cybersicurezza nazionale (ACN) quali "*Autorità nazionali competenti per l' intelligenza artificiale*", ferma restando l' attribuzione alla Banca di Italia, alla CONSOB, e all' IVASS del ruolo di autorità di vigilanza del mercato, ai sensi e secondo quanto previsto dall' articolo 74, par. 6 del Reg. (UE) del 2024 n. 1289 (AI ACT).[468]

In altre parole, l'ACN si vede attribuire un ulteriore ruolo rispetto a quello in materia di *cybersecurity*, consistente *nella vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi AI secondo quanto previsto dalla normativa nazionale e dell' UE.*[469] In virtù della citata disposizione, la vigilanza del mercato IA viene quindi affidata all'ACN e comprenderà i poteri necessari a garantire che i sistemi IA immessi sul mercato ovvero messi in servizio, o utilizzati rispettino i requisiti europei lungo l'intero ciclo di vita,[470]

---

[467] Quest'ultima, si ricorda, è il documento programmatico e procedurale che delinea finalità, priorità e obiettivi per lo sviluppo e l'adozione dell'IA in Italia, e che stabilisce un iter di formazione, aggiornamento e approvazione capace di garantire coerenza, partecipazione e responsabilità.
[468] Art. 20 comma 1 Legge IA.
[469] Art. 20 comma 1 lett. b) Legge IA.
[470] Tra questi requisiti, si ricorda, rientrano anche le disposizioni concernenti la sicurezza informatica.

ferma restando la specialità del settore finanziario, per la quale il legislatore ribadisce la competenza delle autorità di vigilanza del settore. [471]

L'art. 20 Legge IA prevede, da ultimo, che l'ACN sia *responsabile per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza*.[472] Una siffatta disposizione è coerente con il già esaminato art. 18 (Legge IA) nella misura in cui si riconosce che i sistemi AI apportino un fondamentale contributo nell'ambito della sicurezza informatica.

[471] TADDEI ELMI, G., CONTALDO, A., CAVACEPPI, C., & MARCHIAFAVA, S. (Eds.). (2025). Intelligenza artificiale: Legge 23 settembre 2025, n. 132. Il nuovo scenario giuridico italiano. Pacini Giuridica, p. 169.

[472] Art. 20 comma 1 lett. *b)* Legge IA.

CYBERSECURITY E TRADING ALGORITMICO

3.5 CONSIDERAZIONI PRELIMINARI

Nei paragrafi che precedono è stata illustrata, a livello generale, la normativa che il legislatore europeo ed italiano hanno predisposto nell'attività di prevenzione e contrasto alle minacce ed incidenti informatici. Oggetto del presente titolo sarà invece la disamina della normativa in tema di *cybersecurity* che interessa nello specifico le imprese di investimento algoritmiche. Successivamente l'analisi procederà ad esaminare le principali tipologie di minacce informatiche che possono verificarsi in relazione al settore specifico dell'AT e HFT.

3.6 LA NORMATIVA CYBER E IL TRADING ALGORITMICO

3.6.1 REG. UE n. 2554 del 2022 (Reg. DORA)

La prima fonte normativa in materia di *cyber security* che le imprese di investimento algoritmiche, sono tenute a rispettare è il già citato Reg. (UE) n. 2554 del 2022 (d'ora innanzi chiamato Reg. DORA).

Tale regolamento trova applicazione nei confronti di tutte le istituzioni finanziarie dell'UE e dei fornitori di servizi ITC allo scopo di migliorare e intensificare la sicurezza informatica, in ragione del fatto che l'ambito finanziario rappresenta uno tra settori più colpiti dagli attacchi informatici.[473]

In questa prospettiva, il Reg. DORA mira a predisporre una normativa armonizzata per i Paesi dell'Unione al fine di conseguire un elevato livello di "*resilenza operativa digitale*"[474] per tutte le entità finanziarie e istituire un quadro di sorveglianza per i fornitori ITC *critici*[475]*,* ciò sul presupposto che il settore in questione si caratterizza tanto

[473] GCSEC. (2020). L'impatto del cyber risk sul mercato finanziario: Case studies. GCSEC.
[474] Quest' ultima intesa come la "*capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni*" (art. 3 Reg. DORA).
[475] Per "fornitore terzo di servizi TIC" si intende un'impresa che fornisce servizi TIC (art. 3 Reg. DORA).

per un elevato grado di concentrazione degli operatori coinvolti, quanto per un sempre maggiore ricorso di questi ultimi a servizi digitali in regime esternalizzato. [476] A causa di questa stretta interconnessione e interdipendenza, eventuali attacchi alle reti e ai sistemi informativi potrebbero ripercuotersi infatti su tutta la catena dei soggetti causando possibili "effetti contagio".[477]

Mentre la NIS II si limita a porre requisiti concernenti la sicurezza informatica verso un'ampia platea di soggetti destinatari, il Reg. DORA, *lex specialis* rispetto alla direttiva, tratta la medesima materia secondo un approccio settoriale (il settore finanziario)[478] e da una prospettiva *orizzontale.* Esso si rivolge infatti a tutte le imprese del settore indipendentemente dall' attività svolta [479] e dal tipo di tecnologia impiegata,[480] secondo il principio di proporzionalità (art. 4 Reg. DORA), in forza del quale l'applicazione dei precetti deve avvenire tenendo conto delle caratteristiche specifiche e peculiarità di ciascuna entità.

La struttura del regolamento poggia su quattro pilastri, indicati all'art. 1 (Reg. DORA) che sono rispettivamente: a) obblighi applicabili alle entità finanziarie a livello di *corporate governance*; b) obblighi relativi agli accordi contrattuali stipulati tra entità finanziarie e fornitori terzi di servizi ITC; c) norme concernenti la sorveglianza per i fornitori terzi di servizi ITC individuati come *critici* per il settore finanziario; d) norme sulla cooperazione tra le autorità competenti ed entità finanziarie.

Di seguito si analizzeranno e descriveranno i suddetti quattro pilastri.

---

[476] SCHNEIDER, G. (2022). La resilienza operativa digitale come materia di corporate governance: Prime riflessioni a partire dal DORA. *Corporate Governance*, p. 555.
[477] ALFANO, G. (2024). Rischi informatici nel settore finanziario: Strumenti di prevenzione e resilienza operativa digitale. *Rivista di Diritto Bancario*, 4(Suppl.), p. 361.
[478] Il regolamento, tuttavia, non sostituisce la NIS II ma è *lex specialis* di settore. Si veda in proposito il considerando 16 del Reg. "*Tuttavia, dal momento che il presente regolamento accresce il livello di armonizzazione delle varie componenti della resilienza digitale, introducendo requisiti in materia di gestione dei rischi informatici e segnalazione di incidenti connessi alle TIC più rigorosi rispetto a quelli contenuti nell'attuale normativa dell'Unione in materia di servizi finanziari, questo livello più elevato determina un incremento dell'armonizzazione anche rispetto ai requisiti di cui alla direttiva (UE) 2022/2555. Di conseguenza, il presente regolamento costituisce una lex specialis rispetto alla direttiva (UE) 2022/2555*".
[479] L' art. 2 del Reg. DORA individua come destinatari della normativa un ampio numero di soggetti, tra i quali figurano, ad esempio, enti creditizi, sedi di negoziazione, imprese di investimento, agenzie di *rating*, controparti centrali, gestori di fondi alternativi *et cetera*.
[480] SCHNEIDER, G. (2022). La resilienza operativa digitale come materia di corporate governance: Prime riflessioni a partire dal DORA. *Corporate Governance*, p. 560.

Il primo pilastro, che riguarda gli obblighi a livello di *corporate governance,* si fonda sul principio della "*piena e principale responsabilità dell'organo di gestione per la gestione dei rischi informatici dell'entità finanziaria*" [481] eleggendo, pertanto, la *governance* societaria quale sede più effettiva di presidio dei rischi tecnologici. [482]

Posto quindi che la *cyber* sicurezza viene considerata parte integrante della gestione del rischio operativo, [483] il regolamento DORA affida agli organi di amministrazione una serie di compiti, organizzati secondo un modello "ellittico", tracciato attorno a due fuochi[484]: il *quadro di gestione dei rischi informatici* [485] e il *processo di gestione degli incidenti.*[486]

Con riferimento al "*quadro per la gestione dei rischi informatici*", l'ente finanziario (ai fini della presente analisi, un'impresa di investimento algoritmica) è tenuto agli adempimenti che seguono.

In primo luogo, a identificare e classificare tutte le funzioni commerciali o attività operative che dipendono da risorse ITC[487], individuare tutti i patrimoni informativi e le risorse ITC ed infine le possibili fonti di rischio o minacce informatiche connesse a tali risorse.[488]

In secondo luogo, a monitorare e a adottare misure di protezione adeguate per i prodotti ITC onde garantirne un sicuro funzionamento. A tal proposito, il regolamento impone che

---

481 Considerando 46 DORA.
482 SCHNEIDER, G. (2022). La resilienza operativa digitale come materia di corporate governance: Prime riflessioni a partire dal DORA. *Corporate Governance*, p. 563.
483 PÉREZ CARRILLO, E. F. (2023). Cybersecurity in European financial institutions: New grounds for corporate governance reform. *European Business Law Review*, 34(7), p. 1143. (Finding that: "*the new EU Digital Operational Resilience Regulation strengthens the regulatory requirements for cyber risk management in the financial sector. It deals with the issue of cyber security as a part of operational risk management").*
484 CULMONE, M. (2025). Rischi IT nelle entità finanziarie: riflessioni sul regolamento DORA. *Il Nuovo Diritto delle Società*, (8), p. 1517.
485 Art. 6 Reg. DORA. Si tratta di un documento programmatico, da aggiornare periodicamente, che comprende "*strategie, politiche, procedure, protocolli e strumenti in materia di TIC necessari per proteggere debitamente e adeguatamente tutti i patrimoni informativi e i risorse TIC, compresi software, hardware e server, nonché tutte le pertinenti infrastrutture e componenti fisiche, quali i locali, i centri di elaborazione dati e le aree designate come sensibili, così da garantire che tutti i patrimoni informativi e i risorse TIC siano adeguatamente protetti contro i rischi, compresi i danneggiamenti e l'accesso o l'uso non autorizzati*".
486 Art. 17 Reg. DORA.
487 Si rammenta che per risorsa o prodotto ITC si intende un *hardware* o *software* presente all'interno di una rete o sistema informativo (Art. 3 DORA ovvero art. 2 Cybersecurity Act).
488 Art. 8 par. 1, 2 e 4 DORA.

siano utilizzate soluzioni e processi ITC [489] che riducano i rischi di corruzione, perdita e di accesso non autorizzato ai dati; prevengano la mancanza di disponibilità, il deterioramento dell'autenticità e dell'integrità, le violazioni della riservatezza e la perdita di dati; ed, infine, assicurino una protezione dei dati contro i rischi derivanti da una cattiva gestione dei dati stessi. [490] Una siffatta disposizione assume, pertanto, una indubbia rilevanza ove l'impresa di investimento algoritmica dovesse impiegare *dataset* per l'addestramento di algoritmi di intelligenza artificiale.

In terzo luogo, a consentire l'individuazione tempestiva delle attività anomale nonché dei singoli punti di vulnerabilità (i c.d. *points of failure*) anche mediante strumenti di *alert* automatico[491] .

Con riferimento al secondo fuoco ("*processo di gestione degli incidenti connessi alle risorse ITC*"), è stato più volte evidenziato come una minaccia informatica potrebbe oltrepassare le barriere difensive e tradursi in un attacco informatico ovvero in un incidente connesso alle ITC non doloso. Rispetto a tali incidenti, gli enti, nella persona degli amministratori, sono tenuti in base al Reg. DORA a predisporre un "*processo di gestione degli incidenti connessi alle risorse ITC*" al fine di individuare, gestire e notificare i medesimi.

In particolare, il Reg. DORA prevede l'obbligo di segnalazione dei *gravi incidenti TIC* alle autorità competenti.[492] Con tale formulazione si intende la segnalazione di *qualsiasi incidente connesso alle TIC che ha un impatto avverso sui sistemi informatici e di rete a supporto delle funzioni essenziali o importanti dell' entità finanziaria*;[493] inoltre è prevista la notifica su base volontaria delle "minacce informatiche significative"[494] alle medesime autorità.[495]

---

[489] Ossia l'insieme delle attività svolte per progettare, sviluppare, fornire o mantenere un prodotto o servizio TIC.
[490] Art. 9 par. 1 e 3 DORA.
[491] Art. 10 par. 1 DORA.
[492] Nel caso di imprese algoritmiche l'autorità competente sarà verosimilmente la Consob.
[493] Art. 3 punto n. 8 DORA
[494] Per "minaccia informatica significativa" si intende una "*minaccia informatica le cui caratteristiche tecniche indicano che potrebbe potenzialmente causare un grave incidente TIC o un grave incidente operativo o di sicurezza dei pagamenti*" (Art. 3 DORA).
[495] Art. 19 par. 1 e 2 DORA.

Il regolamento DORA declina altresì la gestione del rischio informatico anche a livello "operativo": gli enti sono tenuti con cadenza annuale a svolgere "test di resilienza operativa digitale"[496] tra cui i "test basati su scenari", i "test di compatibilità", i "test di prestazione" e "test *end-to-end*".[497] Particolare rilevanza assume poi il *Threat-led penetration test* (TLPT, ossia test di penetrazione basato sulla minaccia) che consiste in una simulazione di attacco *cyber* da svolgere ogni tre anni allo scopo di mettere alla prova la tenuta del sistema difensivo.[498]

Con riferimento al secondo pilastro ("obblighi relativi agli accordi contrattuali stipulati tra entità finanziarie e fornitori terzi di servizi ITC")[499] è opportuno precisare quanto segue.

La dipendenza da fornitori di prodotti *software* e *hardware* nei mercati finanziari è molto elevata: si pensi ad esempio ad una impresa di investimento algoritmica che si affidi ad un *ITC service provider* per tutto ciò che concerne i servizi di *co-location*[500] ovvero per l'allacciamento alle reti necessarie alla trasmissione degli ordini di borsa o alla ricezione dei dati di mercato.[501]

La dipendenza da parte delle entità finanziarie dall'uso di servizi TIC[502] e la natura pressoché "oligopolistica" di taluni fornitori[503] possono determinare una condizione di *asimmetria contrattuale* tale da generare a sua volta difficoltà "*nel negoziare condizioni contrattuali conformi a norme prudenziali*".[504]

In ragione di ciò, il regolamento DORA impone *in primis* la definizione di una "strategia basata su una varietà di fornitori"[505] nonché l'obbligo di svolgere una accurata *due*

---

[496] Art. 24 par. 1 DORA.
[497] Art. 25 par. 1 DORA.
[498] Art. 26 DORA.
[499] Questi ultimi vengono definiti come "imprese che forniscono servizi ITC" (ART 3 DORA). Per "servizio ITC" si intende invece un servizio "*consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi*" (Art. 2 Cybersecurity Act).
[500] Sulla spiegazione della co-locazione si rinvia al paragrafo 1.3.
[501] A tal proposito può essere citato l'esempio di *Bloomberg L.P.* ossia una multinazionale operativa nel settore dei *mass media* che fornisce dati di mercato nonché, tramite la "*Bloomberg Terminal* consente l'accesso ad una piattaforma per analisi, notizie e monitoraggio dei mercati.
[502] Considerando 27 DORA.
[503] ALFANO, G. (2024). Rischi informatici nel settore finanziario: Strumenti di prevenzione e resilienza operativa digitale. *Rivista di Diritto Bancario*, 4(Suppl.), p. 372.
[504] Considerando 28 DORA.
[505] Art. 28, par. 2 DORA.

diligence prima di stipulare qualsiasi accordo avente ad oggetto servizi o prodotti ITC. *In secundis,* il Reg. DORA prevede l'apposizione di apposite clausole volte a fornire alcune garanzie minime come, ad esempio, il diritto dell'impresa finanziaria di accedere e ispezionare le tecnologie fornite.[506]

Per quanto attiene al terzo pilastro ("norme concernenti la sorveglianza per i fornitori terzi di servizi ITC individuati come *critici* per il settore finanziario"), il Reg. DORA istituisce un quadro di sorveglianza da parte delle autorità competenti per tutti quei fornitori ITC qualificati come *critici* per le entità finanziarie. [507] Ai fini di tale qualificazione, rilevano i criteri forniti dall'art. 31 par. 2 Reg. DORA, la cui puntualizzazione è rimessa ad un atto delegato della Commissione. La *ratio* alla base di tale scelta normativa viene individuata nel fatto che "*alcuni fornitori svolgono un ruolo significativo nella fornitura di servizi finanziari, o sono diventati parte integrante della catena del valore dei servizi finanziari divenendo fondamentali per la stabilità e l'integrità del sistema finanziario dell'Unione".*[508]

Infine, per quanto attiene al quarto ed ultimo pilastro ("norme sulla cooperazione tra le autorità competenti ed entità finanziarie"), occorre rilevare quanto segue. All'interno del Reg. DORA vengono costantemente promosse forme di condivisione dei dati e notizie, e a tal proposito, i "flussi informativi" si muovono in tre direzioni. Un primo gruppo concerne il già attenzionato profilo della segnalazione degli incidenti informatici gravi nonché delle minacce informatiche significative da parte degli enti finanziari alle autorità competenti; un secondo gruppo riguarda la condivisione delle informazioni tra autorità competenti ai sensi del Reg. DORA e altre autorità pubbliche non finanziarie;[509] da ultimo, un terzo flusso informativo viene incoraggiato dal Reg. DORA tra gli stessi operatori finanziari ed è volto alla prevenzione dei rischi informatici. [510] Su questo ultimo punto si fa presente che il meccanismo di condivisione di informazioni deve rispondere alle caratteristiche indicate all'art. 45 (Reg. DORA), onde evitare la qualificazione del

[506] Art. 30 DORA.
[507] Art. 31 DORA
[508] Considerando n. 79 DORA.
[509] Art. 48 e seg. DORA.
[510] Art. 45 DORA.

medesimo come "intesa restrittiva della concorrenza" sanzionabile secondo il diritto *antitrust*.

Dalla complessiva analisi della normativa in esame emerge, in conclusione, che il legislatore eurounitario ha inteso affrontare il tema della *cybersecurity* degli operatori finanziari rinviando principalmente a competenze e responsabilità di *corporate governance*, ricorrendo a scelte strategiche sul versante sia infrastrutturale che operativo.[511] In questo senso, l'adozione, da parte dell' organo di gestione, di reti e sistemi informatici adeguati ricalca l'art 2083 c.c. che prescrive per l' imprenditore il *dovere di istituire un assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa*.

Ne consegue che, in generale, le imprese di investimento e gli altri enti finanziari vedranno un significativo ampliamento dei compiti e doveri attribuiti in seno ai Consigli di amministrazione e agli organi di gestione e anche un incremento dei costi legati all'adeguamento organizzativo e tecnologico, all'implementazione dei presìdi di controllo e alla continua attività di monitoraggio e rendicontazione.[512]

3.6.2 DIRETTIVA UE n. 65 del 2014 (MIFID II)

Il tema della sicurezza informatica trova un riferimento specifico anche all'interno della più volte richiamata Direttiva (UE) n. 65 del 2014 (MiFID II). Occorre premettere che, a differenza del Reg. DORA, le norme concernenti la *cybersecurity* trovano una applicazione *verticale,* in ragione del fatto che il legislatore UE si è preoccupato di trattare la materia con riguardo specificatamente alle imprese che svolgono negoziazione algoritmica. [513]

Ai fini della presente analisi è necessario riferirsi alla disposizione contenuta nel paragrafo 1 dell'art. 17 (MiFID II) rubricato "Negoziazione algoritmica" che recita: "*le imprese di investimento che effettuano negoziazione algoritmica pongono in essere*

[511] PIVA, D. (2022). Cybersecurity e corporate governance tra valutazioni top-down e tecniche bottom-up. *Corporate Governance*, 4, p. 528.
[512] MICHIELI. (2024). Cybersecurity e gestione del rischio ICT: l'impatto sulla corporate governance. *Banca, Impresa, Società*, (2), p. 259.
[513] A differenza del DORA che segue un approccio "orizzontale".

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".

La formulazione ha un valore esplicitamente programmatico e, come sarà tra poco attenzionato, trova una declinazione specifica all'interno dell'articolo 18 del regolamento delegato n. 589 del 2017 (d'ora innanzi RTS 6).[514]

Per quanto concerne la norma in esame, occorre rilevare quanto segue. Innanzitutto, il soggetto che effettua attività di *trading* algoritmico è tenuto a attuare *controlli dei sistemi e del rischio*, che avranno verosimilmente ad oggetto l'infrastruttura formata da "reti" e "sistemi informativi" (ecosistema HFT) che permette il funzionamento della macchina algoritmica.[515]

Tali controlli devono assicurare la "*resilenza dei sistemi*" che può essere qui intesa come capacità di ripristinare le proprie funzionalità dopo un *cyber* incidente doloso o meno,[516] nonché, "*evitare l'invio di ordini erronei o un funzionamento dei sistemi tale da creare un mercato disordinato*".

Tale ultimo inciso merita il seguente approfondimento.

Il riferimento a "*impedire l'invio di ordini erronei o un funzionamento dei sistemi tali da creare un mercato disordinato*" è idoneo a ricomprendere non solo il divieto di programmare la macchina algoritmica allo scopo precipuo di compiere manipolazioni di mercato (HFT come "autore")[517] ma, anche, quello di scongiurare che la medesima sia

---

[514] Regolamento delegato (UE) 19 luglio 2016, 2017/589 della Commissione, recante "Regolamento che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda i requisiti organizzativi e le condizioni di funzionamento delle imprese di investimento che effettuano negoziazioni algoritmiche" (RTS 6), in GUUE L 87 del 31 marzo 2017, pp. 417–460.
[515] La formulazione "efficaci ed idonei per l'attività esercitata" può essere intesa come una declinazione del principio di proporzionalità già formulato dal Reg. DORA (art. 4) e qui adattato a seconda delle dimensioni e tipologia dell'impresa di investimento algoritmica.
[516] Il termine "resilenza" può essere una nozione comprensiva anche del termine "*cyber* resilienza".
[517] A dimostrazione di ciò l'art. 17 par. 1 prosegue affermando: "*Tali imprese pongono in essere anche controlli efficaci dei sistemi e del rischio per garantire che i sistemi di negoziazione non possano essere utilizzati per finalità contrarie al regolamento (UE) n. 596/2014 o alle regole di una sede di negoziazione a cui esse sono collegate*" con un chiaro riferimento alle norme del *Market Abuse Regulation*.

"vittima" di incidenti informatici[518]. In altre parole, il legislatore, richiedendo di sottoporre l'infrastruttura tecnologica algoritmica a verifiche e controlli, mira a prevenire che eventuali attacchi o incidenti non dolosi possano compromettere l'integrità stessa dei sistemi e determinare alterazioni nel funzionamento degli algoritmi. Invero, una eventuale perturbazione esterna del funzionamento della macchina algoritmica, dovuta, ad esempio, ad un attacco informatico, potrebbe innescare effetti distorsivi sui mercati ovvero condurre a condotte che, sebbene non programmate da un operatore umano, siano idonee a qualificarsi come "manipolazioni di mercato". [519]

L'art. 17 MiFID II trova una specifica attuazione all'art. 18 del Reg. delegato n. 589 del 2017 (RTS 6), rubricato "*Sicurezza e* limiti di accesso".

Il legislatore, all'art. 18 paragrafo 1 (RTS 6), riferendosi espressamente alle imprese di investimento che effettuano *trading* algoritmico, richiede che queste ultime attuino una strategia basata su *"un'organizzazione informatica affidabile* e che *sia in linea con una gestione efficace della sicurezza informatica"* [520]. Il legislatore ha inteso riferirsi, quindi, non solo alla predisposizione di presidi e misure di protezione dei sistemi ma anche alla definizione di un assetto organizzativo idoneo a governare l'intero ciclo di vita dell'infrastruttura.

A tal proposito, viene infatti esplicitato all'art. 18 par. 2 (RTS 6) che "*l'impresa di investimento <u>istituisce e mantiene</u> dispositivi adeguati alla sicurezza fisica ed elettronica che riducano al minimo i rischi di attacchi contro i sistemi informatici e che comprendano un'efficace gestione dell'accesso e dell'identità"*.[521] Con tale formulazione il legislatore ha inteso riferirsi, quindi, a una cybersicurezza che deve essere garantita sin dall'origine,

---

[518] Il termine "incidente" deve essere qui inteso in senso ampio, sia come "attacco informatico" sia come "incidente informatico non dipendente da attacco informatico" come bug o malfunzionamenti dei sistemi.
[519] Sul punto si veda: AZZUTTI, A. (2024). AI governance and algorithmic trading: Some regulatory insights from the EU AI Act. *Banking & Finance Law Review*, 41(1), p. 12. (Finding that: "*AI trading systems may <u>act as victims</u> in a market accident or misconduct. In addition to cases of malfunctions, AI systems may be vulnerable to manipulation by other agents, whether human or algorithmic, aimed at negatively impacting their technical integrity and/or operational performance. For instance, a malicious third party may seek to exploit a cybersecurity flaw or other vulnerability to gain access and/or cause unintended behaviour. More simply, algorithmic trading systems may be misled by other traders through specific trading strategies attempting to manipulate them into making decisions that are disadvantageous to themselves. These cases represent examples of "adversarial attack". Present from the earliest GOFAI applications, AI "vulnerability" underpins the need for appropriate governance and regulatory frameworks that ensure the integrity and security of trading technology amidst its growing complexity").*
[520] Art. 18 par. 1 RTS 6.
[521] Art. 18 par. 2 RTS 6.

c.d. *cybersecurity by design*, e lungo tutto il ciclo di vita del sistema ("istituisce e mantiene").[522]

L'art. 18 par. 3 prevede, inoltre, l'obbligo per l'impresa di investimento di "*informare immediatamente l'autorità competente di eventuali violazioni rilevanti delle sue misure di sicurezza fisica o elettronica"* che dovessero verificarsi. [523]

Il paragrafo, impiegando la formula "*violazioni rilevanti delle misure di sicurezza fisica o elettronica*" adotta una terminologia nuova sia con riferimento al Reg. DORA, che distingue ai fini della notifica tra "*grave incidente TIC*" e "*minaccia informatica significativa*"[524] sia con riferimento alla direttiva NIS 2 che adotta i termini di "*incidente significativo*" e "*minaccia informatica significativa*". [525]

A causa del mancato chiarimento da parte del legislatore circa il significato e la portata della formulazione di cui sopra, la medesima potrebbe essere idonea a generare problemi di coordinamento. Sul punto si rinvia, per una analisi più approfondita, al paragrafo 3.8 del presente elaborato.

L'art. 18 par. 4 prevede, altresì, l'obbligo per le imprese di investimento algoritmiche di svolgere con cadenza annuale prove antintrusione (c.d. *penetration test*) e scansioni di vulnerabilità per simulare *cyber* attacchi. Occorre rilevare come il legislatore non abbia voluto imporre specifici requisiti in relazione alle modalità di svolgimento di tali test, conseguendone, pertanto, una certa libertà per le imprese.[526]

Infine, l'art. 18 par 5 conclude stabilendo che "*l'impresa di investimento assicura di essere in grado di identificare tutte le persone che detengono diritti di accesso critici ai suoi sistemi informatici. L'impresa di investimento limita il numero di tali persone e ne*

[522] Art. 18 par. 2 RTS 6.
[523] Art. 18 par. 3 RTS 6 che ulteriormente prevede che l'impresa "*trasmette un rapporto sull'incidente all'autorità competente, indicando la natura dell'incidente, le misure adottate a seguito dell'incidente e le iniziative adottate per evitare il ripetersi di tali incidenti."*
[524] Art. 19 par. 1 DORA per quanto concerne gli obblighi di notifica di "gravi incidenti ITC"; par. 2 per quanto concerne invece la notifica volontaria delle "minacce informatiche significative".
[525] Art. 23 par. 1 per quanto concerne l'obbligo di segnalazione degli "incidenti significativi"; si veda invece il par. 2 per quanto concerne le "minacce informatiche significative".
[526] EUROPEAN SECURITIES AND MARKETS AUTHORITY. (2015*).* Final report: Draft regulatory and implementing technical standards MiFID II/MiFIR (ESMA/2015/1464, p. 203).

monitora l'accesso ai sistemi informatici al fine di garantire la tracciabilità in ogni momento".[527]

La formulazione del paragrafo 5 riprende quanto già esplicitato al paragrafo 1 ("*efficace gestione dell'accesso e dell'identità*") e ne declina il contenuto secondo una procedura a carattere operativo che l'impresa sarà tenuta a adottare.

In particolare, occorre evidenziare il compito dell'impresa di identificare "*tutti coloro che dispongano di diritti di accesso critici ai sistemi informatici"*. Tale enunciato lascia aperte alcune perplessità.

In primo luogo, non sono richiamate in modo espresso le "reti"[528] e ciò potrebbe indurre gli operatori a sottovalutare l'importanza delle medesime, che, come verrà attenzionato, possono costituire una rilevante superficie di attacco.

In secondo luogo, è dubbio se il termine "sistemi informatici" debba interpretarsi in senso assoluto, ossia riferito a tutti i sistemi informatici dell'impresa ovvero, in senso restrittivo, riferito alle sole infrastrutture che consentono l'operatività della macchina algoritmica. Sul punto si ritiene preferibile la seconda interpretazione in virtù del fatto che la disposizione è contenuta in un regolamento delegato volto a specificare la disciplina della negoziazione algoritmica.

In terzo luogo, manca una definizione di cosa si debba intendere per accesso "critico". In proposito si può prospettare una duplice lettura: secondo una prima interpretazione "critico" potrebbe riferirsi a quell'accesso che è tale in relazione all' oggetto del medesimo, e dunque riferito ai sistemi e alle infrastrutture direttamente funzionali al *trading* algoritmico ("sistemi critici"). Secondo una seconda interpretazione, il termine "critico" potrebbe invece alludere alle conseguenze che discendono dall' accesso medesimo, in altre parole sarebbe critico ogni accesso che conferisca una posizione da cui è possibile di incidere in modo significativo sulla confidenzialità, integrità, disponibilità dei sistemi informatici dell'impresa.

---

[527] Art. 18 par. 5 RTS 6.

[528] Il Considerando 2 del medesimo regolamento, tuttavia, afferma: "*le imprese di investimento dovrebbero considerare tutti i rischi che potrebbero compromettere gli elementi essenziali del sistema di negoziazione algoritmica, inclusi i rischi connessi con l'hardware, il software e le linee di comunicazione associate che l'impresa utilizza per l'attività di negoziazione*".

Tale seconda impostazione appare preferibile, poiché adottando la prima interpretazione, il legislatore avrebbe dovuto verosimilmente disporre a carico dell'impresa algoritmica l'obbligo di individuare le infrastrutture *critiche* impiegate e una simile disposizione non si riscontra nel testo dell'articolo in esame.

L'impresa, una volta individuati i titolari di accessi critici è tenuta a limitarne il numero e monitore il loro accesso, al fine di garantirne la tracciabilità in ogni momento. Ne consegue che la scelta del legislatore UE è volta a proteggere i sistemi di *trading* da compromissioni "interne" (le c.d. *insider threat*) intendendosi quelle perpetrate da membri del personale che, con intento malevolo, si siano determinati ad alterare il funzionamento di suddetti sistemi abusando delle loro credenziali di accesso.

In conclusione, si potrebbe avanzare la seguente considerazione: la gestione della politica degli accessi appare una scelta molto saggia del legislatore in quanto permette una *governace* efficace dell'intera infrastruttura tecnologica, in linea con l'approccio di "gestione del rischio" che anima sia le disposizioni della MiFID II sia quelle del Reg. DORA. Tuttavia, nella norma in parola manca un riferimento esplicito all' individuazione e classificazione della componentistica ICT che invece si rinviene nel Regolamento n. 2554 del 2022 (Reg. DORA).[529] La formulazione di un analogo obbligo di identificazione anche nell' articolo 18 (RTS 6) avrebbe probabilmente reso più agevole la stessa politica degli accessi *critici* poiché la tracciabilità dell'accesso presuppone che sia previamente chiaro a quali *asset* esso si riferisca.

[529] Art. 8 Reg. DORA.

3.7 LE MINACCE INFORMATICE E IL TRADING ALGORITMICO

3.7.1 PREMESSA

Il settore finanziario costituisce uno dei principali obiettivi delle minacce informatiche[530] a causa dell'alto valore dei dati finanziari e dei potenziali guadagni che, in termini economici, ne possono derivare.[531]

Secondo il rapporto dell' Agenzia Europea per la Cybersicurezza (ENISA) denominato "*ENISA threat landscape 2024*"[532] i principali autori di minacce informatiche risultano rispettivamente essere: gli *state nexus actors,* ossia soggetti legati o riconducibili a stati, tendenzialmente orientati al *cyber* spionaggio; i *cyber* criminali, ovvero gruppi criminali che svolgono attività informatiche illecite con finalità prevalentemente economiche; gli *Hacktivists*, vale a dire attori motivati da cause politiche e/o sociali; ed infine, gli *insider actors,* questi ultimi intesi come tutti coloro che, operando all'interno di un'organizzazione e disponendo di accessi legittimi a sistemi e dati, possono abusarne in modo doloso, ovvero determinare incidenti per negligenza o errore.

Inoltre, secondo uno studio condotto dalla medesima agenzia (ENISA), [533] nel periodo compreso tra gennaio 2023 e giugno 2024 sono stati registrati, sempre nel settore finanziario, un totale di 488 incidenti, dei quali, 414 hanno colpito organizzazioni o istituzioni operanti all' interno di uno Stato membro, mentre 74 hanno avuto come bersaglio paesi limitrofi. Nel rapporto emerge come le banche e gli istituti di credito risultino essere i soggetti più colpiti (46%) ai quali seguono poi le agenzie governative e

[530] Nel presente paragrafo, con il termine "minacce informatiche" si allude esclusivamente a tutte quelle circostanze che, qualora si realizzino, si traducono in un "attacco informatico". A tal proposito, si ricorda che il Regolamento DORA definisce l'attacco informatico come un "*incidente doloso connesso alle TIC, derivante dal tentativo dell'autore della minaccia di distruggere, rivelare, alterare, disabilitare o utilizzare senza autorizzazione un'attività o un bene, ovvero di accedervi senza autorizzazione*" (art. 3 DORA). Un incidente connesso alle reti e ai sistemi informativi può tuttavia avere anche natura non dolosa; nel presente paragrafo, nondimeno, si terrà conto esclusivamente delle minacce che, per le loro caratteristiche, possono concretamente tradursi in attacchi informatici dolosi.

[531] MAZZA, M., & CAPPELLI, M. (2020). L'impatto del cyber risk sul mercato finanziario: Case studies. GCSEC – Global Cyber Security Center, p. 5.

[532] EUROPEAN UNION AGENCY FOR CYBERSECURITY. (2024). ENISA threat landscape 2024. ENISA, pp. 20–21.

[533] EUROPEAN UNION AGENCY FOR CYBERSECURITY. (2025). ENISA threat landscape: Finance sector (January 2023 to June 2024). ENISA.

le organizzazioni pubbliche attinenti al settore finanziario (13%). Il grafico di seguito conferma l'analisi (Fig. 5).

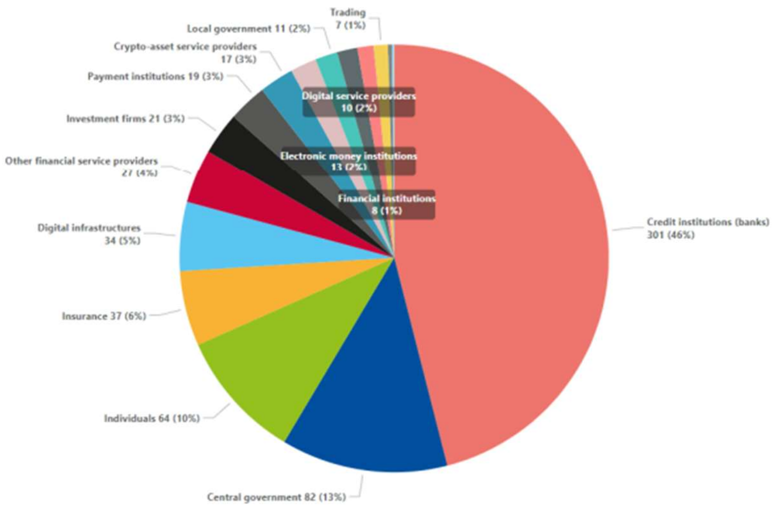

Fig. 5: distribuzione delle minacce informatiche nel settore finanziario (Fonte: Elaborazione su dati ENISA, ENISA Threat Landscape: Finance Sector 2024, European Union Agency for Cybersecurity, 2024).

Posto quindi che il settore finanziario non risulta immune alle minacce informatiche, si premette che, nel prosieguo della trattazione, l'analisi svolta sarà scissa in due parti. *In primis*, verranno attenzionate le minacce informatiche "tradizionali" alle reti e sistemi informativi, che costituiscono l'infrastruttura tecnologica su cui poggia il *trading* ad alta frequenza. *In secundis,* la disamina procederà ad indagare quali siano le possibili e nuove minacce alla sicurezza informatica nei casi in cui un operatore o un *trader* decidessero di impiegare algoritmi avanzati di *machine learning*. Come noto, l'impiego di sistemi AI contribuisce ad incrementare l'efficacia delle operazioni di *trading* ma al contempo ad elevare anche i rischi di minacce ed incidenti informatici verso i suddetti sistemi.

3.7.2 MINACCE INFORMATICHE TRADIZIONALI

Una delle minacce informatiche di natura dolosa che può colpire i sistemi informativi a supporto delle attività di *trading* algoritmico è rappresentata dal *malware.* Con il termine *malware* si allude generalmente a un programma (*software*) progettato con intento malevolo, contenente funzionalità o capacità che possono potenzialmente causare danni, in modo diretto o indiretto, a soggetti o ai loro sistemi informativi.[534]

Un *malware* è tendenzialmente caratterizzato da due componenti – un meccanismo di replicazione (chiamato *dropper*) e un contenuto malevolo (*payload),* quest'ultimo inteso come la parte che realizza in concreto l'effetto dannoso. [535]

Tra le principali categorie di *malware* si ricordano, in particolare, i *virus*, intesi come *software* in grado di replicarsi ogniqualvolta un *file* o programma infetto venga aperto o eseguito dall'utente. Ai *virus* si aggiungono poi i *worms*, che, a differenza dei precedenti, sono in grado di propagarsi in rete in modo automatico, senza che sia necessaria l'esecuzione di un *file* da parte dell'utente.[536] Un dispositivo può poi essere infettato da un *Trojan* (o cavallo di Troia) che, presentandosi apparentemente come un *software* legittimo, consente accessi non autorizzati al *computer* della vittima senza che questa ne sia a conoscenza.[537]

Una volta quindi che il *malware* riesca a penetrare il dispositivo bersaglio, il contenuto malevolo (o *payload*) viene rilasciato. Supponendo che la vittima sia un *computer* di *trading*, un attacco *malware* perpetrato da una impresa concorrente e conclusosi con esito positivo potrebbe condurre alla sottrazione di dati riservati (c.d. *data breach)*, quali ad esempio le strategie di negoziazione contenute nei codici algoritmici ovvero potrebbe alterare il funzionamento stesso dell'algoritmo di negoziazione, con il rischio di generare ordini erronei e idonei ad alterare il mercato (c.d. manipolazione di mercato). Potrebbe verificarsi, altresì, la situazione in cui i dati vengano resi illeggibili mediante un algoritmo crittografico (*encryption*) al fine di chiedere un riscatto: si pensi, ad esempio, ai dati di

---

[534] FINANCIAL STABILITY BOARD. (2023). Cyber lexicon: Updated in 2023. Financial Stability Board.
[535] ANDERSON, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). John Wiley & Sons, p. 713.
[536] BATTELLI, E., & D'IPPOLITO, G. (2025). Compendio di normativa sulla privacy e cybersicurezza 2025. Nel diritto Editore, p. 313.
[537] *Ibidem*.

mercato sulla base dei quali l'algoritmo di *trading* decida se e quali ordini generare. Una tale tipologia di attacco prende il nome di *ransomware* e si svolge secondo tre fasi: in un primo momento il *malware* si introduce nel *computer* bersaglio tramite allegati, *link* dannosi o sfruttando vulnerabilità. Una volta infettato il dispositivo, vi è una seconda fase in cui il *ransomware* "blocca" il *computer* compromesso, criptando i dati al fine di renderli inaccessibili. Da ultimo, il *malware* fa scattare una richiesta di riscatto (*ransom*) necessaria per poter sbloccare i dati criptati.[538] Un attacco *ransomware* costituisce una tra le principali minacce informatiche sui mercati finanziari [539] poiché, se non adeguatamente arginato, è in grado di compromettere per ore, se non giorni, il regolare svolgimento delle negoziazioni di borsa. [540]

Le minacce informatiche non si limitano solamente all'impiego programmi malevoli in grado di compromettere un "sistema informativo" (ad es. un *virus* che infetta un *computer* di *trading*), ma possono ricomprendere altre tipologie di attacchi aventi ad oggetto le "reti" alle quali i sistemi informativi si connettono [541] (si pensi, ad esempio, alle connessioni tra i server di *trading* e i *server* della piattaforma di negoziazione su cui viaggiano gli ordini di borsa).

Data la complessità delle minacce informatiche che potrebbero realizzarsi sulla "rete", si rende necessaria una breve illustrazione di come un *computer* di *trading* "comunichi" con il sistema di abbinamento ordini (*matching engine*) di una piattaforma di negoziazione.[542]

---

[538] CORASANITI, G. (2025). Strategie di contrasto al ransomware e nuove frontiere della criminalità informatica. *Il diritto dell'informazione e dell'informatica*, 41(1), p. 20.

[539] MCCARTHY, J. (2023). Cyber-risks in modern finance: Building operational and regulatory resilience. *Journal of International Banking Law and Regulation*, 38(7), p. 235.

[540] Un esempio su tutti è quello verificatosi il 31 gennaio 2023 quando un attacco *ransomware* ha colpito ION Group, un fornitore di *software* usato da molti intermediari finanziari per gestire e registrare operazioni su derivati, causando un blocco dei servizi e difficoltà diffuse nel processare le operazioni. La ripartenza è stata graduale e, per alcuni operatori, il ritorno alla normalità ha richiesto giorni fino a circa due settimane di attività manuali di recupero.
Sul punto: FUTURES INDUSTRY ASSOCIATION. (2023). FIA Taskforce on Cyber Risk: After Action Report and Findings.

[541] Si ricorda che per "rete" si intende l'insieme dei sistemi che consentono l'instradamento e la trasmissione di segnali tra nodi presenti all'interno della rete stessa.

[542] Si suppone qui che l'impresa di investimento abbia instaurato un collegamento diretto con la piattaforma di negoziazione in quanto ricorre ad un "accesso elettronico al mercato" (DEA). Per tale motivo si giustifica la mancata rappresentazione nell' immagine di un intermediario. Si rinvia al cap. 1 par. 1.3 per la definizione di *direct electronic access*.

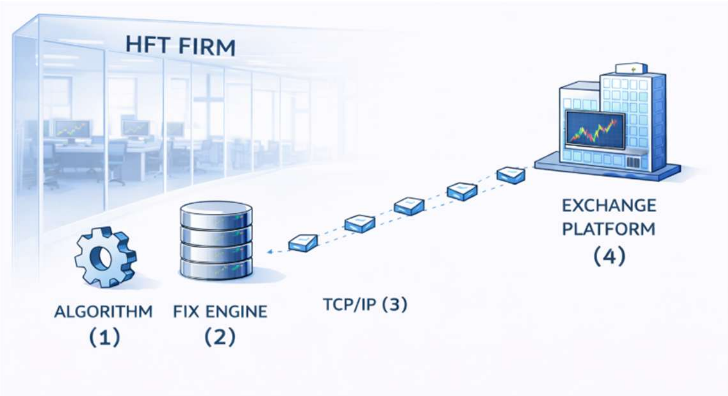

Fig. 6: L' immagine in sovrimpressione, seppur in maniera semplificata e schematica, rappresenta il modo con cui un server di una HFT firm instaura una connessione con una piattaforma di negoziazione al fine di poter inviare ordini di borsa.

Ogni ordine di borsa generato da un algoritmo deve essere in grado di raggiungere il meccanismo di abbinamento degli ordini collocato presso la sede di negoziazione onde poter essere validamente unito con un altro di segno opposto. Al fine di conseguire ciò, i sistemi informatici, rispettivamente quelli situati presso l'impresa di investimento algoritmica e quelli collocati presso la piattaforma di negoziazione, sono interconnessi tramite reti e utilizzano modalità di comunicazione predefinite. In questa prospettiva, anche la singola "istruzione di compravendita" da inviare al mercato è rappresentata in un formato leggibile e comprensibile dal *server* destinatario.[543] Nel *trading* elettronico ciò avviene, di regola, mediante la codifica dell'ordine in un messaggio elettronico conforme allo *standard* FIX (*Financial Infomation eXchange*),[544] il quale funziona come un *linguaggio comune dei sistemi e delle piattaforme di trading, consentendo loro di comunicare in modo uniforme e standardizzato.* [545] La trasformazione dell'istruzione in

[543] HILLS, B. (2000). Common message standards for electronic commerce in wholesale financial markets. *Bank of England Quarterly Bulletin*, 40(3), p. 275.
(Finding that: "*Such automation can be achieved only if the two applications are connected via an electronic network and, in effect, speak the same language. In other words, it requires common message standards for the electronic exchange of transaction data*").
[544] Il FIX (*Financial Information eXchange*) Protocol è uno *standard* aperto, gratuito e non proprietario di messaggistica che funge da linguaggio comune dei mercati finanziari, utilizzato da intermediari *buy-sid*e e *sell-side*, sedi di negoziazione e anche autorità di vigilanza per comunicare elettronicamente le informazioni di trading; esso consiste in una serie di specifiche di messaggistica impiegate nelle comunicazioni relative alle negoziazioni.
Si veda: FIX TRADING COMMUNITY. (n.d.). What is FIX? (Retrieved January 8, 2026).
[545] KOGNOLE, S. (2024). FIX protocol: The backbone of financial trading. *International Journal of Computer Science & Information Technology*, 16(4), p. 99.. (finding that: "*This is something like that*

un messaggio FIX è effettuata da un apposito *software* (*FIX engine*), che costruisce il messaggio secondo precise regole sintattiche e standardizzate. [546]

Una volta generato, il messaggio FIX viene immesso sulla rete e indirizzato verso la sede di negoziazione secondo regole e protocolli che assicurano la trasmissione ordinata e affidabile dei dati. Tendenzialmente tali protocolli sono quelli TCP-IP:[547] il messaggio viene prima scomposto in segmenti di testo e successivamente tali segmenti vengono incapsulati in pacchetti IP, che ne curano il successivo instradamento attraverso la rete verso il destinatario. [548] Quando i pacchetti TCP-IP giungono presso i *server* della borsa, il messaggio viene ricostruito dai sistemi informatici del destinatario e l'ordine così ottenuto viene immesso nel sistema di abbinamento.

Un siffatto e complesso meccanismo di reti e comunicazioni può costituire un bersaglio perfetto per eventuali attacchi informatici. Ad esempio, un attore malevolo potrebbe realizzare quello che in gergo tecnico viene definito un *man in the middle* (*MiMT*), ossia un attacco in cui un terzo si colloca tra due parti che stanno comunicando, al fine di intercettare e/o alterare i dati che transitano tra di esse.[549] Nel caso di una connessione per il *trading* non adeguatamente protetta (ad esempio, conversazioni con messaggi non cifrati tramite VPN o TLS)[550], un terzo potrebbe intercettare il contenuto degli ordini-

because FIX is a protocol that acts more like a language of trading systems/platforms in trades distinctively").

[546] Ciascun messaggio FIX risulta essere composto da coppie di "tag-valore" (*tag-value pairs*), in cui a ciascun numero (*tag*) è associato uno specifico valore, che esprime il contenuto informativo del campo corrispondente. Ad esempio, la coppia "55=AAPL" indica lo strumento finanziario oggetto dell'ordine (tag 55: Symbol; valore: AAPL); "38=100" indica la quantità dello strumento finanziario che si vuole vendere o comprare (tag 38: OrderQty; valore: 100).

[547] Fix Trading Community, la società che controlla e sviluppa le specifiche del protocollo, sul proprio sito riconosce espressamente che "*the FIX session does not require a specific transport layer, although TCP/IP is widely used and is a de facto standard transport layer for FIX sessions. TCP/IP provides an ordered reliable delivery of a stream of bytes during the life of the TCP connection. The FIX session processor reads this stream identifying FIX message boundaries*.").

Si veda in proposito: FIX TRADING COMMUNITY. (2020). FIX session layer online (Technical standard—Errata November 2020). https://www.fixtrading.org/standards/fix-session-layer-online

[548] Il protocollo TCP/IP è l'insieme di regole che consente a due sistemi di scambiarsi dati su una rete ed è alla base del funzionamento della rete Internet. IP identifica e instrada i pacchetti, contenenti i dati e le informazioni, verso l'indirizzo di destinazione, mentre TCP stabilisce la connessione tra le applicazioni (il noto "*three-way handshake*" SYN, SYN-ACK, ACK) e garantisce che i pacchetti contenenti i dati arrivino completi e nell'ordine corretto.

[549] CONTI, M., DRAGONI, N., & LESYK, V. (2016). A survey of man-in-the-middle attacks. *IEEE Communications Surveys & Tutorials*, 18(3), pp. 2027–2051.

[550] La VPN (*Virtual Private Network*) è collegamento "privato" su Internet che crea un canale protetto (di solito cifrato) tra due punti; il TLS (*Transport Layer Security*) è invece un protocollo che cifra e protegge la comunicazione tra un client e un server, garantendo riservatezza e integrità dei dati scambiati.

messaggio al fine di carpirne le informazioni ovvero modificarne il contenuto o i parametri rilevanti. Potrebbe, altresì, verificarsi la situazione in cui l'attore malevolo decida introdurre ritardi nei tempi di consegna dei pacchetti TCP-IP alla piattaforma di negoziazione o, addirittura, dirottare il traffico verso altre destinazioni (tecnica nota come *hijacking*).[551]

Esiste, infine, anche la possibilità che l'attore malevolo inserisca nelle linee di comunicazione un numero elevatissimo di messaggi consistenti, ad esempio, in *market data* (*packet flood*).[552] In una tale situazione, i *server* dell' algoritmo di *trading* vedrebbero giungere in ingresso un traffico di rete eccessivo ed inaspettato che, qualora non efficacemente gestito, potrebbe portare al collasso del meccanismo di funzionamento dell' algoritmo, con conseguenze imprevedibili sui mercati.[553] Un simile attacco prende il nome di *denial of service* (DoS) o *distributed denial of service* (DDoS) e consiste in azioni ripetute volte a *esaurire le risorse del servizio oppure sovraccaricare i componenti dell'infrastruttura di rete*[554] con l'obiettivo ultimo di rendere indisponibile un sistema.[555]

3.7.3 MINACCE INFORMATICHE E INTELLIGENZA ARTIFICIALE

La trattazione del rapporto che lega sicurezza informatica e intelligenza artificiale, comprese le relative implicazioni che ne discendono, è molo amplia e complessa. Una analisi sistematica esorbita ed eccede sicuramente lo scopo e l'oggetto della presente ricerca incentrata, invero, sulle minacce informatiche ai sistemi AI qualora questi siano "incorporati" all' interno delle infrastrutture di *trading*.

---

551 ANDERSON, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). John Wiley & Sons, p. 703.
552 DEMARCO, D. (2012). Exploiting Financial Information Exchange (FIX) Protocol? (GIAC GCIH Gold Certification paper). SANS Institute / GIAC, p. 13.
553 Un esempio di attacco informatico DOS più rilevante è quello verificatosi alla borsa neozelandese (NZX), che nel 2020 fu colpita da ripetuti attacchi DDoS volti a compromettere la disponibilità dei propri servizi informatici. Tali attacchi resero indisponibili infrastrutture essenziali per il funzionamento del mercato, inducendo l'operatore a sospendere le negoziazioni per alcuni giorni.
Si veda in proposito: FINANCIAL MARKETS AUTHORITY. (2021). Market operator obligations targeted review – NZX: Findings from the FMA's targeted review of whether NZX is meeting its licensed market operator obligations. https://www.fma.govt.nz/assets/Reports/Market-Operator-Obligations-Targeted-Review-NZX.pdf.
554 EUROPEAN UNION AGENCY FOR CYBERSECURITY. (2025). ENISA threat landscape: Finance sector (January 2023 to June 2024). ENISA, p. 11.
555 GCSEC. (2020). L'impatto del cyber risk sul mercato finanziario: Case studies. GCSEC, p. 20.

Tuttavia, è degno di nota menzionare come il rapporto tra *cybersecurity* ed AI venga tradizionalmente inteso secondo un approccio "bidirezionale" (*dual use*) come di seguito meglio descritto.[556]

In primo luogo, i sistemi AI costituiscono preziose risorse per contrastare le minacce informatiche e rafforzare i relativi strumenti.[557] Si pensi, ad esempio, al rilevamento automatico di possibili intrusioni (IDS) ovvero all' individuazione, tramite il *machine learning,* di anomalie nel traffico di rete (*outlier detection*), di vulnerabilità sconosciute agli sviluppatori (le c.d. vulnerabilità *zero-day*)[558] o di *malware* mai visti prima.[559] Un sistema intelligente, data poi la sua capacità di autoapprendimento, potrebbe rilevare minacce informatiche avanzate e prolungate (APT, *advanced persistent threat*) [560] ovvero, tramite processi iterativi di aggiornamento, mantenersi al passo con l'evoluzione delle minacce stesse.

In secondo luogo, l'AI potrebbe costituire essa stessa una minaccia in quanto verrebbe impiegata per ampliare le capacità offensive degli attaccanti.[561] In questa prospettiva, è ragionevole supporre come algoritmi di *machine learning* possano essere impiegati per scansionare le difese di un sistema informatico al fine di individuarne le vulnerabilità e penetrarlo più facilmente ovvero per costruire l'infrastruttura di funzionamento di *malware* adattivi, capaci di mutare all' occorrenza. [562]

---

[556] CORASANITI, G. (2025). Sicurezza informatica e intelligenza artificiale: Rischio e resilienza nello spazio giuridico europeo. Giappichelli, Torino, p. 82.

[557] FIORIGLIO, G. (2025). Intelligenza artificiale e cibersicurezza: profili informatico-giuridici, fra vulnerabilità delle macchine e delle persone. *I-lex*, 18(2), p. 7.

[558] Una vulnerabilità *zero-day* viene definita come "*una vulnerabilità precedentemente sconosciuta all'interno di un sistema informativo*." Si veda: FINANCIAL STABILITY BOARD. (2023). Cyber lexicon: Updated in 2023. Financial Stability Board.

[559] OLOYEDE, J. (2024). AI-driven cybersecurity solutions: Enhancing defense mechanisms in the digital era (Manuscript).

[560] Per APT si intende: "*Un attore di minaccia che possiede livelli sofisticati di competenza e risorse significative, che gli consentono di creare opportunità per conseguire i propri obiettivi utilizzando molteplici vettori di attacco. La minaccia avanzata e persistente (advanced persistent threat): (i) persegue i propri obiettivi ripetutamente per un periodo di tempo prolungato; (ii) si adatta agli sforzi dei difensori volti a contrastarla; e (iii) è determinata a portare a termine i propri obiettivi*".
Si veda: FINANCIAL STABILITY BOARD. (2023). Cyber lexicon: Updated in 2023. Financial Stability Board.

[561] Si veda nota n. 492, pg. 7.

[562] MINNELLA, V. (2025). Cybersecurity e intelligenza artificiale: Alleanza indispensabile per la sicurezza del futuro. *Rassegna dell'Arma dei Carabinieri*, (1), p. 99.

L'analisi sino ad ora condotta ha permesso di configurare l'AI in rapporto alla *cybersecurity* come uno "strumento" (*tool*) utilizzabile sia per difendere sia per attaccare una rete o sistema informativo; tuttavia, l'intelligenza artificiale può costituire anche un obiettivo (*target)* di attacco da parte di attori malintenzionati.[563]

L' eventualità che gli stessi algoritmi di *machine learning* diventino bersagli di minacce informatiche ad opera di *competitors* rivali costituisce, soprattutto nel settore del *trading* algoritmico,[564] una concreta possibilità. [565]

In questa prospettiva, rileva *in primis* il c.d. *data poisoning* (o avvelenamento dei dati di addestramento). Prima che un algoritmo di *machine learning* venga impiegato a livello operativo, è necessario che il medesimo sia sottoposto ad una preventiva fase di "addestramento", detta *training*; in tale fase vengono prima raccolti una serie di dati (nel caso dell'AT o HFT i dati coincideranno con quelli di mercato) che andranno a comporre il *dataset* di addestramento e successivamente, sul medesimo, l'utente procederà allenare il modello. Una volta concluso l'addestramento, l'algoritmo verrà quindi sottoposto a nuovi dati mai visti prima, i c.d. *input* (nel caso di AT e HFT gli *input* saranno i dati di mercato correnti e attuali) al fine di adempiere correttamente la funzione assegnata.[566] In un siffatto contesto, è possibile ipotizzare che un terzo (ad esempio una HFT *firm* rivale) decida di manipolare volutamente i set di addestramento, inserendo informazioni errate o

---

[563] EUROPEAN UNION AGENCY FOR CYBERSECURITY. (2024). ENISA threat landscape 2024. ENISA, p. 14.

[564] REDDY, R. K. V., KHAN, A. N., GARG, S., G, N. K., KASIREDDY, L. C., & DAYALAN, P. (2025). Cybersecurity risks in real-time stock market analytics and digital marketing campaigns. *Journal of Informatics Education and Research*, 5(1), p. 3656.
(Finding that: "*Financial institutions are seriously threatened by market manipulation techniques as pump-and-dump schemes, high-frequency trading (HFT) attacks, and data poisoning in prediction models. Stock trading platforms are vulnerable to hacks that could upset market stability and erode investor confidence in the absence of a strong cybersecurity policy*").

[565] YUSSUF, M. (2025). Advanced cyber risk containment in algorithmic trading: Securing automated investment strategies from malicious data manipulation. *International Research Journal of Modernization in Engineering Technology and Science*, p. 884.
(Finding that: "*With the increasing digitization of financial markets, algorithmic trading systems have become prime targets for cyber threats. These threats originate from malicious actors aiming to exploit vulnerabilities in trading algorithms, infrastructure, and data feeds to disrupt market operations or manipulate prices*").

[566] CINÀ, A. E., GROSSE, K., DEMONTIS, A., BIGGIO, B., ROLI, F., & PELILLO, M. (2024). Machine learning security against data poisoning: Are we there yet? *Computer*, 57(3), p. 3.

incomplete così da alterare le prestazioni e il comportamento del modello, compromettendone, pertanto, l'accuratezza e l'affidabilità.[567]

In secundis, una ulteriore minaccia connessa ai sistemi di *trading* basati su *machine learning* è rappresentata dagli *adversarial attack* (o attacchi antagonisti).[568] Una siffatta tipologia di attacco, che si svolge durante la fase "operativa" e non già in quella precedente di "addestramento" della macchina (come avviene nel caso di *data poisoning*) ha come obiettivo quello di indurre in errore il modello AI, mediante la somministrazione di *input* errati non percettibili da operatori umani in modo che l'algoritmo produca predizioni errate ovvero effettui condotte inattese.

Un classico esempio di attacco antagonista è quello connesso ai veicoli a guida autonoma, in cui un mutamento impercettibile della grafica dei segnali stradali può indurre il modello a classificare erroneamente un segnale di stop.[569] Tuttavia, qualora tale pratica si verificasse nel settore del *trading* algoritmico, un attacco antagonista comporterebbe non solo *vulnus* alla sicurezza e all'integrità dei sistemi informatici interessati, ma sarebbe potenzialmente idoneo a configurare anche una forma di manipolazione di mercato.[570]

Invero, l'attore malevolo, attraverso l'inserimento e la cancellazione strategica di ordini, che potrebbe qualificarsi alla stregua di una manipolazione di mercato, andrebbe ad alterare lo stato del libro degli ordini (*order book*)[571] ingannando quindi l'algoritmo di negoziazione e spingendolo ad eseguire operazioni erronee ovvero a manipolare a sua volta il mercato, con l'effetto di generare perdite significative e instabilità.[572]

---

[567] FIORIGLIO, G. (2025). Intelligenza artificiale e cibersicurezza: profili informatico-giuridici, fra vulnerabilità delle macchine e delle persone. *I-lex*, 18(2), pp. 7–8.

[568] FAGHAN, Y., PIAZZA, N., BEHZADAN, V., & FATHI, A. (2020). Adversarial attacks on deep algorithmic trading policies. arXiv.

[569] EYKHOLT, et AL. (2018). Robust physical-world attacks on deep learning models. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*.

[570] SHIMAO, et AL. (2025). Adversarial attacks on machine learning-driven high-frequency trading models., p. 2.
(Finding that: "*When applied to HFT, this technique constitutes a new and sophisticated form of market manipulation. By strategically placing or canceling small orders, a malicious actor could subtly alter the state of the limit order book (LOB)—a primary input for many HFT models—and trick a model into executing suboptimal trades, potentially triggering significant losses or market instability*").

[571] Il libro degli ordini costituisce una fondamentale fonte di input per i sistemi di negoziazione ad alta frequenza.

[572] Sul punto si consulti anche: GOLDBLUM, M., SCHWARZSCHILD, A., PATEL, A. B., & GOLDSTEIN, T. (2021). Adversarial attacks on machine learning systems for high-frequency trading (arXiv:2002.09565v4). arXiv.

VALUTAZIONI

3.8 DE IURE CONDITO

L'analisi complessiva della normativa *cyber* europea ed italiana, compresa quella riguardante le imprese di investimento algoritmiche, permette di mettere in luce alcuni aspetti di centrale rilevanza.

In primo luogo, la NIS II, il regolamento DORA e l'art. 18 RTS 6 testimoniano quanto sia importante per il singolo operatore economico sviluppare una politica interna di gestione dei rischi informatici. Ciò implica che la *cybersecurity* non sia più una materia riservata esclusivamente ad un ufficio o responsabile IT ma interessi e animi l'intera organizzazione, a partire dagli organi gestori e dai Consigli di amministrazione.

In questa prospettiva, si comprende meglio la disposizione contenuta all'art. 5 Reg. DORA che richiede ai membri dell'organo di gestione dell'entità finanziaria di *mantenere attivamente aggiornate conoscenze e competenze adeguate per comprendere e valutare i rischi informatici e il loro impatto sulle operazioni dell'entità finanziaria, anche seguendo una formazione specifica su base regolare, commisurata ai rischi informatici gestiti*. [573]

La circostanza che vengano avviati processi di formazione specifici risponde poi alla più ampia necessità di una maggiore consapevolezza circa l'importanza della sicurezza informatica, un tema che, trasversalmente, deve interessare non solo la singola impresa ma anche l'intera generalità dei consociati. Purtroppo, l'errore tipico al quale spesso si assiste e che molti attori economici e le singole persone fisiche fanno è quello di considerare il rischio cibernetico come *rischio importante, molto importante, forse il più importante, ma, esclusivamente, come un banale rischio informatico.*[574] Tuttavia, come è stato ampiamente illustrato nel presente elaborato, quel "banale rischio informatico" è capace di propagarsi in maniera trasversale nell' intera azienda, ostruendone i circuiti

[573] Art. 5 par. 4 DORA.
[574] BARBARA, G. (2022). La cybersecurity: minacce, evoluzione normativa, corporate governance e nuove prospettive. *Corporate Governance*, (4), p. 514.

produttivi e compromettendone la stessa funzionalità, con ricadute, specie nel settore del *trading* ad alta frequenza, potenzialmente sistemiche.

In secondo luogo, dall'analisi della normativa *cyber* concernente le imprese di investimento algoritmiche emergono alcune perplessità. A tal proposito, sembra idoneo a destare difficoltà interpretative l'obbligo posto in capo all' impresa che effettua *trading* algoritmico di notificare agli organi competenti gli incidenti che dovessero verificarsi. Tale obbligo si rinviene in due diverse fonti normative.

In primis, rileva l'art. 19 Reg. DORA, *lex specialis* della NIS 2, che obbliga in generale ogni ente finanziario, quindi verosimilmente anche una impresa di investimento algoritmica, a *segnalare alle autorità competenti i gravi incidenti ITC.*

A questa disposizione si aggiunge, *in secundis*, quella contenuta all'interno dell'art. 18 del regolamento delegato MiFID II (RTS 6) che prescrive per l'impresa di investimento algoritmica *di informare immediatamente l'autorità competente di eventuali violazioni rilevanti delle sue misure di sicurezza fisica o elettronica.*

Dalla lettura sinottica delle disposizioni in esame emerge, in primo luogo, la difficoltà interpretativa nel comprendere se tali formulazioni si riferiscano a uno stesso incidente ovvero a due aventi natura differente

In proposito, se dalla definizione di "*gravi incidenti TIC*"[575] il legislatore ha inteso riferirsi ad un incidente che colpisce le risorse TIC (ossia risorse *hardware* e *software* presenti nei sistemi informatici e di rete) e che a sua volta ha un impatto negativo ("avverso") sui sistemi informatici e di rete necessari per l'attività dell' ente, dubbi sussistono, invece, in relazione al termine "*violazioni rilevanti delle misure di sicurezza fisica ed elettronica*", utilizzato dal legislatore all'interno dell'art. 18 RTS 6.

Sul punto si può rilevare come il termine impiegato sia formulato in termini piuttosto ampi e generici, che non trovi un analogo all'interno del Reg. DORA e che, inoltre, il legislatore non abbia nemmeno fornito, per esso, una specifica definizione normativa.

---

[575] Si ricorda che l'art. 3 punto n. 10 definisce "grave incidente TIC": "*un incidente connesso alle TIC che ha un impatto avverso sui sistemi informatici e di rete a supporto delle funzioni essenziali o importanti dell'entità finanziaria".*

Parrebbe che in tale ipotesi il legislatore abbia inteso riferirsi a due distinte tipologie di incidenti e che, pertanto, sorgano differenti obblighi di notifica in capo all'impresa di investimento.

In particolare, nel caso di "*gravi incidenti TIC*" l'obbligo di notifica sorge nella misura in cui l'incidente abbia inciso sull' infrastruttura tecnologica che permette lo svolgimento delle "funzioni essenziali o importanti" [576] dell'ente. In altre parole, l'impatto dell'incidente è di una gravità tale da compromettere l'operatività stessa dell'azienda: si pensi, ad esempio, ad un attacco *ransomware* che blocchi completamente i *server* di *trading* impedendo loro di funzionare ovvero a un attacco *man in the middle* in cui un terzo antagonista invii una elevatissima ed inaspettata quantità di messaggi ai *server* dell'impresa HFT deputati alla ricezione dei dati di mercato, compromettendone così l'intero funzionamento (DDOS *attack*).

Diversa è la valutazione da farsi nel caso dell'art. 18 (RTS 6). In tal caso, il legislatore sembra aver "anticipato" tale obbligo di notifica, in quanto il medesimo è idoneo a sorgere in presenza di una compromissione significativa dei presidi di sicurezza ("*violazioni rilevanti delle misure di sicurezza fisica ed elettronica*"), a prescindere dal fatto che alla violazione abbia fatto seguito un impatto avverso sulla continuità operativa dell'impresa. A titolo di esempio, si pensi ad un *Trojan* che riesca a penetrare i sistemi informatici dell'impresa al fine di sottrarre dati (ad es. le strategie di negoziazione), ma senza alterarne le funzioni essenziali o importanti.

Dall'analisi complessiva delle disposizioni sembra quindi possibile concludere che, nel caso di incidenti aventi ad oggetto i sistemi informatici e di rete di una impresa HFT, si assista a un duplice e differente ordine di obblighi di notifica per il soggetto coinvolto. Tali notifiche, si specifica, devono essere indirizzate all'Autorità competente di settore (Consob).

[576] Il DORA definisce "funzione essenziale o importante": "*una funzione la cui interruzione comprometterebbe sostanzialmente i risultati finanziari di un'entità finanziaria o ancora la solidità o la continuità dei suoi servizi e delle sue attività, o la cui esecuzione interrotta, carente o insufficiente comprometterebbe sostanzialmente il costante adempimento, da parte dell'entità finanziaria, delle condizioni e degli obblighi inerenti alla sua autorizzazione o di altri obblighi previsti dalla normativa applicabile in materia di servizi finanziari*" (Art. 3 punto 22 Reg. DORA).

In secondo luogo, un ulteriore aspetto che potrebbe essere idoneo a destare perplessità riguarda il caso in cui l'impresa algoritmica sia anche un soggetto rientrante nel c.d. "Perimetro di Sicurezza Nazionale Cibernetica". In tal caso, l'impresa è tenuta, ai sensi dell'art. 1 comma 3 lett. *a,),* a notificare ogni *incidente avente impatto su reti, sistemi informativi e servizi informatici al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT).*

Quanto alla natura dell'incidente, la norma sembra essere sufficientemente chiara da non lasciare spazio ad interpretazioni. Invero, rileverebbe, ai fini della notifica, ogni incidente che dovesse verificarsi alle reti, sistemi informativi e servizi informatici *da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello stato e dal cui malfunzionamento, interruzione o utilizzo improprio possa derivarne un pregiudizio per la sicurezza nazionale*.

Tuttavia, l'aspetto controverso risiederebbe nel soggetto destinatario della comunicazione: se l'impresa di investimento algoritmica è allo stesso tempo Soggetto Perimetro, la medesima potrebbe vedersi costretta a segnalare l'incidente, rispettivamente, allo CSIRT Italia, ai sensi del decreto legge 21 settembre 2019 n. 105 (PSNC) e alla stessa Consob, in quanto Autorità competente, ai sensi del Reg. DORA ovvero ai sensi dell'art. 18 reg. delegato RTS 6. Come è agevole comprendere, un siffatto complesso meccanismo di notifiche è idoneo a generare un carico procedurale notevole che potrebbe appesantire la stessa attività di contrasto all'attacco informatico, che, per sua natura, richiede un immediato e pronto intervento.

In conclusione, sembra opportuno evidenziare come la normativa concernente la sicurezza informatica rilevante per la negoziazione algoritmica sia connotata da una non perfetta chiarezza di talune disposizioni e da obblighi tra loro sovrapposti. Una siffatta circostanza risulta essere problematica poichè potrebbe esporre le imprese a incertezze circa la qualificazione degli incidenti, la determinazione delle soglie di notifica e a plurime comunicazioni alle autorità.

In questa prospettiva, si sottolinea come l'idea perseguita dal legislatore UE sia stata quella di stimolare le imprese nel cercare di "governare" i rischi derivanti dalle tecnologie impiegate (risorse TIC, reti e sistemi informativi) onde poterne garantire un uso sicuro ed affidabile. Tuttavia, un siffatto approccio ha portato le istituzioni ad emanare, nel corso del tempo, normative sempre più numerose, specifiche e stratificate, tali da rendere necessaria la presenza di esperti del diritto. [577]

Una siffatta difficoltà non dovrebbe essere sottovalutata: la maggior parte degli attacchi informatici oggigiorno coinvolge sempre più piccole e medie imprese (si stima circa il 75% degli attacchi) [578] che spesso dispongono di poche risorse e personale poco qualificato. Pertanto, in una tale situazione, una complessa architettura normativa come quella ad oggi vigente potrebbe porre significative discriminazioni a livello competitivo in quanto solamente le imprese più floride e strutturate sarebbero in grado di far fronte agli elevati costi di *compliance* e ad investimenti in misure di sicurezza all' avanguardia.

3.9 DE IURE CONDENDO

Nel presente capitolo è stato più volte menzionato il termine di *security by design,* con ciò intendendosi la predisposizione di misure di sicurezza all'interno di un sistema *hardware* o *software* fin dalla loro ideazione e progettazione. In altre parole, il legislatore eurounitario ha inteso la cybersicurezza come un requisito prioritario del singolo prodotto sin dalle primissime fasi di vita e non come un elemento da aggiungere *a posteriori,* una volta realizzato.[579]

Parallelamente, nel presente elaborato, è stato avanzato anche il concetto di "ecosistema HFT", un termine con cui si intende alludere all'insieme delle risorse *hardware* e *software* che rendono in concreto possibile il funzionamento della negoziazione algoritmica. In sostanza, si tratta di considerare la negoziazione algoritmica da una prospettiva

---

[577] In questo senso, si pensi all' ampio novero di fonti normative UE che sono state analizzate all'interno del presente elaborato.

[578] MELE, S. (22 gennaio 2026). Intervento alla tavola rotonda del convegno *Sicurezza dei dati nelle PMI: strumenti di compliance tra GDPR, NIS 2 e AI Act* (Camera dei Deputati, Sala Matteotti, Roma).

[579] Sotto questo profilo, si pensi al Reg. UE n. 2847 del 2024 denominato *Cyber Resilience Act* che impone ai fabbricanti di prodotti con elementi digitali specifici obblighi nella fase di progettazione, sviluppo e manutenzione in materia di *cybersecurity*; sulla stessa prospettiva, anche il Reg. EU n. 1689 del 2024 noto come AI ACT obbliga i fornitori di sistemi AI ad "alto rischio" a progettare e sviluppare modelli algoritmici il *più resilienti possibile* sia rispetto ad errori, guasti e malfunzionamenti sia rispetto a eventuali manipolazioni esterne (art. 15 AI ACT).

meramente tecnica, ossia, come il risultato finale di una complessa attività svolta da un insieme di "reti" e "sistemi informativi" al cui interno sono presenti e interagiscono tra loro diverse risorse fisiche (ad esempio, gli impianti *hardware* per i sistemi di *co-location*) e logiche (ad esempio, l'algoritmo di *trading* ovvero il FIX *engine*).

Nel loro complesso, tali risorse (o "prodotti TIC") risultano essenziali per il funzionamento complessivo della macchina. Tuttavia, da una eventuale loro alterazione si potrebbero generare effetti negativi per l'attività di negoziazione e, di conseguenza, ne risentirebbe anche lo stesso mercato. Pertanto, risulta essenziale che tali prodotti TIC funzionino in modo corretto e sicuro.

In ragione di ciò, sarebbe opportuno introdurre, per le imprese di investimento algoritmiche, l'obbligo di avvalersi di prodotti TIC certificati a livelli minimi di affidabilità e rilasciati in conformità a un Sistema europeo di certificazione della cibersicurezza.

L'obbligo sopra prospettato potrebbe discendere dal seguente quadro normativo.

Il Reg. (EU) n. 881 del 2019 noto come *Cybersecurity Act* (di seguito CSA) ha introdotto e definito un "Quadro europeo di certificazione della sicurezza cibernetica" al fine di stabilire i principali requisiti orizzontali per i "Sistemi europei di certificazione della cibersicurezza"[580].

In altre parole, l'obiettivo che il legislatore UE ha inteso perseguire con tale normativa, consiste nella elaborazione di un assetto normativo (denominato "Quadro europeo di certificazione della sicurezza cibernetica") all'interno del quale definire regole comuni circa l'organizzazione della certificazione di prodotti, servizi e processi TIC[581] al fine di aumentare tanto il grado di fiducia dei medesimi, quanto evitare il proliferare di sistemi di certificazione nazionali confliggenti e sovrapposti.[582]

[580] Per "Sistema europeo di certificazione della sicurezza informatica" si intende "una serie completa, di regole, requisiti tecnici, norme e procedure stabiliti a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti TIC, servizi TIC e processi TIC" (art. 2 punto n. 9 CSA).
[581] Considerando 66 CSA.
[582] Considerando 69 CSA.

All'interno di questo "Quadro europeo", il legislatore ha quindi attribuito alla Commissione UE la facoltà di adottare, sulla base di una "proposta di sistema" elaborata dall' ENISA, i c.d. "Sistemi europei di certificazione della cibersicurezza" (di seguito denominati come "Sistemi");[583] Tali Sistemi consistono in una *serie di regole, requisiti tecnici, norme e procedure stabilite a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti, servizi e processi ITC*.[584] In altre parole, si tratta di veri e propri schemi di regole che consentono di ottenere un certificato europeo ufficiale per i prodotti, servizi e processi ITC.

Un "Certificato europeo di cibersicurezza"[585] attesta, pertanto, che un determinato prodotto, servizio o processo TIC[586] è stato sottoposto, con esito positivo, a una "valutazione di conformità"[587] operata da un soggetto terzo indipendente denominato "organismo di valutazione della conformità",[588] atta a verificare che il medesimo rispetti le specifiche tecniche[589] di cybersicurezza stabilite all'interno del "Sistema" ovvero da esso richiamate.[590] [591]

---

[583] Art. 49 par. 7 CSA.
[584] Art. 2 punto n. 9 CSA.
[585] L' art. 2 punto n. 11 lo definisce come "*un documento rilasciato dall'organismo pertinente che attesta che un determinato prodotto TIC, servizio TIC o processo TIC è stato oggetto di una valutazione di conformità con i requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione della cibersicurezza*".
[586] Un certificato può attestare anche la conformità dei "servizi" e "processi" ITC, tuttavia, ai fini del presente elaborato l'attenzione verrà rivolta solamente alla certificazione di prodotti ITC.
[587] L' art. 2 punto 17 (CSA) nel definire la "valutazione di conformità" rinvia all'art. 2, punto 12) del Reg. (CE) n.765/2008 che afferma che essa è "*la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo siano state rispettate*".
[588] L' art. 2 punto n. 18 del Reg. CSA definisce tale organo rinviando all'art. 2 , punto n.13) del reg. CE n.765/2008. Tale è l'organo che "*svolge attività di valutazione della conformità, fra cui tarature, prove, certificazioni e ispezioni*".
[589] Per "specifica tecnica" il CSA intende "*un documento che prescrive i requisiti tecnici che un prodotto ITC, un servizio TIC o un processo TIC deve soddisfare, o le relative procedure di valutazione della conformità*" (art. 2 punto n. 20 CSA).
[590] L'art. 54 par. 1 (CSA) afferma che tra gli elementi ricompresi all'interno di un "sistema europeo di certificazione della cibersicurezza" rientrano i "*riferimenti alle norme internazionali, europee o nazionali applicate nella valutazione o, laddove tali norme non siano disponibili o adeguate, alle specifiche tecniche che rispettano le prescrizioni enunciate all'allegato II del Reg. UE n. 1025/2012 oppure, se tali specifiche non sono disponibili, alle specifiche tecniche o ad altri requisiti di cibersicurezza definiti nel sistema europeo di certificazione della cibersicurezza*" (lett. *c*).
[591] Considerando n. 75 CSA che afferma: "*Lo scopo dei sistemi europei di certificazione della cibersicurezza dovrebbe essere quello di assicurare che i prodotti TIC, servizi TIC e processi TIC certificati nel loro ambito siano conformi a determinati requisiti volti a proteggere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati, trasmessi o trattati o delle funzioni di o dei servizi offerti da o accessibili tramite tali prodotti, servizi e processi per tutto il loro ciclo di vita*."

Il suddetto certificato viene rilasciato da un organo competente, denominato "organismo di certificazione" e specifica un "livello di affidabilità" (si prevedono fino a tre livelli di affidabilità: "di base", "sostanziale" o "elevato") [592] che riflette la profondità della valutazione effettuata, calibrata in base al rischio legato all'uso del prodotto TIC,[593] ed esprime il grado di fiducia riponibile in quel determinato prodotto. [594]

Tornando all'ipotesi prospettata in precedenza (l'obbligo per le imprese di investimento algoritmiche di dotarsi di prodotti ITC certificati secondo uno Sistema europeo di certificazione di cibersicurezza), è ragionevole ritenere che l'introduzione di un tale obbligo sia valida e legittima per due ordini di ragioni.

In primo luogo, l'art. 56 par. 2 del Reg. CSA (n. 881/2019) ammette espressamente la possibilità di introdurre certificazioni della cibersicurezza "obbligatorie" nella parte in cui afferma: "*la certificazione della cibersicurezza è volontaria, salvo diversamente specificato dal diritto dell'Unione o degli Stati membri*". Si tratterebbe, pertanto, di introdurre un obbligo normativo in forza del disposto di cui all'articolo 56 par. 2.

In secondo luogo, risulta essere vigente un "Sistema europeo di certificazione" che permette il rilascio di un "Certificato EU di cybersicurezza" relativo a prodotti TIC. Tale Sistema è identificato nel Reg. (UE) di esecuzione n. 482 emanato dalla Commissione europea 31 gennaio 2024 recante "*modalità di applicazione del Reg. (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC)*".[595]

---

[592] Il regolamento CSA prevede che un sistema europeo di certificazione della cibersicurezza debba specificare i livelli di affidabilità per i certificati europei di cibersicurezza. Ciascun certificato, pertanto, può fare riferimento a uno dei livelli di affidabilità, rispettivamente, "di base", "sostanziale" e "affidabilità elevata".

[593] Considerando 78 CSA che afferma "*La scelta della certificazione appropriata e dei relativi requisiti di sicurezza da parte degli utenti dei certificati europei di cibersicurezza dovrebbe fondarsi su un'analisi dei rischi associati all'uso di un prodotto TIC, servizio TIC o processo TIC. Conseguentemente, il livello di affidabilità dovrebbe essere commisurato al livello del rischio associato al previsto uso di un prodotto TIC, servizio TIC o processo TIC*".

[594] L'art. 2 punto n. 21 definisce "livello di affidabilità" come "*base per la fiducia nel fatto che un prodotto TIC, servizio TIC o processo TIC soddisfa i requisiti di sicurezza di uno specifico sistema europeo di certificazione della cibersicurezza e indica il livello al quale un prodotto TIC, servizio TIC o processo TIC è stato valutato, ma di per sé non misura la sicurezza del prodotto TIC, servizio TIC o processo TIC interessato*".

[595] Regolamento di esecuzione (UE) 31 gennaio 2024, 2024/482 della Commissione, recante "Regolamento che stabilisce norme di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del

Tale regolamento istituisce il "Sistema europeo di certificazione della cibersicurezza basato sui *common criteria*" (Sistema EUCC") relativo a tutti i "prodotti delle tecnologie dell'informazione e della comunicazione" (prodotti TIC) che sono presentati ai fini della certificazione nel quadro EUCC.[596] Il Sistema si rivolge, in sostanza, a tutti i prodotti TIC che sono stati sottoposti a una valutazione di conformità condotta secondo la metodologia internazionale denominata *Common Criteria.*[597] Tale metodologia consiste in un insieme di regole e procedure standardizzate impiegate per valutare la sicurezza di un determinato prodotto (*Target of Evaluation*, TOE), operando un raffronto tra il medesimo e i requisiti di sicurezza dichiarati dal produttore all'interno di un documento, denominato *Security Target* (ST)[598] o, se richiamato dallo ST, nel *Protection Profile* (PP). [599] [600] In particolare, durante la suddetta valutazione viene effettuata un'analisi delle vulnerabilità del prodotto, secondo un livello AVA_VAN [601] predefinito. [602] Una volta che il prodotto dovesse superare con esito positivo la valutazione, il medesimo può quindi ottenere il certificato EUCC da parte dell'organismo di certificazione, che attesta un grado di affidabilità "sostanziale" ovvero "elevato" a seconda del livello AVA_VAN concretamente adottato.[603]

In conclusione, in base alla normativa sopra illustrata, è ragionevole ipotizzare l'introduzione dell'obbligo per le imprese di investimento algoritmiche di dotarsi di prodotti TIC certificati in forza dell'articolo 56 par. 2 Reg. CSA. Tale certificato potrebbe

---

Consiglio per quanto riguarda l'adozione dello schema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC)" (EUCC), in GUUE L 2024/482 del 7 febbraio 2024.

[596] Art. 1 par. 1 e par. 2 Reg. 2024/482.

[597] Per *Common Criteria* si intendono "*i criteri comuni per la valutazione della sicurezza delle tecnologie dell'informazione quali definiti nella norma ISO/IEC 15408*" (art. 2 par. 1 Reg. 482/2024).

[598] Per *Security Target* si intende "*una dichiarazione dei requisiti di sicurezza dipendenti dall'implementazione per uno specifico prodotto ITC*". (Art. 2 punto n.4).

[599] Per *Protection Profile* si fa riferimento a un documento "standard" dei *Common Criteria* che descrive, in modo generico per una categoria di prodotti, quali requisiti di sicurezza debbano essere soddisfatti in un certo contesto d'uso.

[600] Art. 5 par.1 Reg. di esecuzione n. 482 del 2024.

[601] Per "Livello AVA_VAN" si intende "*un livello di analisi della vulnerabilità dell'affidabilità che indica il grado delle attività di valutazione della cibersicurezza svolte per determinare il livello di resistenza rispetto alla potenziale possibilità di sfruttare i difetti o i punti deboli dell'oggetto della valutazione nel suo ambiente operativo, come stabilito nei criteri comuni*" (Art. 2 pt. n. 8).

[602] I livelli AVA_VAN variano da un'intensità della valutazione minima corrispondente a 1, fino a una massima di 5.

[603] Art. 4 par. 1 Reg. di esecuzione n. 482 del 2024. In particolare, si specifica che i certficati EUCC al livello di affidabilità "sostanziale" corrispondono a certificati relativi al livello AVA_VAN 1 o 2. Invece, i certificati EUCC con livello di affidabilità "elevato" corrispondono a certificati relativi al livello AVA_VAN 3, 4 o 5.

ragionevolmente consistere nel "Certificato EUCC", rilasciato in conformità al "Sistema di certificazione della cibersicurezza basato sui *common criteria*" e introdotto dal Reg. UE di esecuzione n. 482 del 2024.

Siffatto obbligo rappresenterebbe una soluzione coerente con il Reg. DORA che all'art. 7 par. 1 DORA richiede alle entità finanziarie di "*utilizzare e mantenere aggiornati sistemi, protocolli e strumenti TIC che sono: a) affidabili; b) dotati di sufficiente capacità per elaborare in maniera accurata i dati necessari per lo svolgimento delle attività e la tempestiva fornitura di servizi, nonché per sostenere i picchi di volume di ordini, messaggi ed operazioni a seconda delle necessità, anche nel caso di introduzione di nuove tecnologie; e c) tecnologicamente resilienti, in modo da fare adeguatamente fronte alle esigenze di informazioni supplementari richieste da condizioni di stress del mercato o da altre situazioni avverse"* nonché coerente con la prospettiva di *security by design,* già fatta propria dal legislatore EU, e permetterebbe altresì di ridurre il rischio di *supply chain* in quanto le imprese sarebbero spinte a dotarsi di prodotti verificati e con garanzie di sicurezza e di affidabilità maggiori.

L'obbligo in parola, tuttavia, non dovrebbe applicarsi indiscriminatamente a tutti i componenti TIC concretamente impiegati: risulterebbe eccessivo, dispendioso nonché difficilmente attuabile data la mole ampia di sistemi *hardware* e *software* che un'impresa HFT utilizza. A tal riguardo, sembra maggiormente fattibile circoscriverne la portata a quei prodotti TIC inseriti all'interno di sistemi informativi o di rete *da cui dipendono funzioni essenziali o importanti dell'attività* dell'impresa di investimento algoritmica.

CONCLUSIONI

Nel presente elaborato è stato approfondito cosa si intenda per *trading* algoritmico e analizzati i relativi aspetti delle manipolazioni di mercato e di sicurezza informatica, pertanto, pare opportuno in questa sede trarre alcune riflessioni conclusive.

Nel primo capitolo si è appreso come dalle suddette forme di negoziazione possano derivare molteplici rischi ed effetti negativi quali, ad esempio, riduzioni della liquidità, forti volatilità nonché possibili turbolenze sui mercati (*flash crash*). In virtù di tali aspetti, il legislatore EU ha cercato di disciplinare il fenomeno in questione attraverso la Direttiva MiFID II e i regolamenti delegati (RTS). Nel complesso, le disposizioni contenute all'interno della MiFID II si contraddistinguono per essere "tecnologicamente neutre", in quanto mirano a disciplinare i rischi che possano derivare da una siffatta modalità di negoziazione, piuttosto che disciplinare la tecnologia in quanto tale. Tale qualità risulta essere di cruciale importanza, in quanto in tal modo è possibile scongiurare normative obsolete a causa degli incessanti e repentini sviluppi tecnologici.

Una dimostrazione di ciò risiede nella definizione stessa di *Trading* Algoritmico contenuta all'interno dell'art. 4 (1)(39) della MiFID II che adotta una formulazione volutamente ampia e neutra da ricomprendere anche forme di negoziazione realizzabili mediante intelligenza artificiale.

Al contrario, una simile "neutralità tecnologica" non sembra rinvenirsi all'interno dei regolamenti delegati (RTS). A tal proposito, nel presente elaborato è stato messo in luce come la formulazione di alcune disposizioni contenute negli RTS possa porsi in aperta contraddizione rispetto alle caratteristiche tipiche dell'intelligenza artificiale, facendo così emergere interrogativi circa la legittimità di quelle forme di negoziazione che dovessero ricorrere ad algoritmi auto apprendenti. Un divieto ricavabile in via interpretativa dovrebbe, tuttavia, essere escluso, in quanto contrasterebbe con la stessa logica del legislatore UE che, regolando il fenomeno dell'AT e dell'HFT "tradizionale", ha ammesso entro soglie di rischio tollerabili tali forme di negoziazione. Ciononostante, questa forma di inadeguatezza da ultimo evidenziata non dovrebbe essere sottovalutata: se è vero che risulta difficile predisporre normative allineate e aggiornate ai più recenti sviluppi tecnologici, le istituzioni competenti potrebbero valutare l'opportunità di estendere il contenuto degli RTS adottando una nozione di "rischio" più ampia e comprensiva anche di quei pericoli che possano derivare da un ricorso a sistemi di IA nelle operazioni di *trading*.

Nel secondo capitolo la disamina si è concentrata sull'argomento delle manipolazioni di mercato e, da tale analisi, è emerso come sia la normativa europea sia la normativa italiana, in particolare la recentissima legge 23 settembre 2025 n. 132 (Legge IA), abbiano adottato la dimensione "antropocentrica" quale principio cardine dei sistemi IA, dal quale ne consegue *naturaliter* quello di *machina deliquere et puniri non potest*.

Da una siffatta indagine si è evidenziato un duplice ordine di problematiche. *In primis,* le disposizioni contenute nel *Market Abuse Regulation* (MAR) e, di riflesso, quelle predisposte a livello interno nel Testo Unico Finanziario (T.U.F.) possono incontrare un *deficit* di attuazione in tutti quei casi in cui l'illecito dovesse essere compiuto tramite sistemi di IA caratterizzati da un elevato livello di opacità (*black box*). Invero, data la formulazione di tali norme, risulterebbe assai problematica per le Autorità competenti la dimostrazione dell'elemento soggettivo in capo a colui che si è servito della macchina; *in secundis,* un ulteriore profilo di problematicità emerge in tutti quei casi in cui l'attività di negoziazione venisse svolta all'interno di organizzazioni strutturate e complesse. In tal caso, potrebbe rendersi assai complicata l'individuazione di una persona fisica responsabile dell'illecito, a causa della lunga catena di soggetti astrattamente individuabili (*many hands problem*).

Con riferimento al primo aspetto (il possibile *deficit* di attuazione), nel presente elaborato è stata avanzata la proposta di adottare, anche nel settore del *trading* algoritmico, un *corpus* di norme consistenti in obblighi volti ad incrementare i livelli di trasparenza e spiegabilità dei modelli algoritmici e matematici impiegati per la negoziazione. Tali obblighi, si è evidenziato, dovrebbero essere posti in capo ai *providers* di tali modelli, in linea con le disposizioni contenute nell'AI ACT riguardanti i sistemi ad alto rischio.

Con riferimento al secondo aspetto problematico (*many hands problem*), è stato argomento come una siffatta circostanza potrebbe essere in parte risolta ricorrendo ai meccanismi previsti dall'art. 8 del d.lgs. 231/2001 (recante la disciplina in materia di responsabilità dell'ente per gli illeciti amministrativi dipendenti da reato). In particolare, l’impresa di investimento algoritmica potrebbe essere ritenuta responsabile del reato di manipolazione di mercato, laddove venisse dimostrato un *deficit* dell’organizzazione interna che abbia impedito l’esatta identificazione del responsabile e venisse provato che tale reato sia stato compiuto *nell’ interesse* o *a vantaggio* dell’ente stesso.

Nel terzo ed ultimo capitolo, la disamina si è concentrata sul tema della sicurezza informatica. Dall’analisi complessiva delle norme è emerso come il legislatore EU abbia predisposto per le imprese di investimento algoritmiche un assetto formato, rispettivamente, dal Reg. DORA e dalla Direttiva MiFID II (in particolare si richiama l’art. 18 RTS 6) e volto alla gestione dei rischi informatici. Dall’analisi di tale assetto normativo sono emerse una serie di aspetti problematici.

In particolare, si è evidenziato come talune disposizioni non risultino pienamente chiare quanto alla tipologia di incidenti che, in concreto, debbano essere segnalati alle Autorità competenti, con la conseguenza di generare incertezze in capo alle singole imprese circa la corretta qualificazione degli stessi. Inoltre, è stato segnalato come, a seconda del soggetto coinvolto, si possa assistere anche a una duplicazione degli obblighi di notifica tale da appesantire il carico procedurale e ostacolare una risposta pronta e immediata all’incidente.

La normativa concernente la *cybersecurity* delle imprese algoritmiche ma, più in generale, anche la normativa *cyber* europea ed italiana largamente intesa, si caratterizzano per una elevata complessità tecnica, un ampio novero di fonti e da una stratificazione degli obblighi che rendono necessaria la presenza di esperti di diritto in materia. In questa prospettiva, è stato messo in luce come nelle imprese più piccole, meno strutturate e con poche risorse a disposizione, un tale assetto stratificato di regole a cui ottemperare potrebbe comportare svantaggi competitivi e, nel lungo periodo, potrebbe causare altresì la perdita di quote di mercato a vantaggio di entità più grandi.

A tal proposito, dal momento che le piccole e medie imprese rappresentano una parte fondamentale del tessuto produttivo nazionale e che, pertanto, risulta fondamentale assicurare per esse una adeguata protezione da minacce informatiche, potrebbe prospettarsi ragionevole la creazione di un “collaborazione virtuosa” tra queste ultime e il legislatore italiano, in virtù del quale le prime sono chiamate a fornire dettagli ed informazioni sulla natura degli incidenti [604] mentre, il secondo, a intervenire con incentivi e misure di sostegno economico in modo da favorire investimenti in infrastrutture digitali, sicure e resilienti.

Nel terzo capitolo, infine, è stata avanzata *de iure condendo* la proposta di introdurre l'obbligo per le imprese algoritmiche, di avvalersi di prodotti ITC recanti certificato EUCC, attestante un livello di cibersicurezza "sostanziale" o "elevato" e rilasciato in conformità al "Sistema di certificazione della cibersicurezza basata sui C*ommon Criteria*". L'introduzione di un tale obbligo consentirebbe alle imprese, secondo un approccio di *cybersecurity by design,* di dotarsi di prodotti ITC con garanzie di sicurezza e affidabilità maggiori e, allo stesso tempo, ridurre il rischio che un eventuale incidente informatico possa ripercuotersi negativamente sui mercati.

La disamina sino ad ora svolta si conclude con una riflessione concernente un tema che ha fatto da sfondo a tutti i tre capitoli e che risulta essere di centrale rilevanza in relazione al *trading* algoritmico e all'intelligenza artificiale, ossia quello del "fattore umano".

Con il termine "fattore umano" si intende generalmente l'insieme dei comportamenti assunti, delle decisioni prese, dei limiti e delle capacità delle persone ogniqualvolta queste si interfaccino con un'organizzazione, una procedura o una tecnologia.

Per quanto concerne le manipolazioni di mercato, il "fattore umano" acquisisce un ruolo di grande rilievo. Salvo i casi imprevedibili ed incolpevoli di una macchina che arrivi a compiere un illecito in maniera autonoma e indipendente da un contributo umano, una manipolazione di mercato operata da un algoritmo è di fatto il frutto di una programmazione dolosa o, perlomeno colpevole, di un individuo che sceglie di sfruttare un mezzo in cui decide di immettere *ciò che è e che lo rispecchia*. In questa prospettiva, si rende necessario, allora, non solo interrogarsi sull'adeguatezza della normativa ma anche sull'etica del singolo o, detto altrimenti, sull' "algoretica"[605] che dovrebbe ispirare

---

[604] Si sottolinea come sia di fondamentale importanza per le Autorità acquisire informazioni di dettaglio sui singoli incidenti al fine di sviluppare comprendere le tattiche degli aggressori e di individuare minacce in anticipo e attuare contromisure efficaci, tuttavia, le imprese sono spesso restie a condividere tali informazioni.

[605] Per "Algoretica" si intende un approccio etico "per" e "dentro" gli algoritmi, volto a tradurre principi e valori umani (come dignità, equità, non discriminazione, trasparenza, responsabilità) in criteri operativi di progettazione, addestramento, implementazione e controllo dei sistemi, così da assicurare la centralità della persona umana. BENANTI, P. (2018). Oracoli. Tra algoretica e algocrazia. Luca Sossella Editore.

le scelte individuali affinché la tecnologia sia uno strumento utilizzato in modo *corretto, trasparente e responsabile* (art. 1 Legge IA).

Il concetto di “fattore umano” acquisisce, inoltre, una rilevanza centrale anche all’interno della *cybersecurity*. L’essere umano è, infatti, il primo presidio di sicurezza e, di conseguenza, risulta necessario assicurare che la generalità dei consociati sia correttamente informata circa i rischi che discendono da un impiego delle tecnologie digitali.

Infatti, al giorno d’oggi risulta essere sempre più ampiamente diffuso il c.d. fenomeno di “primitivismo digitale”[606] un termine che allude alla mancanza di conoscenze e di adeguata preparazione circa l’uso degli strumenti tecnologici.

Di conseguenza, risulta cruciale la promozione di una maggior consapevolezza circa l’importanza della sicurezza informatica tra gli stessi cittadini, che spesso sono portati a sottostimare i rischi e a ritenere che un semplice *antivirus* sia in grado di risolvere la maggior parte dei problemi. Di tale aspetto, il legislatore italiano ha colto l’importanza: infatti, nel decreto-legge n. 82 del 2021 convertito dalla legge n. 109 del 2021 e istitutivo dell’Autorità per la cybersicurezza nazionale, all’ articolo 7 co. 2 lett *u)* viene affidato all’ ACN il compito *di comunicazione e promozione di una consapevolezza in materia di cybersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia*.

Da ultimo, il “fattore umano” acquisisce una rilevanza fondamentale anche in rapporto alla stessa intelligenza artificiale, in quanto tale tecnologia, nata per “imitare” l’intelligenza umana, finisce per spingere sempre più *l’individuo a conoscere e a interrogarsi su se stesso*.[607]

Domandarsi cosa significhi “essere umani” e indagare sulle differenze rispetto a una macchina si rende, ad oggi, più che mai necessario. Invero, la caratteristica più intrinseca dell’uomo e che una macchina non possederà mai, in quanto irriducibile a leggi fisiche o a meri segnali elettrici o biochimici, è la coscienza. Quest’ultima è intesa come lo *spazio*

---

[606] FRATTASI, B. (27 gennaio 2026). Direttore generale dell’Agenzia per la Cybersicurezza Nazionale (ACN), intervento alla conferenza *Zero Trust, Infinite Possibility: Costruire un ecosistema sicuro e resiliente per accelerare la trasformazione digitale* (LUISS Guido Carli, Roma).
[607] BOVASSI, G. (2025). Attrazione digitale. Il lato oscuro del transumano e dell’intelligenza artificiale. Il Timone, p. 76.

semantico interiore dove i segnali provenienti dal mondo fisico, all'interno del corpo e all'esterno del corpo, ed elaborati dal cervello, assumono la forma di sentimenti, sensazioni e significati. [608] Essere coscienti significa quindi trasformare i segnali fisici e i dati simbolici del mondo esterno in sensazioni, emozioni, pensieri e sentimenti, e da essi "estrarre" un significato personale e soggettivo che ci rende consapevoli dell'esperienza concreta e che ci collega emotivamente, cognitivamente e associativamente a tutta la nostra esperienza di vita.[609]

In altre parole, se per una macchina la parola "amore" significa leggere una sequenza di 40 "bit" (01100001 01101101 01101111 01110010 01100101) da rappresentare mediante il codice ASCII, per l'uomo "amore" ha una semantica più profonda e radicale, da muovere praticamente la composizione di tutta la letteratura mondiale, in ogni luogo e in ogni tempo.[610]

L'idea di equiparare l'uomo ad una macchina o considerare l'essere umano un *quid minus* rispetto ad essa, sottintende una visione del mondo deterministica e materialistica, che riduce la coscienza umana e lo stesso libero arbitrio a mero prodotto di leggi della fisica spiegabili e, di conseguenza, replicabili.

Da ciò deduciamo quindi che l'essere umano *è molto meno, ma incredibilmente di più* [611] della capacità computazionale di una macchina, e non riconoscerlo significherebbe fare un torto a noi stessi.

---

[608] FAGGIN, F. (2022). Irriducibile. La coscienza, la vita, i computer e la nostra natura. Mondadori, p. 147.
[609] DICASTERO PER LA DOTTRINA DELLA FEDE, & DICASTERO PER LA CULTURA E L'EDUCAZIONE. (2025). Antiqua et nova: Nota sul rapporto tra intelligenza artificiale e intelligenza umana (nn. 31–32). Vatican.va.: "*Sebbene i sistemi avanzati possano "imparare" attraverso processi quali l'apprendimento automatico, questa sorta di addestramento è essenzialmente diverso dallo sviluppo di crescita dell'intelligenza umana, essendo questa plasmata dalle sue esperienze corporee: stimoli sensoriali, risposte emotive interazioni sociali e il contesto che caratterizza ogni momento. Questi elementi modellano e formano il singolo individuo nella sua storia personale. Al contrario, l'IA, sprovvista di un corpo fisico si affida al ragionamento computazionale e all'apprendimento su vasti insiemi di dati che comprendono esperienze e conoscenze comunque raccolte da essere umani. Di conseguenza, sebbene l'IA possa simulare alcuni aspetti del ragionamento umano ed eseguire certi compiti con incredibile velocità ed efficienza, e sue capacità di calcolo rappresentano solo una frazione delle più ampie possibilità della mente umana"*.
[610] BENANTI, P. (2025). L'uomo è un algoritmo? Il senso dell'umano e l'intelligenza artificiale. Castelvecchi, p. 44.
[611] FAGGIN, F. (2024). Oltre l'invisibile: Dove scienza e spiritualità si uniscono. Mondadori, p. 233.

BIBLIOGRAFIA

Agenzia per l'Italia Digitale (AgID). (2024). Strategia italiana per l'intelligenza artificiale 2024–2026.

Aldridge, I. (2013). High-frequency trading: A practical guide to algorithmic strategies and trading systems (2nd ed.). John Wiley & Sons.

Alfano, G. (2024). Rischi informatici nel settore finanziario: Strumenti di prevenzione e resilienza operativa digitale. *Rivista di Diritto Bancario*, 4(Suppl.).

Alvaro, S., & Ventoruzzo, M. (2016). «High-frequency trading»: note per una discussione. *Banca Impresa Società, 35*(3).

Amati, L. (2012). Abusi di mercato e sistema penale. Giappichelli, Torino.

Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). John Wiley & Sons.

Angel, J. J., Harris, L., & Spatt, C. S. (2010). Equity trading in the 21st century (Marshall School of Business Working Paper No. FBE 09-10). University of Southern California, Marshall School of Business, Los Angeles, CA.

Annunziata, F. (2018). La disciplina delle trading venues nell'era delle rivoluzioni tecnologiche: Dalle criptovalute alla distributed ledger technology. *Orizzonti del Diritto Commerciale*, 6(3).

Annunziata, F. (2023). Artificial intelligence and the regulation of market abuse: A European perspective. Edward Elgar Publishing, Cheltenham (UK)–Northampton, MA (USA).

Annunziata, F. (2023). La Disciplina Del Mercato Dei Capitali. Giappichelli, Torino.

Annunziata, F. (2024). Intelligenza artificiale e disciplina degli abusi di mercato. XV Convegno Nazionale Orizzonti del Diritto Commerciale – Imprese e mercati: numeri e computer science (Atti dell'anno 2024). Orizzonti del Diritto Commerciale.

Annunziata, F. (2024). The Market Abuse Regulation and the use of general clauses thereunder (Bocconi Legal Studies Research Paper Series).

Ardito, S. (2025). Tutela della cybersecurity e dell'intelligenza artificiale. In G. Cassano & E. Prosperetti (a cura di), *Le regole dei dati e dell'intelligenza artificiale: Dal GDPR alla Legge 132/2025* Maggioli Editore.

Arner, D. W., Barberis, J., & Buckley, R. P. (2015). The evolution of FinTech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47.

Arulkumaran, K., Deisenroth, M. P., Brundage, M., & Bharath, A. A. (2017). A brief survey of deep reinforcement learning. *IEEE Signal Processing Magazine*, 34(6).

Asaro, P. M. (2011). A body to kick, but still no soul to damn: Legal perspectives on robotics. In P. Lin, K. Abney, & G. A. Bekey (Eds.), *Robot ethics: The ethical and social implications of robotics*. MIT Press.

Azzutti, A. (2022). The algorithmic future of EU market conduct supervision: A preliminary check. In Böffel, L., & Schürger, J. (Eds.), Digitalisation, Sustainability, and the Banking and Capital Markets Union: Thoughts on Current Issues of EU Financial Regulation. Palgrave Macmillan, Cham

Azzutti, A. (2024). AI governance and algorithmic trading: Some regulatory insights from the EU AI Act. *Banking & Finance Law Review*, 41(1).

Azzutti, A., Ringe, W.-G., & Stiehl, H. S. (2021). Machine learning, market manipulation and collusion on capital markets: Why the "black box" matters. *University of Pennsylvania Journal of International Law*, 43(1).

Azzutti, A., Ringe, W.-G., & Stiehl, H. S. (2022). The regulation of AI trading from an AI life cycle perspective (European Banking Institute Working Paper No. 130).

Azzutti, A. (2022). The algorithmic future of EU market conduct supervision: A preliminary check. In Böffel, L., & Schürger, J. (Eds.), Digitalisation, Sustainability, and the Banking and Capital Markets Union: Thoughts on Current Issues of EU Financial Regulation, pp. 53–98. Palgrave Macmillan, Cham.

Bagni, F. (2023). La sandbox regolamentare e la sfida a tema cybersecurity: dall'Artificial Intelligence Act al Cyber Resilience Act. *Rivista Italiana Di Informatica E Diritto*, 5(2).

Balaji, A. J., Ram, D. S. H., & Nair, B. B. (2018). Applicability of deep learning models for stock price forecasting: An empirical study on BANKEX data. *Procedia Computer Science*, 143.

Baldauf, M., & Mollner, J. (2020). High-Frequency Trading and Market Performance. *The Journal of Finance, 75*(3).

Balp, G., & Strampelli, G. (2018). Preserving capital markets efficiency in the high-frequency trading era (Bocconi Legal Studies Research Paper No. 3097723).

Barbara, G. (2022). La cybersecurity: minacce, evoluzione normativa, corporate governance e nuove prospettive. *Corporate Governance*, (4).

Basile, F. (2019). Intelligenza artificiale e diritto penale: Quattro possibili percorsi di indagine. *Diritto penale e uomo*, 10/2019.

Bathaee, Y. (2018). The Artificial Intelligence Black Box and the Failure of Intent and Causation. *Harvard Journal of Law & Technology*, 31(2).

Battelli, E., & D'Ippolito, G. (2025). Compendio di normativa sulla privacy e cybersicurezza 2025. Nel diritto Editore.

Bell, H., & Searles, H. (2014). An analysis of global HFT regulation: Motivations, market failures, and alternative outcomes (Mercatus Center Working Paper No. 14-11). Mercatus Center at George Mason University.

Benanti, P. (2018). Oracoli. Tra algoretica e algocrazia. Luca Sossella Editore.

Benanti, P. (2025). L'uomo è un algoritmo? Il senso dell'umano e l'intelligenza artificiale. Castelvecchi.

Bershova, N., & Rakhlin, D. (2013). High-frequency trading and long-term investors: A view from the buy-side. *Journal of Investment Strategies, 2*(2).

Bertani, M. (2019). Trading algoritmico ad alta frequenza e tutela dello «slow trader». *Analisi Giuridica dell'Economia – Studi e discussioni sul diritto dell'impresa*, (1).

Bevivino, V., & Gimigliano, G. (2024). Il rischio sistemico ESG delle attività della FinTech. *Mercato Concorrenza Regole: Rivista quadrimestrale*, 1–2.

Bishop, C. M. (2006). Pattern recognition and machine learning. Springer, New York, NY, p. 1.

Boden, M. A. (2014). GOFAI. In Frankish, K., & Ramsey, W. M. (Eds.), *The Cambridge handbook of artificial intelligence*. Cambridge University Press.

Boehmer, E., Fong, K., & Wu, J. (2021). Algorithmic trading and market quality: International evidence. *Journal of Financial and Quantitative Analysis, 56*(8)

Borch, C., & Min, B. H. (2023). Machine learning and social action in markets: From first- to second-generation automated trading. *Economy and Society*, 52(1).

Bovassi, G. (2025). Attrazione digitale. Il lato oscuro del transumano e dell'intelligenza artificiale. Il Timone.

Brogaard, J. A. (2010). High frequency trading and its impact on market quality (Working paper). Northwestern University, Kellogg School of Management, Evanston, IL.

Brogaard, J., Hendershott, T. J., & Riordan, R. (2013). High-frequency trading and price discovery (Working paper).

Brummer, C. (2020). Fintech law in a nutshell. West Academic Publishing, St. Paul, MN.

Buffa, M. (2023). La direttiva NIS II cybersecurity in Europa: tra innovazione, formazione e diritto vivente. *Democrazia e Diritti Sociali*, 2023(1).

Busch, D. (2017). MiFID II: Regulating high frequency trading, other forms of algorithmic trading and direct electronic market access (Working paper; published in *Law and Financial Markets Review, 10*(2), 72–82, 2016).

Byrd, D. (2022). Learning not to spoof. In ICAIF '22: 3rd ACM International Conference on AI in Finance (pp. 1–9). Association for Computing Machinery.

Caivano, V. (2015). The impact of high-frequency trading on volatility: Evidence from the Italian market (CONSOB Working Paper No. 80). CONSOB.

Caivano, V., et al. (2012). Il trading ad alta frequenza – Caratteristiche, effetti, questioni di policy (CONSOB Discussion Paper No. 5).

Camaldo, G. Caneschi, B. Fragasso, & D. Milani (a cura di), *Intelligenza artificiale: Diritto, giustizia, economia ed etica*, Giappichelli.

Cappellini, A. (2018). Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale. *Criminalia*.

Castaldo, F. (2019). Dalla cyber defense alla cyber resilience dell'infrastruttura critica. Alcune implicazioni strategiche e organizzative. *Rivista di economia e politica dei trasporti*, (3), Articolo 2.

Chahal, A., & Gulia, P. (2019). Machine learning and deep learning. *International Journal of Innovative Technology and Exploring Engineering*, 8(12).

Chiara, P. G. (2023). Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali. *Rivista Italiana Di Informatica E Diritto*, 5(1).

Chiara, P. G., & Brighi, R. (2024). La dimensione della "resilienza" nel diritto UE della cybersicurezza. *Ragion Pratica*, 2.

Chlistalla, M. (2011, February 7). High-frequency trading: Better than its reputation? (Research Briefing). Deutsche Bank Research, Frankfurt am Main, Germany.

Christensen, C. M., Raynor, M. E., & McDonald, R. (2015). What is disruptive innovation? *Harvard Business Review.*

Cinà, A. E., Grosse, K., Demontis, A., Biggio, B., Roli, F., & Pelillo, M. (2024). Machine learning security against data poisoning: Are we there yet? *Computer*, 57(3).

Coffee, J. C., Jr. (1981). "No Soul to Damn: No Body to Kick": An unscandalized inquiry into the problem of corporate punishment. *Michigan Law Review*, 79(3).

Consob. (2023). Guida operativa – Algo-Trading e High Frequency Trading: mappatura del quadro regolamentare e degli obblighi di comunicazione alla Consob (Sez. 2, par. 2.1.5).

Consulich, F. (2018). Il nastro di Möbius: Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato. *Banca, Borsa e Titoli di Credito*, 71(2).

Consulich, F. (2020). Rischio consentito. In M. Donini (Dir.), *Reato colposo* (Enciclopedia del diritto – I Tematici, p. 1102 ss.). Giuffrè

Consulich, F. (2023). Il diritto penale al tempo dell'intelligenza artificiale: Prospettive punitive nazionali dopo l'AI Act. *Diritto e Difesa*, 3–4.

Consulich, F., Maugeri, M., Milia, C., Poli, T. N., & Trovatore, G. (2023). AI and market abuse: Do the laws of robotics apply to financial trading? (CONSOB Legal Research Papers, *Quaderni Giuridici* No. 29).

Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man-in-the-middle attacks. *IEEE Communications Surveys & Tutorials*, 18(3).

Corasaniti, G. (2022). Data science e diritto, certezze digitali e benefici del dubbio. G. Giappichelli Editore, Torino.

Corasaniti, G. (2025). Sicurezza informatica e intelligenza artificiale: Rischio e resilienza nello spazio giuridico europeo. Giappichelli, Torino.

Corasaniti, G. (2025). Strategie di contrasto al ransomware e nuove frontiere della criminalità informatica. *Il diritto dell'informazione e dell'informatica*, 41(1).

Cucchiara, M. F. (2017). Market abuse e doppio binario sanzionatorio: L'applicazione dei criteri elaborati dalla Grande Camera EDU al caso in cui il processo penale sia definito con sentenza di patteggiamento. *Giurisprudenza Penale*, 2017(5).

Čuk, T., & Van Waeyenberge, A. (2020). European legal framework for algorithmic and high frequency trading (MiFID II and MAR): A global approach to managing the risks of the modern trading paradigm (Working paper).

Culmone, M. (2025). Rischi IT nelle entità finanziarie: riflessioni sul regolamento DORA. *Il Nuovo Diritto delle Società*, (8).

Dalko, V., & Wang, M. H. (2020). High-frequency trading: Order-based innovation or manipulation? *Journal of Banking Regulation*, 21.

De Jong, F., & Rindi, B. (2009). The Microstructure Of Financial Markets. Cambridge University Press.

Dellagiacoma, M. (2025). Negoziazione algoritmica, intelligenza artificiale e market abuse oltre l'high frequency trading: I profili di rilevanza penale (Tesi di dottorato, Università Commerciale Luigi Bocconi).

DeMarco, D. (2012). Exploiting Financial Information Exchange (FIX) Protocol? (GIAC GCIH Gold Certification paper). SANS Institute / GIAC.

Deng, Y., Bao, F., Kong, Y., Ren, Z., & Dai, Q. (2017). Deep direct reinforcement learning for financial signal representation and trading. *IEEE Transactions on Neural Networks and Learning Systems*, 28(3).

Dicastero per la Dottrina della Fede, & Dicastero per la Cultura e l'Educazione. (2025). *Antiqua et nova: Nota sul rapporto tra intelligenza artificiale e intelligenza umana*. Vatican.va.

Di Ciommo, F. (2019). Smart contract e (non-)diritto: Il caso dei mercati finanziari. *Nuovo Diritto Civile, IV*(1).

Di Michele, M. (2024). Intelligenza artificiale. Etica, rischi e opportunità di una tecnologia rivoluzionaria. Diarkos, Roma.

Di Noia, C. (2012). Pending issues in the review of the European market abuse rules (ECMI Policy Brief No. 19). European Capital Markets Institute.

Díaz, D., & Theodoulidis, B. (2013). Financial markets monitoring and surveillance: A quote stuffing case study. In Proceedings of the 17th Panhellenic Conference on Informatics. IEEE.

Do, B. L., & Putniņš, T. J. (2023). Detecting layering and spoofing in markets (SSRN Working Paper No. 4525036).

Dutch Authority for the Financial Markets [AFM]. (2023). Machine learning in algorithmic trading: Application by Dutch proprietary trading firms and possible risks. Dutch Authority for the Financial Markets.

Dutch Authority for the Financial Markets. (2023). Machine learning in algorithmic trading: Application by Dutch proprietary trading firms and possible risks..

European Commission. (2021). Commission staff working document impact assessment accompanying the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts (SWD(2021) 84 final). European Commission, Brussels. n. 237.

European Securities and Markets Authority (ESMA). (2017). Final report – Guidelines on the calibration of circuit breakers and the publication and reporting of trading halts under MiFID II (ESMA70-872942901-17). ESMA.

European Securities And Markets Authority. (2012). Guidelines on systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities (ESMA/2012/122). ESMA.

European Securities And Markets Authority. (2014). Final Report: ESMA's Technical Advice To The Commission On Mifid II And Mifir (ESMA/2014/1569). ESMA, Paris.

European Securities and Markets Authority. (2021). MiFID II/MiFIR review report on algorithmic trading (Ref. ESMA70-156-4572). ESMA, Paris, France.

European Securities And Markets Authority. (2022). Questions And Answers On Mifid II And Mifir Market Structures Topics (ESMA70-872942901-38). ESMA, Paris.

European Union Agency For Cybersecurity (2025). *ENISA threat landscape: Finance sector (January 2023 to June 2024)*. ENISA

European Union Agency for Cybersecurity. (2025). ENISA threat landscape: Finance sector (January 2023 to June 2024). ENISA.

Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T., & Song, D. (2018). Robust physical-world attacks on deep learning models. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*.

Faggin, F. (2022). Irriducibile. La coscienza, la vita, i computer e la nostra natura. Mondadori.

Faggin, F. (2024). Oltre l'invisibile: Dove scienza e spiritualità si uniscono. Mondadori.

Faghan, Y., Piazza, N., Behzadan, V., & Fathi, A. (2020). Adversarial attacks on deep algorithmic trading policies. arXiv.

Fama, E. F. (1970). Efficient capital markets: A review of theory and empirical work. *The Journal of Finance*, 25(2).

Financial Stability Board [FSB]. (2017). Artificial intelligence and machine learning in financial services: Market developments and financial stability implications. Financial Stability Board.

Financial Stability Board. (2023). Cyber lexicon: Updated in 2023. Financial Stability Board.

Fioriglio, G. (2025). Intelligenza artificiale e cibersicurezza: profili informatico-giuridici, fra vulnerabilità delle macchine e delle persone. *I-lex*, 18(2).

Forti, G. (1990). Colpa ed evento nel diritto penale. Giuffrè.

Fragasso, B. (2024). Intelligenza artificiale e crisi del diritto penale d'evento: Profili di responsabilità penale del produttore di sistemi di I.A. In F. Basile, M. Biasi, L.

Camaldo, G. Caneschi, B. Fragasso, & D. Milani (a cura di), *Intelligenza artificiale: Diritto, giustizia, economia ed etica*, Giappichelli.

Futures Industry Association. (2023). FIA Taskforce on Cyber Risk: After Action Report and Findings.

Gargantini, M., & Siri, M. (2019). Il "prezzo dei prezzi": Una soluzione di mercato ai rischi dell'high frequency trading? (Relazione al X Convegno annuale dell'Associazione Italiana dei Professori Universitari di Diritto Commerciale "Orizzonti del Diritto Commerciale", "L'evoluzione tecnologica e il diritto commerciale", Roma).

Governo italiano. (2021). Programma strategico per l'intelligenza artificiale 2022–2024. Ministero dell'Università e della Ricerca; Ministero dello Sviluppo Economico; Ministro per l'Innovazione tecnologica e la Transizione Digitale.

GCSEC. (2020). L'impatto del cyber risk sul mercato finanziario: Case studies. GCSEC.

Gerig, A. (2015). High-frequency trading synchronizes prices in financial markets (Working paper).

Giupponi, T. F. (2024). Il governo nazionale della cybersicurezza. *Quaderni Costituzionali*, 2/2024.

Gless, S., Silverman, E., & Weigend, T. (2016). If robots cause harm, who is to blame? *New Criminal Law Review*, 19(3).

Goldblum, M., Schwarzschild, A., Patel, A. B., & Goldstein, T. (2021). Adversarial attacks on machine learning systems for high-frequency trading (arXiv:2002.09565v4). arXiv.

Gould, A. L. (2011). Regulating high-frequency trading: Man v. machine. *Journal of High Technology Law*, 12.

Hallevy, G. (2015). Liability for crimes involving artificial intelligence systems. Springer.

Harris, J. H., & Schultz, P. H. (1998). The trading profits of SOES bandits. *Journal of Financial Economics, 50*(2).

Hendershott, T. J., Jones, C. M., & Menkveld, A. J. (2011). Does algorithmic trading improve liquidity? *The Journal of Finance, 66*(1).

Hills, B. (2000). Common message standards for electronic commerce in wholesale financial markets. *Bank of England Quarterly Bulletin*, 40(3).

International Organization of Securities Commissions [IOSCO]. (2021). The use of artificial intelligence and machine learning by market intermediaries and asset managers (FR06/2021, Final Report). International Organization of Securities Commissions.

Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning. *Electronic Markets*, 31(3).

Jarrow, R. A., & Protter, P. (2011). A dysfunctional role of high frequency trading in electronic markets (Johnson School Research Paper Series No. 08-2011). Cornell University, Samuel Curtis Johnson Graduate.

Kearns, M., & Nevmyvaka, Y. (2013). Machine learning for market microstructure and high frequency trading. In Easley, D. A., López de Prado, M., & O'Hara, M. (Eds.), High-frequency trading: New realities for traders, markets and regulators. Risk Books, London.

Kirilienko, A., Kyle, A. S., Samadi, M., & Tuzun, T. (2014). The flash crash: The impact of high frequency trading on an electronic market (CFTC Working Paper). U.S. Commodity Futures Trading Commission.

Kognole, S. (2024). FIX protocol: The backbone of financial trading. *International Journal of Computer Science & Information Technology*, 16(4).

Korsmo, C. (2014). High-frequency trading: A regulatory strategy. *University of Richmond Law Review, 48*(2).

Ladley, D., Oriol, N., & Veryzhenko, I. (2024). High-frequency spoofing, market fairness and regulation (Preprint submitted to Elsevier).

Lee, J., & Schu, L. (2021). Regulation of algorithmic trading: Frameworks for human supervision and direct market interventions. *European Business Law Review*.

Leis, D. (2012*). High-Frequency Trading: Market Manipulation And Systemic Risks From An EU Perspective* (Working Paper).

Lerch, M. P. (2022). Algorithmic trading and high-frequency trading. In R. Veil (Ed.), *European capital markets law* (3rd ed.).

Lewis, M. (2014). Flash Boys: A Wall Street Revolt. W. W. Norton & Company.

Li, Y., Zheng, W., & Zheng, Z. (2019). Deep robust reinforcement learning for practical algorithmic trading. *IEEE Access*, 7.

Lin, B. L. D., & Putniņš, T. J. (2015). The new market manipulation. Charles Sturt University, School of Accounting and Finance.

Lin, T. C. W. (2017). The new market manipulation. *Emory Law Journal*, 66.

Lipton, Z. C. (2017). The mythos of model interpretability. *Communications of the ACM*, 61(10).

Liza, F. F. (2022). Challenges of enforcing regulations in Artificial Intelligence Act — Analyzing quantity requirement in data and data governance. CEUR Workshop Proceedings, 3221.

Lucantoni, P. (2019). L'«high frequency trading» nel prisma della vigilanza algoritmica del mercato. *Analisi Giuridica dell'Economia*, (1).

Mackenzie, D. (2018). Material Signals: A Historical Sociology Of High-Frequency Trading. *American Journal Of Sociology, 123*(6).

Magnuson, W. J. (2020). Artificial financial intelligence. *Harvard Business Law Review*, 10(2).

Magro, M. B. (2020). Decisione umana e decisione robotica: Un'ipotesi di responsabilità da procreazione robotica. In *Giustizia penale e nuove tecnologie* Giappichelli.

Manes, V. (2020). L'oracolo algoritmico e la giustizia penale: Al bivio tra tecnologia e tecnocrazia. In U. Ruffolo (a cura di), *Intelligenza artificiale: Il diritto, i diritti, l'etica* (p. 5). Giuffrè.

Mangiameli, S. (2023). La sovranità digitale. *Diritti fondamentali*, (3).

Marinucci, G., Dolcini, E., & Gatta, G. L. (2023). Manuale di diritto penale. Parte generale (12ª ed.). Giuffrè Francis Lefebvre.

Mark, G. (2019). Spoofing and layering. *The Journal of Corporation Law*, 45(2).

Martínez-Miranda, E., McBurney, P., & Howard, M. J. W. (2015). Learning unfair trading: A market manipulation analysis from the reinforcement learning perspective (arXiv Preprint No. arXiv:1511.00740).

Marziali, A. (2020). Cybersecurity: come la NATO si adatta alle nuove sfide. ISPI.

Mazza, M., & Cappelli, M. (2020). L'impatto del cyber risk sul mercato finanziario: Case studies. GCSEC – Global Cyber Security Center.

McCarthy, J. (2023). Cyber-risks in modern finance: Building operational and regulatory resilience. *Journal of International Banking Law and Regulation*, 38(7).

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (1955). A proposal for the Dartmouth Summer Research Project on Artificial Intelligence [Proposta dattiloscritta non pubblicata]. Dartmouth College, Hanover, NH.

McGowan, M. J. (2010). The rise of computerized high frequency trading: Use and controversy. *Duke Law & Technology Review, 9*(1).

Michieli, N. (2024). Cybersecurity e gestione del rischio ICT: l'impatto sulla corporate governance. *Banca Impresa Società*, 2.

Minnella, V. (2025). Cybersecurity e intelligenza artificiale: Alleanza indispensabile per la sicurezza del futuro. *Rassegna dell'Arma dei Carabinieri*, (1).

Mizuta, T. (2020). Does an artificial intelligence perform market manipulation with its own discretion? A genetic algorithm learns in an artificial market simulation (arXiv Preprint No. arXiv:2005.10488).

Moloney, N. (2014). EU securities and financial markets regulation (3rd ed.). Oxford University Press, Oxford.

Myklebust, T. (2020). Fairness and integrity in high-frequency markets – A critical assessment of the European regulatory approach. *European Business Law Review, 31*(1).

Oloyede, J. (2024). AI-driven cybersecurity solutions: Enhancing defense mechanisms in the digital era [Manuscript].

Ozbayoğlu, A. M., Gudelek, M. U., & Sezer, O. B. (2020). Deep learning for financial applications: A survey. *Applied Soft Computing*, 93, Article 106384.

Palmisano, M. (2019). L'abuso di mercato nell'era delle nuove tecnologie: Trading algoritmico e principio di personalità dell'illecito penale. *Diritto penale contemporaneo – Rivista trimestrale*, 2/2019.

Pansa, A. (2019). La sicurezza nazionale: innovazione e nuovi limiti. *Gnosis*, 25(1).

Pascale, N. (2022). Machine Learning e Deep Learning: applicazioni e dubbi etici. In NATALE, A. (a cura di), *Fintech. I confini dell'innovazione nella finanza*, p. 245. Giuffrè Francis Lefebvre, Milano.

Pedreschi, D., Giannotti, F., Guidotti, R., Monreale, A., Ruggieri, S., & Turini, F. (2019). Meaningful explanations of black box AI decision systems. Proceedings of the AAAI Conference on Artificial Intelligence, 33(01).

Pérez Carrillo, E. F. (2023). Cybersecurity in European financial institutions: New grounds for corporate governance reform. *European Business Law Review*, 34(7).

Perrone, A. (2024). Il Diritto Del Mercato Dei Capitali. Giuffrè Francis Lefebvre.

Picotti, L. (Ed.). (2023). Resolution on traditional criminal law categories and AI. AIDP – International Association of Penal Law.

Piergallini, C. (1995). Danno da prodotto e responsabilità penale. Giuffrè.

Piergallini, C. (2020). Intelligenza artificiale: da "mezzo" a "autore" del reato? *Rivista italiana di diritto e procedura penale*, 63(4).

Piva, D. (2022). Cybersecurity e corporate governance tra valutazioni top-down e tecniche bottom-up. *Corporate Governance*, 4.

Piva, D. (2022). Machina discere, (deinde) delinquere et puniri potest. *Rivista italiana di diritto e procedura penale*, 65(4).

Poletti, S. (2023). La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica. *MediaLaws – Rivista di diritto dei media*, 2.

Previti, L. (2022). Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico. *Federalismi.it*, (25).

Pricope, T.-V. (2021). Deep reinforcement learning in quantitative algorithmic trading: A review (arXiv:2106.00123). arXiv.

Pujol, G. (2009). Smart Order Routing And Best Execution (AMCIS 2009 Proceedings, Paper 155)

Puorro, A. (2013). High frequency trading: Una panoramica (Banca d'Italia, Occasional Paper n. 198).

Putniņš, T. J. (2020). An overview of market manipulation. In C. Alexander & D. Cumming (Eds.), Corruption and fraud in financial markets: Malpractice, misconduct and manipulation. John Wiley & Sons.

Raffaele, F., & Manna, M. (2024). High Frequency Trading e informazioni privilegiate: Insider Trading "strutturale" o lecita superiorità informativa? *Orizzonti del Diritto Commerciale*, (1).

Raschner, P. (2021). Algorithms put to test: Control of algorithms in securities trading through mandatory market simulations? (European Banking Institute Working Paper No. 87).

Reddy, R. K. V., Khan, A. N., Garg, S., G, N. K., Kasireddy, L. C., & Dayalan, P. (2025). Cybersecurity risks in real-time stock market analytics and digital marketing campaigns. *Journal of Informatics Education and Research*, 5(1).

Rizzi, M. A., & Serini, F. (2024). Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano. *Rivista Italiana Di Informatica E Diritto*, 6(2).

Sadaf et al. (2021). Algorithmic trading, high-frequency trading: Implications for MiFID II and Market Abuse Regulation (MAR) in the EU.

Sanchini, F. (2025). Sicurezza cibernetica e architettura istituzionale: verso una governance costituzionalmente orientata? *Federalismi.it*, (26).

Schneider, G. (2022). La resilienza operativa digitale come materia di corporate governance: Prime riflessioni a partire dal DORA. *Corporate Governance*.

Schwab, K. (2018). La quarta rivoluzione industriale (2ª ed.). FrancoAngeli.

Sciarrone Alibrandi, A., Rabitti, M., & Schneider, G. (2023). The European AI Act's impact on financial markets: From governance to co-regulation (SSRN Working paper).

Seminara, S. (2022). Diritto penale commerciale. Vol. 3: Il diritto penale del mercato mobiliare. Giappichelli, Torino.

Serini, F. (2024). La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana. *Rivista Italiana Di Informatica E Diritto*, 5(2).

Shearer, M., Rauterberg, G., & Wellman, M. P. (2023). Learning to manipulate a financial benchmark. In ICAIF '23: 4th ACM International Conference on AI in Finance (pp. 592–600). Association for Computing Machinery.

Shimao, H., Saengchote, K., Chakraborty, K., Wang, C., & Khern-am-nuai, W. (2025). Adversarial attacks on machine learning-driven high-frequency trading models.

Spindler, G. (2020). Control of algorithms in financial markets – The example of high frequency trading. In Ebers, M., & Navas, S. (Eds.), Algorithms and law. Cambridge University Press.

Spooner, T., Fearnley, J., Savani, R., & Koukorinis, A. (2018). Market making via reinforcement learning. In Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS 2018). International Foundation for Autonomous Agents and Multiagent Systems, Stockholm.

Stiglitz, J. E. (2014). Tapping the Brakes: Are Less Active Markets Safer and Better for the Economy? (Unpublished manuscript prepared for the Federal Reserve Bank of Atlanta). Federal Reserve Bank of Atlanta.

Stoll, H. R. (2006). Electronic Trading In Stock Markets. *Journal Of Economic Perspectives, 20*(1).

Taddei Elmi, G., Contaldo, A., Cavaceppi, C., & Marchiafava, S. (Eds.). (2025). Intelligenza artificiale: Legge 23 settembre 2025, n. 132. Il nuovo scenario giuridico italiano. Pacini Giuridica.

Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, 361(6404).

Tong, L. (2015). A blessing or a curse? The impact of high frequency trading on institutional investors (European Finance Association Annual Meetings 2014 Paper Series).

Tritto, N. M. (2025). Verso il c.d. diritto digitale: prime riflessioni sulla riforma in materia di intelligenza artificiale. *Internet & Diritto*, 9/2025.

U.S. Securities And Exchange Commission, & U.S. Commodity Futures Trading Commission. (2010). Findings Regarding the Market Events of May 6, 2010: Report of the staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues (Report of the staffs of the CFTC and SEC). SEC/CFTC.

U.S. Securities and Exchange Commission. (1998, December 8). Regulation of Exchanges and Alternative Trading Systems (Securities Exchange Act Release No. 34-40760). *Federal Register, 63*, 70844–70951, spec. p. 70844.

U.S. Securities and Exchange Commission. (2005, June 9). Regulation National Market System (Regulation NMS) (Securities Exchange Act Release No. 34-51808; 17 C.F.R. pt. 242). *Federal Register, 70*(123), p. 37496 ss.

U.S. Securities and Exchange Commission. (2013). SEC charges Knight Capital with violations of market access rule (Press Release No. 2013-222).

Veil, R. (Ed.). (2017). European capital markets law (2nd ed.). Hart Publishing, Oxford.

Wang, X., & Wellman, M. P. (2017). Spoofing the limit order book: An agent-based model. In Das, S., Durfee, E. H., Larson, K., & Winikoff, M. (Eds.), Proceedings of the 16th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2017).

Woodward, M. (2017). The need for speed: Regulatory approaches to high frequency trading in the United States and the European Union. *Vanderbilt Journal of Transnational Law*, 50(5).

Yadav, Y. (2015). How algorithmic trading undermines efficiency in capital markets. *Vanderbilt Law Review, 68*(6).

Yussuf, M. (2025). Advanced cyber risk containment in algorithmic trading: Securing automated investment strategies from malicious data manipulation. *International Research Journal of Modernization in Engineering Technology and Science*.

Zhang, F. (2010). High-frequency trading, stock volatility, and price discovery (Working paper).

Zhang, Z., Zohren, S., & Roberts, S. (2020). Deep reinforcement learning for trading. *The Journal of Financial Data Science*, 2(2).

Ziccardi, G. (2025). Una lettura dell’Artificial Intelligence Act: norme, etica, adempimenti, attuazione. In F. Basile et al. (a cura di), Intelligenza artificiale. Diritto, giustizia, economia ed etica. Giappichelli, Torino.

Zirulia, S. (2018). Esposizione a sostanze tossiche e responsabilità penale. Giuffrè.

SITOGRAFIA

Aracino, U., & Margaria, R. (2015). Negoziazione algoritmica e mirror trading: dinamiche operative e qualificazioni giuridiche. Diritto Bancario – Approfondimenti. https://www.dirittobancario.it/art/negoziazione-algoritmica-e-mirror-trading-dinamiche-operative-e-qualificazioni-giuridiche/.

Borsa Italiana. (n.d.). Mercato quote driven [Glossario]. Borsa Italiana https://www.borsaitaliana.it/borsa/glossario/mercato-quote-driven.html.

Financial Markets Authority. (2021). Market operator obligations targeted review – NZX: Findings from the FMA's targeted review of whether NZX is meeting its licensed market operator obligations. https://www.fma.govt.nz/assets/Reports/Market-Operator-Obligations-Targeted-Review-NZX.pdf

FIX Trading Community. (2020). FIX session layer online (Technical standard—Errata November 2020). https://www.fixtrading.org/standards/fix-session-layer-online.

FIX Trading Community. (n.d.). What is FIX?. https://www.fixtrading.org/what-is-fix/.

Frasso, E. (2023). Quando l'intelligenza artificiale batte gli umani: I casi più recenti. AI News, n.p. (https://ainews.it/quando-lintelligenza-artificiale-batte-gli-umani-i-casi-piu-recenti/.

Kosinski, M. (2024). Che cos'è la black box AI? IBM Think. https://www.ibm.com/it-it/think/topics/black-box-ai.

Milmo, D. (2024). Company worker in Hong Kong pays out £20m in deepfake video call scam. The Guardian. https://www.theguardian.com/world/2024/feb/05/hong-kong-company-deepfake-video-conference-call-scam.

Moore, H., & Roberts, D. (2013). AP Twitter hack causes panic on Wall Street and sends Dow plunging. *The Guardian*. https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall

Sgarlato, G. (2023). Quando l'IA batte l'uomo: La storia di Lee Se-dol e le cinque fasi del lutto digitale. *Il Sole 24 Ore – 24+*, n.p. (https://24plus.ilsole24ore.com/art/quando-l-ia-batte-l-uomo-storia-lee-se-dol-e-cinque-fasi-lutto-digitale-AHaQRtvB.

Stryker, C. (s.d.). What are LLMs? IBM Think, https://www.ibm.com/think/topics/large-language-models.

Treanor, J. (2015). The 2010 'flash crash': how it unfolded. *The Guardian*. https://www.theguardian.com/business/2015/apr/22/2010-flash-crash-new-york-stock-exchange-unfolded.

Treccani. *(n.d.). Latenza [Vocabolario on line]. Istituto dell'Enciclopedia Italiana Treccani. https://www.treccani.it/vocabolario/latenza.*

Varughese J., *What is a GAN?*, IBM Think, s.d., disponibile su: https://www.ibm.com/think/topics/generative-adversarial-networks.

Valsania, M. (2020). JpMorgan, multa da 920 milioni $ per manipolazione dei futures su oro e argento. *Il Sole 24 Ore*. https://www.ilsole24ore.com/art/jpmorgan-multa-920-milioni-%24-manipolazione-futures-oro-e-argento-ADUskSs.

GIURISPRUDENZA

Corte costituzionale, 8 marzo 1962, n. 19.

Corte europea dei diritti dell'uomo, Engel e altri c. Paesi Bassi, ricorsi nn. 5100/71, 5101/71, 5102/71, 5354/72 e 5370/72, sentenza 8 giugno 1976.

Corte europea dei diritti dell'uomo, Grande Stevens e altri c. Italia, ricorsi nn. 18640/10, 18647/10, 18663/10 e 18698/10, sentenza 4 marzo 2014.

Corte di cassazione, Sez. IV pen., 18 settembre 2014, n. 38343 (ThyssenKrupp), in Cassazione penale.

Corte europea dei diritti dell'uomo, A e B c. Norvegia, ricorsi nn. 24130/11 e 29758/11, sentenza 15 novembre 2016 (Grande Camera).

Corte di giustizia dell'Unione europea, Garlsson Real Estate SA e a. c. Commissione Nazionale per le Società e la Borsa (CONSOB), causa C-537/16, sentenza 20 marzo 2018.

Corte costituzionale, sentenza 2 marzo 2018, n. 43.

Corte costituzionale, sentenza 10 maggio 2022, n. 149.

Corte di cassazione, Sez. V, 1 febbraio 2022, n. 3555.