Pubblicazione Trimestrale
ISSN: 2279-9737

Rivista di Diritto Bancario

dottrina
e giurisprudenza
commentata

Supplemento
Ottobre / Dicembre
2024

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

2024

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

NORME PER LA VALUTAZIONE E LA PUBBLICAZIONE

La Rivista di Diritto Bancario seleziona i contributi oggetto di pubblicazione sulla base delle norme seguenti.

I contributi proposti alla Rivista per la pubblicazione vengono assegnati dal sistema informatico a due valutatori, sorteggiati all'interno di un elenco di ordinari, associati e ricercatori in materie giuridiche, estratti da una lista periodicamente soggetta a rinnovamento.

I contributi sono anonimizzati prima dell'invio ai valutatori.

Le schede di valutazione sono inviate agli autori previa anonimizzazione.

Qualora uno o entrambi i valutatori esprimano un parere favorevole alla pubblicazione subordinato all'introduzione di modifiche aggiunte e correzioni, la direzione esecutiva verifica che l'autore abbia apportato le modifiche richieste.

Qualora entrambi i valutatori esprimano parere negativo alla pubblicazione, il contributo viene rifiutato. Qualora solo uno dei valutatori esprima parere negativo alla pubblicazione, il contributo è sottoposto al Comitato Esecutivo, il quale assume la decisione finale in ordine alla pubblicazione previo parere di un componente della Direzione scelto ratione materiae.

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

SEDE DELLA REDAZIONE

Università degli Studi di Trento, Facoltà di Giurisprudenza, via Verdi 53,
(38122) Trento – tel. 0461 283836

MATTEO ARRIGONI

Intelligenza artificiale e manipolazione informativa del mercato finanziario*

SOMMARIO: 1. L'efficienza informativa dei mercati finanziari e il divieto di manipolazione informativa. – 2. Le peculiarità dei sistemi di intelligenza artificiale e i problemi di applicazione dei regimi di responsabilità. – 3. Informazioni false o fuorvianti e responsabilità civile. – 4. Informazioni false o fuorvianti e responsabilità penale. – 5. Informazioni false o fuorvianti e responsabilità amministrativa. – 6. (segue) Una possibile soluzione al problema. – 7. I poteri attribuiti al gestore del mercato finanziario e all'autorità di vigilanza competente. – 8. Le iniziative legislative promosse nell'Unione europea. – 9. Conclusione.

1. *L'efficienza informativa dei mercati finanziari e il divieto di manipolazione informativa*

La «piena ed effettiva trasparenza del mercato» è ritenuta «un requisito fondamentale affinché tutti gli attori economici siano in grado di operare su mercati finanziari integrati» (così il Considerando n. 7 del Regolamento (UE) n. 596/2014: d'ora in poi "MAR"). La ragionevolezza di una simile impostazione si fonda sulla valorizzazione di alcune acquisizioni della moderna finanza e, in particolare, sulla considerazione delle conseguenze che la diffusione di informazioni "rilevanti" determina sul prezzo degli strumenti finanziari ai quali tali informazioni si riferiscono[1].

Più nel dettaglio, è dato sufficientemente consolidato che quanto diffuso dagli emittenti formi oggetto di analisi da parte di un ristretto numero di investitori (gestori di fondi comuni di investimento e banche di investimento, cioè i cc.dd. *information traders*) che, sulla base dell'esame effettuato, formulano un'offerta di acquisto a un

* Il presente lavoro sviluppa la relazione presentata al Convegno "Regolazione del rischio nel Diritto dei mercati finanziari", organizzato dall'Associazione dei docenti di diritto dell'economia, ADDE (Cagliari, 13-14 giugno 2024). Ringrazio Matteo Ortino e Ugo Malvagna per le puntuali osservazioni a una versione precedente. Eventuali errori e omissioni rimangono miei.

[1] Per un approfondimento, sia consentito il riferimento a M. ARRIGONI, *Informazioni privilegiate e funzionamento dei mercati finanziari*, Milano, 2022, 3 ss.

determinato prezzo[2]. Il prezzo che viene così a formarsi nel concorso delle varie offerte di acquisto dipende pertanto dalle informazioni comunicate[3]. A questa stregua, le informazioni "rilevanti" diffuse dagli emittenti influenzano non già la decisione del singolo investitore, quanto piuttosto il meccanismo di formazione del prezzo al quale lo strumento finanziario è offerto al mercato. Con parole diverse, la diffusione delle informazioni incide non tanto sulla decisione di investimento, quanto piuttosto sul prezzo dello strumento finanziario[4]. In questo modo, il mercato è in grado di esprimere "in tempo reale" prezzi che riflettano le informazioni disponibili (c.d. efficienza informativa del mercato finanziario: *Efficient Market Hypothesis*)[5] e in questo modo, in effetti, «*tutti* gli attori economici» sono «in grado di

[2] L'originaria osservazione di R.J. GILSON - R.H. KRAAKMAN, *The Mechanism of Market Efficiency*, in 70.4. *Va. L. Rev.* (1984), 572 ss. è ribadita, *ex multis*, da F.H. EASTERBROOK - D.R. FISCHEL, *The Economic Structure of Corporate Law*, Cambridge-London, 1991, 297 e Z. GOSHEN - G. PARCHOMOVSKY, *The Essential Role of Securities Regulation*, in 55.4. *Duke L. J.* (2006), 722 ss.

[3] Per tutti, A. PERRONE, *Il diritto del mercato dei capitali*[4], Milano, 2024, 75 s. e G. STRAMPELLI, *L'informazione societaria a quindici anni dal TUF: profili evolutivi e problemi*, in *Riv. Soc.*, 2014, 999; ma v. già F.H. EASTERBROOK - D.R. FISCHEL, *Disclosure and the Protection of Investors*, in 70.4. *Va. L. Rev.* (1984), 689 e R.J. GILSON - R.H. KRAAKMAN, *The Mechanism of Market Efficiency*, cit., 575. La nota espressione secondo cui «a market in which prices always "fully reflect" all available information is called "efficient"» (così E.F. FAMA, *Efficient Capital Markets: A Review of Theory and Empirical Work*, in 25.2. *The J. of Finance* (1970), 383) sintetizza la conclusione per cui «in an efficient market, on the average, competition will cause the full effects of new information on intrinsic values to be reflected "instantaneously" in actual prices» (così E.F. FAMA, *Random Walks in Stock Market Prices*, in 21.5. *Fin. Analysts J.* (1965), 56).

[4] Formulata con riferimento al contesto della negoziazione di strumenti finanziari già emessi, l'osservazione si deve a D.R. FISCHEL, *Use of Modern Finance Theory in Securities Fraud Cases Involving Actively Traded Securities*, in 38 *Bus. Law.* (1982), 3 ss.; nella letteratura domestica, per tutti, F. SARTORI, *Informazione economica e responsabilità civile*, Padova, 2011, 67 e 117.

[5] Il tradizionale riferimento è a E.F. FAMA, *Efficient Capital Markets: A Review of Theory and Empirical Work*, cit., 383, sintesi delle formulazioni di modelli antecedenti: per tutti, E.F. FAMA - L. FISHER - M.C. JENSEN - R. ROLL, *The Adjustment of Stock Prices to New Information*, in 10.1. *Int. Ec. Rev.* (1969), 1, P.A. SAMUELSON, *Proof That Properly Anticipated Prices Fluctuate Randomly*, in 6.2. *Industrial Management Rev.* (1965), 41 e B. MANDELBROT, *Forecast of Future Prices, Unbiased Markets, and "Martingale" Models*, in 39.1. *The J. of Business* (1966), 242.

operare su mercati finanziari integrati» (così sempre il Considerando n. 7 del MAR, corsivo aggiunto).

L'efficacia del meccanismo in base al quale i prezzi degli strumenti finanziari "incorporano" le informazioni disponibili dipende, in buona sostanza, dal costo di raccolta, elaborazione e verifica delle informazioni[6], sostenuto dagli *information traders*, nonché dai costi relativi all'attività di arbitraggio[7]. Da un lato, le informazioni private o costose sono più difficilmente raccolte ed elaborate e, di conseguenza, "incorporate" con più lentezza nei prezzi degli strumenti finanziari, mentre al contrario la riduzione dei costi per la propria attività permette agli stessi *information traders* di individuare un maggior numero di distorsioni dei prezzi, il che rende più redditizio tale lavoro, con la conseguenza di comportare un aumento di questa tipologia di investitori e della competizione tra di loro[8]. Per altro verso, meccanismi di arbitraggio dispendiosi sono poco efficaci e ostacolano la "correzione" di eventuali distorsioni dei prezzi[9].

---

[6] La tassonomia dei costi relativi alle informazioni presentata da R.J. GILSON - R.H. KRAAKMAN, *The Mechanism of Market Efficiency*, cit., 594 ss. è stata poi sviluppata da Z. GOSHEN - G. PARCHOMOVSKY, *op. cit.*, 721.

[7] R.J. GILSON - R.H. KRAAKMAN, *Market Efficiency after the Financial Crisis: It's Still a Matter of Information Costs*, in 100 *Va L. Rev.* (2014), 330 e, aggiungendo la rilevanza dell'accesso alle informazioni rilevanti anche per la *corporate governance*, A.I. SAAD - D. STRAUSS, *The New "Reasonable Investor" and Changing Frontiers of Materiality: Increasing Investor Reliance on ESG Disclosures and Implications for Securities Litigation*, in 17:2 *Berkeley Bus. L. J.* (2020), 403. In altre parole, «quanto più le informazioni sono pubblicamente disponibili – e quindi poco costose – e quanto più nel mercato sono presenti investitori professionali in grado di elaborarle e verificarle in modo efficiente …, tanto più i prezzi tendono a riflettere completamente tutte le informazioni accessibili»: A. PERRONE, *Informazione al mercato e tutele dell'investitore*, Milano, 2003, 8.

[8] L'aumento della *disclosure* da parte di un emittente comporta, infatti: un incremento del numero di analisti finanziari che seguono il relativo titolo (C.A. BOTOSAN - M.S. HARRIS, *Motivation for a Change in Disclosure Frequency and Its Consequences: An Examination of Voluntary Quarterly Segment Disclosures*, in 38.2. *J. of Accounting Research* (2000), 352 e M.H. LANG - R.J. LUNDHOLM, *Corporate Disclosure Policy and Analyst Behavior*, in 71.4. *The Accounting Rev.* (1996), 467), nonché un incentivo per gli investitori istituzionali a partecipare nella società (B.J. BUSHEE - C.F. NOE, *Corporate Disclosure Practices, Institutional Investors, and Stock Return Volatility*, in 38 Supplement *J. of Accounting Research* (2000), 188 ss.).

[9] R.J. GILSON - R.H. KRAAKMAN, *Market Efficiency after the Financial Crisis: It's Still a Matter of Information Costs*, cit., 373, ma v. anche *ivi*, 593.

Sulla scorta del noto modello relativo al meccanismo per un mercato efficiente (c.d. *Mechanism of Market Efficiency*[10]), la regolamentazione finanziaria deve perciò ridurre i costi relativi all'attività degli *information traders* e degli arbitraggisti[11]. In altri termini, l'efficienza informativa del mercato finanziario richiede che le informazioni utili per valutare uno strumento finanziario siano facilmente accessibili[12], e, allo stesso tempo, che il processo di raccolta, verifica ed elaborazione di queste informazioni da parte degli investitori non sia ostacolato, ad esempio dalla diffusione di informazioni false e fuorvianti.

All'interno dell'Unione europea, per raggiungere questi obiettivi, da un lato, gli emittenti sono tenuti a diffondere le informazioni "rilevanti". Così, ad esempio, le società quotate devono pubblicare un prospetto informativo nel mercato primario (art. 3, par. 1, Regolamento (UE) n. 2017/1129: c.d. Regolamento Prospetto) e comunicare le informazioni privilegiate nel mercato secondario (art. 17, par. 1, MAR). Per altro verso, non è consentito intralciare il corretto funzionamento del meccanismo di formazione dei prezzi. Così, ad esempio, è vietata la «diffusione di informazioni tramite i mezzi di informazione, compreso Internet, o tramite ogni altro mezzo … 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» (art. 12, par. 1, lett. *c*, e art. 15 MAR)[13].

---

[10] Il riferimento è al *seminal work* di R.J. GILSON - R.H. KRAAKMAN, *The Mechanism of Market Efficiency*, cit., 549.

[11] Nello stesso senso, J.C. COFFEE JR., *Market Failure and the Economic Case for a Mandatory Disclosure System*, in 70.4. *Va L. Rev.* (1984), 722 e, più di recente, C.A. FROST - E.A. GORDON - A.F. HAYES, *Stock Exchange Disclosure and Market Liquidity: An Analysis of 50 International Exchanges*, in 44.3. *J. of Accounting Research* (2006), 438.

[12] Y. YADAV, *Algorithmic Trading and Market Regulation*, in W. MATTLI (ed.), *Global Algorithmic Capital Markets: High Frequency Trading, Dark Pools, and Regulatory Challenges*, Oxford, 2019, 252; nel senso che «il buon funzionamento del mercato mobiliare in quanto tale richiede la diffusione in via continuativa di informazioni complete e attendibili relative alle società quotate e agli strumenti finanziari da queste emessi», F. SARTORI, *op. cit.*, 44.

[13] Per l'affermazione secondo cui «mediante il divieto di manipolazione del mercato … l'ordinamento giuridico intende … scongiurare che informazioni false o fuorvianti non solo rallentino il processo di convergenza verso i *fundamentals* ma addirittura lo impediscano», F. CONSULICH - M. MAUGERI - C. MILIA - T.N. POLI - G.

Nelle parole del legislatore europeo, «un mercato finanziario integrato, efficiente e trasparente non può esistere senza che se ne tuteli l'integrità», sicché risulta opportuno preservare «il regolare funzionamento dei mercati mobiliari e la fiducia del pubblico nei mercati» (così il Considerando n. 2 del MAR), attraverso la previsione di un regime normativo *ad hoc* e l'attribuzione di pubblici poteri alle autorità competenti.

2. *Le peculiarità dei sistemi di intelligenza artificiale e i problemi di applicazione dei regimi di responsabilità*

In un tale contesto, la diffusione di informazioni false o fuorvianti ad opera di sistemi di intelligenza artificiale (d'ora in poi "IA"), specialmente tramite siti web, blog o *social networks* (cfr. il Considerando n. 48 del MAR: la c.d. "*mass misinformation*"[14]) minaccia l'efficienza informativa e l'integrità del mercato finanziario, compromettendo, allo stesso tempo, la fiducia del pubblico[15].

TROVATORE, *AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?*, Quaderni giuridici Consob, 2023, 35; sugli obiettivi del MAR e in particolare del divieto di abusi di mercato, di recente, F. ANNUNZIATA, *Artificial Intelligence and Market Abuse*, Cheltenham-Northampton, 2023, 8 ss. e 25 ss., ma v. già G. FERRARINI, *The European Market Abuse Directive*, in 41 *Common Market L. Rev.* (2004), 716. In Italia, «salve le sanzioni penali quando il fatto costituisce reato, è punito con la sanzione amministrativa pecuniaria da ventimila euro a cinque milioni di euro chiunque viola il divieto di manipolazione del mercato di cui all'articolo 15 del regolamento (UE) n. 596/2014» (art. 187-*ter*, co. 1, TUF).

[14] T.C.W. LIN, *The New Market Manipulation*, in 66 *Emory L. J.* (2017), 1292.

[15] Il fenomeno è stato osservato fin dalle origini: con particolare riferimento al ruolo di internet, IOSCO, *Investigating and Prosecuting Market Manipulation*, May 2000, 2 s.; avendo riguardo, invece, all'uso dei *social media* e, in particolare, di Twitter, Y. BATHAEE, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, in 31.2 *Harv. J. of L. & Tech.* (2018), 911 ss. Per la sottolineatura del rischio di manipolazione del mercato tramite sistemi di intelligenza artificiale, di recente, G. LEITNER - J. SINGH - A. VAN DER KRAAIJ - B. ZSÁMBOKI, *The rise of artificial intelligence: benefits and risks for financial stability*, in *ECB Financial Stability Review*, May 2024. Il problema è comune ad altri ambiti: ad esempio, la disinformazione in concomitanza a delle elezioni democratiche (*A Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, Proposed for public signature and announcement by technology companies at the Munich Security Conference on February 16, 2024; O. POLLICINO - P. DUNN, *Disinformazione e intelligenza artificiale*

Non sono mancati, in effetti, episodi di diffusione di *fake news* tramite i *social network* che hanno avuto impatti sulla volatilità di alcuni strumenti finanziari. Ad esempio, nel 2009, due persone avevano diffuso false notizie su alcuni titoli della Borsa di New York. Nel 2010, la falsa informazione riguardava il fatto che un aereo della compagnia australiana Qantas era precipitato in Indonesia. Nel 2013, inoltre, alcuni hacker avevano boicottato l'account Twitter dell'agenzia di stampa Associated Press diffondendo la falsa notizia di un attacco alla Casa Bianca, mentre, nello stesso anno, un investitore aveva creato falsi account Twitter di società di ricerca finanziaria che diffondevano la falsa notizia che la società Sarepta Therapeutics fosse sotto inchiesta[16]. Nel 2015, infine, un investitore aveva presentato false offerte di acquisizione per Avon e Rocky Mountain Chocolate, mentre, poco dopo, alcune persone avevano creato un falso sito web Bloomberg News per pubblicizzare un'inesistente acquisizione di Twitter[17].

Per gestire i rischi che le nuove tecnologie pongono nei mercati finanziari, risulta pertanto opportuno valutare l'efficacia dei meccanismi di *enforcement* dell'attuale sistema normativo.

In particolare, per quanto riguarda la responsabilità civile, amministrativa o penale, i sistemi di IA "forti" «dotati di capacità di autoapprendimento» e in grado produrre «*outputs* autonomi e imprevedibili rispetto agli *inputs* iniziali di produttore, programmatore o utente»[18] presentano criticità significative. Da un lato, la difficoltà di

nell'anno delle global elections: rischi (ed opportunità), in *Federalismi.it*, 2024, iv ss.; cfr. art. 3, co. 4, *Disposizioni e delega al Governo in materia di intelligenza artificiale*, Disegno di legge, Analisi tecnico-normativa, 31: d'ora in poi "DDL IA") o nel campo della medicina (L. WEIDINGER ET AL., *Taxonomy of Risks posed by Language Models*, in *FAccT*, ACM, 2022, 219).

[16] F. CONSULICH - M. MAUGERI - C. MILIA - T.N. POLI - G. TROVATORE, *op. cit.*, 62 s. e nota 170, citando M. LONGO, *Allarme social network. Così insidiano le Borse*, in *Il Sole 24 ore*, 22 marzo 2018, 1 e 3.

[17] T.C.W. LIN, *op. cit.*, 1293, ove altri esempi di "*mass misinformation*".

[18] F. CONSULICH - M. MAUGERI - C. MILIA - T.N. POLI - G. TROVATORE, *op. cit.*, 24; viceversa, i sistemi di IA "deboli" sono quelli «i cui *outputs* dipendono dalle istruzioni prestabilite da produttori, programmatori o utenti» (*ivi*, 23 s.); questi ultimi – «rule-based algorithms [that] are designed to automatically execute rules encoded by their programmers, following the classical 'if → then logic' as other types of software» – «do not put victims of harm in a fundamentally more difficult situation than other types of software»: così EUROPEAN COMMISSION, *Accompanying the*

prevedere tutti i modi in cui un sistema di IA strutturato come una *black box* si comporta[19] e la generazione di *output* autonomi[20] potrebbero escludere, rispettivamente, la presenza della colpa o del dolo. In altri termini, risulta complicato imputare la condotta ai programmatori o agli utilizzatori di questi sistemi[21], salvo che sussistano i casi di «operational failure or of the conscious use by humans»[22]. Per altro verso, «l'autonomia dei sistemi di [IA] forti complica notevolmente l'individuazione di un nesso causale tra la condotta, commissiva o omissiva, di un agente umano e l'evento produttivo di illecito»[23].

3. *Informazioni false o fuorvianti e responsabilità civile*

Nell'ambito della responsabilità civile, le caratteristiche dei sistemi di IA "forti" appena delineate rendono problematico ricorrere alle forme di responsabilità basate sulla colpa. Più idonee, invece, sembrano essere le forme di responsabilità oggettiva previste dalle normative nazionali o dalla direttiva europea sulla responsabilità del produttore per i danni derivanti da prodotti difettosi (Direttiva (UE) 2024/2853,

document Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence, Impact Assessment, Brussels, 28.9.2022 SWD(2022) 319 final, 2.

[19] A. AZZUTTI - W-G. RINGE - H.S. STIEHL, *Machine Learning, Market Manipulation and Collusion on Capital Markets: Why the "Black Box" Matters*, in 43.1. *U. of Penn. J. of Int. Law* (2021), disponibile su SSRN: *https://ssrn.com/abstract=3788872*, 90 e 115 ss.

[20] Per tutti, Y. BATHAEE, *op. cit.*, 906 ss.

[21] Con specifico riferimento agli abusi di mercato, per l'affermazione secondo cui «resta pur sempre evidente la difficoltà, anche sul piano normativo, di utilizzare per i sistemi di [IA] forti i consolidati principi generali di imputabilità, quali la causalità e la colpevolezza», F. CONSULICH - M. MAUGERI - C. MILIA - T.N. POLI - G. TROVATORE, *op. cit.*, 25; più in generale, EUROPEAN COMMISSION, *Liability for emerging digital technologies*, Working Document, Brussels, 25.4.2018, SWD(2018) 137 final, 10; v. anche N. MOLONEY, *EU Securities and Financial Market Regulation*[4], Oxford, 2023, 691.

[22] A. AZZUTTI - W-G. RINGE - H.S. STIEHL, *Machine Learning, Market Manipulation and Collusion on Capital Markets: Why the "Black Box" Matters*, cit., 116 ss.

[23] F. CONSULICH - M. MAUGERI - C. MILIA - T.N. POLI - G. TROVATORE, *op. cit.*, 25, ma v. già Y. BATHAEE, *op. cit.*, 922 ss.

c.d. *Product Liability Directive II*: d'ora in poi "PLD II")[24]: sebbene rimanga comunque difficile provare il nesso di causalità, non è necessario, di contro, dimostrare la sussistenza dell'elemento soggettivo, risolvendo così almeno il problema dell'imputabilità della condotta[25].

Più nel dettaglio, nell'Unione europea, un operatore economico è responsabile per i danni causati da un prodotto difettoso (art. 1 PLD)[26].

[24] «Per ragioni di certezza del diritto, la presente direttiva non si applica ai prodotti immessi sul mercato o messi in servizio prima del 9 dicembre 2026» (così il Considerando n. 63 della PLD II; cfr. inoltre gli artt. 2, 21 e 22 PLD II).

[25] Nelle parole del legislatore europeo, «la responsabilità oggettiva degli operatori economici rimane l'unica soluzione adeguata per affrontare il problema di una giusta ripartizione del rischio inerente alla produzione tecnologica moderna» (così il Considerando n. 2 della PLD II): nello stesso senso, affermando che «le norme nazionali vigenti in materia di responsabilità, in particolare per colpa, non sono adatte a gestire le azioni di responsabilità per danni causati da prodotti e servizi basati sull'IA», COMMISSIONE EUROPEA, *Proposta di Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale)*, Bruxelles, 28.9.2022, COM(2022) 496 final, 1 (c.d. "Proposta di AI Liability Directive": d'ora in poi "Proposta AILD"), sulla base dell'argomento secondo cui «le caratteristiche specifiche dell'IA, tra cui la complessità, l'autonomia e l'opacità (il cosiddetto effetto "scatola nera"), possono rendere difficile o eccessivamente costoso, per quanti subiscono un danno, identificare la persona responsabile e dimostrare che sussistono i presupposti ai fini dell'esito positivo di un'azione di responsabilità. In particolare, quando chiedono un risarcimento, i danneggiati potrebbero dover sostenere costi iniziali molto elevati e affrontare procedimenti giudiziari notevolmente più lunghi rispetto a quanto accade nei casi che non riguardano l'IA» (*ivi*, 1). V. anche il Considerando n. 3 della Proposta AILD e T. MADIEGA, *Artificial intelligence liability directive*, Briefing, EU Legislation in Progress, 2023, 3.

[26] La Corte di giustizia ha indicato che la PLD si applica ai prodotti utilizzati durante la fornitura di qualsiasi servizio, ma che la responsabilità di un fornitore di servizi non rientra nell'ambito di applicazione della direttiva. Tuttavia, la direttiva non impedisce agli Stati membri di applicare norme nazionali in base alle quali un fornitore di servizi che utilizza un prodotto difettoso è responsabile dei danni causati da tale utilizzo: v. EUROPEAN COMMISSION, *Liability for emerging digital technologies*, cit., 6; cfr., tuttavia, CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, *Skov Æg c Bilka Lavprisvarehus A/S and Bilka Lavprisvarehus A/S c Jette Mikkelsen and Michael Due Nielsen*, C-402/03, 10 gennaio 2006, nn. 37 e 45, secondo cui «la [PLD] dev'essere interpretata nel senso che osta ad una regola nazionale secondo la quale il fornitore risponde illimitatamente della responsabilità del produttore in base alla [PLD]». Ad esempio, «typically aircraft are subject to a strict liability regime and the

Per le peculiarità dei sistemi di IA e, in particolare, per la struttura come *black box* può risultare, tuttavia, complicato provare gli elementi richiesti dalla legge, ossia il carattere difettoso del prodotto, il danno subito e il nesso di causalità tra il difetto e il danno (art. 10 PLD II)[27]. Sembrano, invece, ormai risolte le incertezze su come e in quale misura la precedente Direttiva 85/374/CEE (c.d. *Product Liability Directive*: d'ora in poi "PLD") si applicasse a determinati tipi di difetti, come quelli derivanti dalla vulnerabilità nella sicurezza informatica del prodotto[28]. Accogliendo la richiesta di un intervento normativo[29], la nuova direttiva chiarisce, infatti, che un *software* deve essere considerato come un prodotto all'interno dell'ambito di applicazione della direttiva (cfr. i Considerando n. 6 e 13 della PLD II e art. 4, par.

party liable for damage is generally the operator[, who,] in the case of autonomous drones[, is] the person or entity that, although not remotely or manually steering it, has control on the overall use of the drone»: EUROPEAN COMMISSION, *Liability for emerging digital technologies*, cit., 12.

[27] EUROPEAN COMMISSION, *On Artificial Intelligence - A European approach to excellence and trust*, White Paper, Brussels, 19.2.2020 COM(2020) 65 final, 12 s. and EUROPEAN COMMISSION, *Accompanying the document Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence*, cit., 8, 12 ss. e 120 ss.

[28] Cfr. il Considerando n. 32 della PLD II, EUROPEAN COMMISSION, *Liability for emerging digital technologies*, cit., 17 s., EUROPEAN COMMISSION, *Accompanying the document Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence*, cit., 10 ss., e EUROPEAN COMMISSION, *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*, Impact Assessment, Brussels, 21.4.2021, SWD(2021) 84 final, PART 1/2, 8 e nota 49; più in generale, EUROPEAN COMMISSION, *Artificial Intelligence for Europe*, Communication, Brussels, 25.4.2018, COM(2018) 237 final, 16.

[29] Le nuove tecnologie sfidano l'attuale contesto normativo, in particolare basato sulla PLD, e quindi risulta opportuno un intervento legislativo: COMMISSIONE EUROPEA, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, Bruxelles, 19.2.2020 COM(2020) 64 final, 15 ss. Più in generale, e con specifico riferimento al contesto italiano, ritiene che sia «necessario» un «intervento normativo» a causa della «assenza di una normativa nazionale organica e di efficaci strumenti di tutela a favore di cittadini e imprese», DDL IA, 31.

1, PLD II)[30] e ritiene che un prodotto possa risultare difettoso «anche in ragione della sua vulnerabilità in termini di cibersicurezza», così come i fabbricanti potrebbero essere responsabili nel caso di «omissione nel fornire aggiornamenti o migliorie di sicurezza del software necessari per rimediare alle vulnerabilità del prodotto in risposta all'evoluzione dei rischi di cibersicurezza» (così i Considerando n. 32 e 51 della PLD II; artt. 7, par. 2, lett. *f*, e 11, par. 2, lett. *b* e *c*, PLD II)[31].

La PLD II introduce, inoltre, un'ipotesi di responsabilità da prodotto difettoso nel caso in cui si effettuino modifiche sostanziali a un prodotto «che venga successivamente messo a disposizione sul mercato» (così il Considerando n. 39 della PLD II) così come nel caso di produzione del bene al di fuori dell'Unione europea (Considerando n. 37 della PLD II; art. 8, par. 1, lett. *c*, PLD II). Ancora, alleggerisce l'onere della prova per i danneggiati in presenza di determinate circostanze (cfr. i Considerando n. 42, 47 e 48 della PLD II e gli artt. 9 e 10 PLD II) e, infine, estende la natura dei danni alle perdite materiali derivanti da morte o lesioni personali o alla distruzione o corruzione di dati (Considerando nn. 20, 21 e 23 della PLD II; art. 6, par. 1, lett. *a* e *c*, PLD II).

Sia pur utile a risolvere il problema dell'imputabilità della condotta, tale direttiva non sembra, tuttavia, sufficientemente adeguata a gestire il problema dell'onere della prova. La presunzione del carattere difettoso di un prodotto, infatti, si affida a una triplice ipotesi, tra cui la condizione secondo la quale «l'attore dimostra che il danno è stato

[30] Nel contesto della precedente PLD, era possibile arrivare a tale esito in via interpretativa, in base alla nozione ampia di «prodotto» (art. 2 PLD). Sostiene che la PLD «covers all types of products, ranging from raw materials to complex industrial products, now including emerging digital technology products», EUROPEAN COMMISSION, *Liability for emerging digital technologies*, cit., 6.

[31] Nel contesto della precedente PLD, era possibile arrivare a tale esito in via interpretativa, in base alla nozione ampia di prodotto «difettoso» (art. 6 PLD). Per l'affermazione secondo cui «even though products are much more complex today than in 1985, the Product Liability Directive continues to be an adequate tool. However, we need to clarify the legal understanding of certain concepts (such as product, producer, defect, damage and the burden of proof)», EUROPEAN COMMISSION, *on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products*, Report, Brussels, 7.5.2018 COM(2018) 246 final, 2.

causato da un malfunzionamento evidente del prodotto durante l'uso ragionevolmente prevedibile o in circostanze ordinarie» (art. 10, par. 2, lett. *c*, PLD II). Si presume, inoltre, l'esistenza del nesso causale quando «sia stato provato che il prodotto è difettoso e che la natura del danno cagionato è compatibile con il difetto in questione» (art. 10, par. 3, PLD II). La reale tutela degli investitori passa, inevitabilmente, dalla concreta applicazione di tali norme.

Questa soluzione non risulta, tuttavia, pienamente efficace perché la responsabilità civile richiede un'azione che non necessariamente è intrapresa da un investitore danneggiato dalle informazioni false o fuorvianti diffuse dai sistemi di IA, per i costi di transazione ad essa associati. Per tale ragione, in questo contesto la tradizionale considerazione che le norme sulla responsabilità civile forniscono incentivi economici alla parte responsabile per evitare di causare danni[32] incontra peculiari difficoltà, rendendo così la responsabilità civile di minore utilità in questo specifico contesto a prevenire le esternalità negative[33]. Più in generale, se non si possono prevedere le soluzioni che un sistema di IA può raggiungere o gli effetti che può avere, non si può nemmeno mettere in atto la condotta che la responsabilità oggettiva intende incentivare, come quella di prendere le precauzioni necessarie o di calibrare il livello di rischio che si è disposti a tollerare[34].

[32] Per tutti F. SARTORI, *op. cit.*, 211 e nota 36 ove ampi riff.

[33] In termini generali COMMISSIONE EUROPEA, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, cit., 12; affermando che solo «effective liability rules [could] provide an economic incentive to comply with safety rules and therefore contribute to preventing the occurrence of damage», Proposta AILD, 3, EUROPEAN COMMISSION, *Accompanying the document Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence*, cit., 6, e EUROPEAN COMMISSION, *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*, cit., 88.

[34] Y. BATHAEE, *op. cit.*, 894 e 931 s.

4. *Informazioni false o fuorvianti e responsabilità penale*

Priva di costi di transazione che i privati dovrebbero sopportare risulta, di contro, la possibilità di perseguire la responsabilità penale del programmatore o dell'utilizzatore del sistema di IA. Tuttavia, tale responsabilità richiede la prova del dolo: «gli Stati membri», infatti, «adottano le misure necessarie affinché la manipolazione del mercato … costituisca reato, almeno nei casi gravi e se commessa con dolo» (art. 5, par. 1, Direttiva 2014/57/UE, d'ora in poi "MAD II"). Ciò rende difficile applicarla ai sistemi di IA "forti" in quanto: (1) l'*output* non dipende dall'interazione umana e quindi manca una consapevolezza sufficientemente determinata della situazione nella quale si verifica il reato[35]; e (2) potrebbe mancare anche la volizione che, al suo livello più basso – e cioè il dolo eventuale – potrebbe sussistere solo se emerge, dalle circostanze di fatto, che l'utilizzatore del sistema di IA ha accettato la possibilità che il sistema diffondesse informazioni false o fuorvianti[36].

Meno arduo sembra, semmai, dimostrare la responsabilità da reato dell'ente che potrebbe risultare utile per via del suo effetto di deterrenza. Con specifico riferimento all'ordinamento italiano, ad

[35] F. CONSULICH, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca borsa tit. cred.*, 2018, 218 s. In via generale, «given the automated, fast, interconnected, and increasingly sophisticated nature of algorithmic trading systems due to AI, traditional liability rules and tests – eg, intent, causation, foreseeability, negligence – will find an increasingly troublesome scope of application», A. AZZUTTI - W-G. RINGE - H.S. STIEHL, *The Regulation of AI Trading from an AI Life Cycle Perspective*, EBI Working Paper Series no. 130, 2022, 22 e sostenendo che «black-box AI may do things in ways the creators of the AI may not understand or be able to predict» e quindi «intent tests become impossible to satisfy. If intent tests cannot be satisfied, laws relying on them will cease to function», Y. BATHAEE, *op. cit.*, 907. Per la verità, «anche una volta individuato il nesso causale tra *input* umano e *output* algoritmico gli illeciti di abuso di mercato richiedono, sul piano della responsabilità penale, quale elemento soggettivo indefettibile una componente intenzionale ravvisabile unicamente quando l'algoritmo sia usato come strumento per la commissione del reato», F. CONSULICH - M. MAUGERI - C. MILIA - T.N. POLI - G. TROVATORE, *op. cit.*, 37.

[36] Limitatamente al problema oggetto del presente lavoro, pare allora inefficace la proposta di modifica dell'art. 185 TUF che aumenta la pena in caso di manipolazione informativa «se i fatti sono commessi mediante l'impiego di sistemi di intelligenza artificiale» (art. 25, co. 4, DDL IA).

esempio, «la responsabilità dell'ente sussiste anche quando l'autore del reato non è stato identificato o non è imputabile» (art. 8, co. 1, lett. *a*, D. Lgs. 8 giugno 2001, n. 231)[37]. Oltre al fatto che non si applica nel caso di un individuo che utilizza un sistema di IA "forte", tale soluzione non è comunque agevole. Anzitutto, la norma italiana «continua a richiedere un fatto commesso da un individuo, pur non imputabile, punibile o individuato»[38], ciò che nel caso di specie non si verifica. Inoltre, anche qualora sia sufficiente provare il "fatto di reato", occorre dimostrare comunque anche la colpa in organizzazione della società. In terzo luogo, rimane comunque difficile individuare persone fisiche in posizione di garanzia quando il prodotto – e cioè il sistema di IA "forte" – è tipicamente opera di un *team* e non di un singolo individuo[39]. In ogni caso, è necessario da ultimo verificare se l'evento realizzato rientri o meno nel rischio consentito, perché ci sono eventi avversi che non sono puniti.

5. *Informazioni false o fuorvianti e responsabilità amministrativa*

Nel contesto della responsabilità amministrativa, è innegabile che «la semplice idoneità delle dichiarazioni non veritiere a produrre effetti sui mercati rende le stesse illecite e sanzionabili, indipendentemente dall'eventuale finalità ludica del *deepfake* e, più in generale, dalla circostanza che gli autori del *deepfake* intendano o meno manipolare il prezzo di uno o più strumenti finanziari»[40].

Allo stesso tempo, però, il divieto di manipolazione informativa si applica solo se «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*, MAR; più in generale, in Italia, è previsto che «nelle violazioni cui è applicabile una sanzione amministrativa

[37] Sul punto, F. CONSULICH, *op. cit.*, 224 ss.

[38] Così F. CONSULICH - M. MAUGERI - C. MILIA - T.N. POLI - G. TROVATORE, *op. cit.*, 82.

[39] Potrebbero, in altri termini, difettare le condizioni necessarie per imputare la responsabilità: M. COECKELBERGH, *Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability*, in 26.4. *Science and Engineering Ethics* (2020), 2055.

[40] F. CONSULICH - M. MAUGERI - C. MILIA - T.N. POLI - G. TROVATORE, *op. cit.*, 58.

ciascuno è responsabile della propria azione od omissione, cosciente e volontaria, sia essa dolosa o colposa»: art. 3 della legge 24 novembre 1981, n. 689). Di conseguenza, è necessario dimostrare la colpa o il dolo per attribuire la responsabilità di tipo amministrativo[41].

Ora, pacifica la sua sussistenza dell'elemento soggettivo nel caso di utilizzo di un sistema di IA "debole" il cui *output* dipende dagli *input* immessi dal programmatore o dall'utilizzatore[42], non è altrettanto chiaro se tale elemento sussista nel caso di utilizzo di un sistema di IA "forte". Secondo l'orientamento prevalente, i problemi menzionati in esordio (*supra*, par. 2) escludono l'esistenza di una responsabilità amministrativa: risulta difficile sostenere che, nel caso concreto, il responsabile del sistema di IA "forte" fosse – o potesse essere – a conoscenza del fatto che l'informazione specifica generata e divulgata dal sistema fosse falsa o fuorviante[43].

---

[41] Sulla necessità dell'elemento soggettivo per la responsabilità amministrativa c'è ampio dibattito. Ad esempio, con specifico riferimento all'ipotesi di invio di segnali falsi o fuorvianti, nel senso che non sia necessario l'elemento soggettivo, poiché l'esistenza di tali segnali per il mercato dovrebbe essere condotta sulla base di criteri oggettivi, CORTE AELS, *Criminal proceedings against F and G.*, causa E-5/19, 4 febbraio 2020, spec. par. 53 ss., sulla quale, *contra*, C. PICCIAU, *Recenti spunti giurisprudenziali sulla frammentaria nozione di manipolazione del mercato*, in *Nuove leggi civ. comm.*, 2020, 1304, secondo cui l'elemento soggettivo sarebbe «implicito o sottointeso nel dettato normativo europeo», non essendo possibile distinguere «tra condotte lecite e manipolazioni vietate sul piano esclusivamente oggettivo»; ritiene, invece, «disproportionate to sanction a behaviour without the mental element of the investor», V.D. TOUNTOPOULOS, *Manipulation in Illiquid Markets – A Tale of Inefficiency?*, in 14.3 *ECFR* (2017), 484; ma v. già, facendo leva sulla lettera dell'Allegato, sezione B, della proposta di direttiva c.d. MAD I, G. FERRARINI, *op. cit.*, 724 ss. Il discorso, tuttavia, non rileva nel caso della manipolazione informativa, perché la lettera dell'art. 12, par. 1, lett. *c*, MAR, suggerisce che «an intention requirement applies»: in questo senso anche N. MOLONEY, *op. cit.*, 719, da cui la cit.

[42] Infatti, «per i sistemi di [IA] deboli le regole giuridiche in vigore poss[o]no essere applicate estensivamente per contrastare tali condotte illecite»: così F. CONSULICH - M. MAUGERI - C. MILIA - T.N. POLI - G. TROVATORE, *op. cit.*, 58.

[43] Esprimono dubbi al riguardo F. CONSULICH - M. MAUGERI - C. MILIA - T.N. POLI - G. TROVATORE, *op. cit.*, 58, che suggeriscono quindi «un intervento correttivo delle fattispecie previste dal … MAR» e aggiungono, inoltre, che «per i sistemi di [IA] forti è invece necessario adottare *ex novo* criteri di imputazione della responsabilità, che rendano effettivi i presidi che tutelano il regolare funzionamento degli scambi» (*ivi*, 97); nel senso che manchi questa condizione, A. AZZUTTI - W-G.

6. (segue). *Una possibile soluzione al problema*

Una possibile soluzione per mitigare il rischio di ledere l'integrità dei mercati finanziari e compromettere la fiducia del pubblico (*supra*, par. 1) potrebbe consistere allora nel ritenere sanzionabile il comportamento dell'utilizzatore di un sistema di IA "forte" in due ipotesi: in un primo scenario, se l'utilizzatore non si attiva per rimuovere e rettificare l'informazione falsa o fuorviante inizialmente diffusa e conosciuta; in un secondo scenario, se il sistema di IA già utilizzato diffonde un'ulteriore informazione falsa o fuorviante a causa dello stesso difetto presente in occasione della prima informazione diffusa[44].

In entrambi i casi, infatti, si configura anzitutto un comportamento illecito, perché l'utilizzatore ha diffuso una informazione «tramite i mezzi di informazione, compreso Internet, o tramite ogni altro mezzo» idonea a «fissare il prezzo di mercato di uno o più strumenti finanziari a un livello anormale o artificiale» (art. 12, par. 1, lett. *c*, e art. 15 MAR). Pare possibile, inoltre, muovere un rimprovero a titolo di dolo o colpa all'utilizzatore[45], secondo un'impostazione già adottata con riferimento alle piattaforme digitali.

RINGE - H.S. STIEHL, *Machine Learning, Market Manipulation and Collusion on Capital Markets: Why the "Black Box" Matters*, cit., 118 s. e A. AZZUTTI - W-G. RINGE - H.S. STIEHL, *The Regulation of AI Trading from an AI Life Cycle Perspective*, cit., 21 s.; più di recente, F. ANNUNZIATA, *op. cit.*, 8 ss., 70 e 153 ss.

[44] Non mancano, naturalmente, ulteriori ipotesi. Ad esempio, nel caso di manipolazione informativa ad opera di una impresa di investimento che utilizzi algoritmi, potrebbero applicarsi analogicamente, per identità di *ratio*, le norme in materia di negoziazione algoritmica: nel regime di MiFID, «le imprese di investimento che effettuano negoziazione algoritmica» devono porre «in essere controlli dei sistemi e del rischio efficaci e idonei per l'attività esercitata volti a garantire che i propri sistemi di negoziazione … impediscano l'invio di ordini erronei o comunque un funzionamento dei sistemi tale da creare un mercato disordinato o contribuirvi»; le imprese di investimento devono porre «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 [MAR]» (art. 17, par. 1, MiFID II; cfr., inoltre, il Considerando n. 10 del Regolamento Delegato (UE) 2017/589). Nel testo si è preferito, nondimeno, trattare di casi più generali.

[45] Con specifico riferimento all'uso di sistemi di IA, esclude «an intentional design decision», ma ammette che ci possa essere «negligence», Y. BATHAEE, *op. cit.*, 914.

In quel contesto, i gestori delle piattaforme non sono tenuti a «ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite» all'interno del sistema e su di essi non grava «un obbligo generale di sorveglianza» sulla condotta degli utenti (art. 15, par. 1, Direttiva 2000/31/CE: c.d. *Directive on electronic commerce*, d'ora in poi "DEC"; Considerando n. 30 e art. 8 Regolamento (UE) 2022/2065: c.d. *Digital Services Act*, d'ora in poi "DSA"). Tuttavia, sono responsabili della memorizzazione e diffusione presso il pubblico delle informazioni e dei contenuti digitali forniti dagli utenti se – venuti a conoscenza della loro effettiva illiceità, o avendo colpevolmente ignorato tale circostanza – non si sono attivati «immediatamente» per rimuoverli (art. 14, par. 1, lett. *b*, DEC; Considerando n. 22 e art. 6, par. 1, lett. *b*, DSA)[46]. Stando all'orientamento giurisprudenziale in materia, la responsabilità dei gestori – che, come è evidente, sorge in un momento successivo alla diffusione delle informazioni – non è oggettiva, ma per colpa[47].

Né vale obiettare che, diversamente dal contesto delle piattaforme digitali, non sussiste un dovere esplicito di attivarsi per rimuovere o rettificare informazioni false o fuorvianti diffuse da un sistema di IA "forte". Il confronto con il regime delle piattaforme digitali, infatti, non serve a identificare un nuovo obbligo in capo agli utilizzatori di un sistema di IA "forte", ma aiuta, invece, unicamente, a comprendere che possa sussistere l'elemento soggettivo.

Ora, la soluzione proposta è *ex post* e può applicarsi solamente una volta che la prima informazione falsa è stata diffusa. Potrebbe quindi non essere pienamente efficace a prevenire esternalità negative. In

[46] Per un approfondimento, E.R. RESTELLI, *Le piattaforme digitali*, Milano, 2022, 17.

[47] Facendo leva sul fatto che «l'illegalità dell'attività» deve essere «manifesta», ritiene che il gestore della piattaforma risponda solo per dolo o colpa grave, Cass., 21 marzo 2019, n. 7708, con nota adesiva di E. TOSI, *La disciplina applicabile all'*hosting provider *per la pubblicazione di contenuti digitali protetti dal diritto di autore. Tra speciale irresponsabilità dell'ISP passivo e comune responsabilità dell'ISP attivo alla luce di Cassazione 7708/2019 e 7709/2019*, in *Riv. dir. ind.*, 2019, 245; considera, invece, «sufficiente che il prestatore di servizi sia stato, in qualunque modo, al corrente di fatti o circostanze in base alle quali un operatore economico diligente avrebbe dovuto constatare l'illiceità» dei contenuti pubblicitari, CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, *cause riunite F. Peterson c YouTube e Elsevier c Cyando*, C-682/18 - C. 683/18, 22 giugno 2021, n. 115.

attesa di interventi *de jure condendo* che attribuiscano un potere preventivo, questa strategia consente, in ogni caso, di limitare i danni derivanti da una diffusione indiscriminata di informazioni e può anche incentivare preventivamente gli utilizzatori a testare i propri sistemi di IA per evitare che si verifichino tali eventi. Infatti, sarebbe poco efficiente investire in sistemi di IA se poi l'utilizzatore fosse costretto a bloccare il sistema in caso di diffusione di informazioni false o fuorvianti[48].

7. *I poteri attribuiti al gestore del mercato finanziario e all'autorità di vigilanza competente*

In ogni caso, l'ordinamento giuridico prevede ulteriori strategie di *enforcement*, quali i poteri attribuiti al gestore del mercato finanziario e all'autorità di vigilanza competente.

Da un lato, un mercato regolamentato ha il potere «di sospendere o limitare temporaneamente le negoziazioni qualora si registri un'oscillazione significativa nel prezzo di uno strumento finanziario in tale mercato o in un mercato correlato in un breve lasso di tempo e, in casi eccezionali» ha il potere di «sopprimere, modificare o correggere qualsiasi transazione» (c.d. "*trading halt*" o "*circuit breaker*": art. 48, par. 5, Direttiva 2014/65/UE: d'ora in poi "MiFID II")[49]. Questo potere rappresenta la "prima linea di difesa" per gestire il rischio di un malfunzionamento dei mercati finanziari ed è giustificato dalla

[48] L'esito interpretativo a cui conduce l'argomentazione nel primo scenario potrebbe, nondimeno, esporsi a criticità. Perché possa essere comminata una sanzione amministrativa nel caso di manipolazione informativa ad opera di un sistema di IA "forte" è necessario, infatti, in tal caso, uno sfasamento temporale tra la commissione del fatto e il sorgere dell'elemento soggettivo. Il perseguimento di interessi pubblici suggerisce, in ogni caso, la preferenza verso la soluzione adottata. Se si ritiene, di contro, che lo sfasamento temporale impedisca l'applicazione di sanzioni amministrative, si può muovere allora verso una prospettiva *de jure condendo*: sarebbe, pertanto, opportuno che il legislatore imponesse agli utilizzatori di sistemi di IA "forti" di attivarsi immediatamente per rimuovere o rettificare informazioni false o fuorvianti diffuse.

[49] Sul punto, nella letteratura domestica e in quella statunitense, per tutti, rispettivamente, G. STRAMPELLI, *op. cit.*, 1005 e F. PARTNOY, *The Abram L. Pomeranz Lecture: Don't Blink. Snap Decisions and Securities Regulation*, in 77.1 *Brooklyn L. Rev.* (2011), 168 ss., spec. 173 ss. Per ulteriori poteri delle *trading venues*, F. ANNUNZIATA, *op. cit.*, 134 ss.

funzione di *gatekeeping* svolta dai gestori. Una pluralità di circostanze ostacola, tuttavia, l'esercizio di questo potere. Anzitutto, il rischio di qualificare l'esercizio di tale potere come manipolazione del mercato o, comunque, come una pratica anti-competitiva (es. rallentare gli ordini di investimento nel caso di *high frequency trading*: c.d. "*speed bumps*"[50]) costituisce un disincentivo all'utilizzo di tale potere. In secondo luogo, per evidenti motivi commerciali, i gestori potrebbero non essere sufficientemente incoraggiati a condurre un rigido *screening* sugli algoritmi, soprattutto quando sono in presenza di una dinamica altamente competitiva con le altre sedi di negoziazione che cercano di attirare clienti. Un ulteriore ostacolo è rappresentato, infine, dalla portata limitata della vigilanza *cross-border*, che può effettivamente essere fonte di fallimento della vigilanza[51].

Per altro verso, l'autorità di vigilanza può utilizzare i poteri interdittivi previsti dalla legge. In Italia, ad esempio, «qualora sussistano elementi che facciano presumere l'esistenza di violazioni delle norme» in materia di abusi di mercato, la Consob può, anche in via cautelare: (1) «ordinare la cessazione temporanea o permanente di qualunque pratica o condotta» (art. 187-*octies*, co. 6, lett. *a*, TUF); e (2) «adottare tutte le misure necessarie a garantire che il pubblico sia correttamente informato con riguardo, tra l'altro, alla correzione di informazioni false o fuorvianti precedentemente divulgate, anche imponendo ai soggetti interessati di pubblicare una dichiarazione di rettifica» (art. 187-*octies*, co. 6, lett. *b*, TUF). Questi poteri rappresentano la "seconda linea di difesa" e sono giustificati dalla funzione pubblica svolta dalle autorità di vigilanza. Diversamente dal potere dei mercati regolamentati, sono inoltre più facili da usare, perché il regime di responsabilità previsto per l'improprio utilizzo di tali poteri da parte delle autorità di vigilanza non ha un effetto deterrente analogo. Inoltre, diversamente dalle organizzazioni private, le autorità preposte alla vigilanza sui mercati finanziari non perseguono interessi privati che

[50] F. ANNUNZIATA, *op. cit.*, 136 s.

[51] A. AZZUTTI - W-G. RINGE - H.S. STIEHL, *Machine Learning, Market Manipulation and Collusion on Capital Markets: Why the "Black Box" Matters*, cit., 125.

possano, in qualche modo, alleviare la funzione di *gatekeeping*[52]. Infine, potendo essere un *enforcement* pubblico *ex ante*, risulta anche la strategia più efficace a prevenire esternalità negative.

8. *Le iniziative legislative promosse nell'Unione europea*

Il fenomeno affrontato è in continua evoluzione, così come il relativo regime normativo. L'Unione europea, infatti, ha adottato – o è in procinto di adottare – una pluralità di atti normativi in questo ambito.

Più nel dettaglio, con specifico riferimento alla responsabilità civile, è stata pubblicata una proposta di AI Liability Directive (Proposta AILD)[53], che consente di presumere la colpevolezza del convenuto in alcuni casi (art. 3, par. 5, Proposta AILD). Anch'essa utile per risolvere il problema dell'imputazione della condotta, soffre del medesimo limite già analizzato con riferimento alla PLD II, relativo alla prova del nesso di causalità tra la condotta e il danno. È vero che la Proposta AILD prevede la possibilità di presumere anche il nesso di causalità. Tuttavia, oltre alla dimostrazione della colpa del convenuto oppure all'affidamento del meccanismo della presunzione, si richiede che si possa «ritenere ragionevolmente probabile, sulla base delle circostanze del caso, che il comportamento colposo abbia influito sull'output prodotto dal sistema di IA» (art. 4, par. 1, lett. *a* e *b*, Proposta AILD), il che pare arduo nel caso di utilizzo di sistemi di IA "forti".

Sotto un diverso profilo, il problema della diffusione di informazioni false o fuorvianti ad opera di un sistema di IA può essere affrontato dal Regolamento (UE) 2024/1689 (c.d. *Artificial Intelligence Act*: d'ora in poi "AI Act"). In particolare, «i fornitori di sistemi di IA, compresi i

[52] A. AZZUTTI - W-G. RINGE - H.S. STIEHL, *Machine Learning, Market Manipulation and Collusion on Capital Markets: Why the "Black Box" Matters*, cit., 132 s.

[53] Questa proposta di legge vuole adattare le norme sulla responsabilità extracontrattuale, in particolare quella basata sulla colpa, all'intelligenza artificiale e, pertanto, per le ragioni già esposte (*supra*, par. 2), non sembra così efficace nel prevenire il problema discusso in questo lavoro. Alcune nuove norme potrebbero però aiutare: ad esempio, quella che consente al giudice di presumere la colpa del convenuto qualora questi non si conformi «all'ordinanza con cui l'organo giurisdizionale nazionale, nel contesto di una domanda di risarcimento del danno, gli ingiunge di divulgare o conservare gli elementi di prova a sua disposizione» (art. 3, par. 5, Proposta AILD).

sistemi di IA per finalità generali, che generano contenuti audio, immagine, video o testuali sintetici, garantiscono che gli output del sistema di IA siano marcati in un formato leggibile meccanicamente e rilevabili come generati o manipolati artificialmente» (art. 50, par. 2, AI Act). Inoltre, «i *deployer* di un sistema di IA che genera o manipola immagini o contenuti audio o video che costituiscono un "deep fake" rendono noto che il contenuto è stato generato o manipolato artificialmente» (art. 50, par. 4, co. 1, AI Act). Allo stesso modo, «i *deployer* di un sistema di IA che genera o manipola un testo pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico rendono noto che il testo è stato generato o manipolato artificialmente» (art. 50, par. 4, co. 2, AI Act). Tali informazioni devono essere «fornite alle persone fisiche interessate in maniera chiara e distinguibile al più tardi al momento della prima interazione o esposizione» (art. 50, par. 5, AI Act). Inoltre, la non conformità agli obblighi di trasparenza per i fornitori e i *deployers ex* art. 50 AI Act «è soggetta a sanzioni amministrative pecuniarie fino a 15 000 000 EUR o, se l'autore del reato è un'impresa, fino al 3 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore» (art. 99, par. 4, lett. *g*, AI Act), oltre alla possibilità per gli Stati membri di stabilire «le norme relative alle sanzioni e alle altre misure di esecuzione, che possono includere anche avvertimenti e misure non pecuniarie» in caso di violazione dell'AI Act (art. 99, par. 1, AI Act). Come emerge dall'ampio dibattito sulla funzione della trasparenza nei mercati finanziari[54], non è detto, tuttavia, che un *warning* sia completamente efficace a tutelare gli investitori e a prevenire comportamenti irrazionali. Del resto, «essere informati che un *output* è generato artificialmente non fornisce alcuna informazione sulla sua fattualità o veridicità»[55].

9. *Conclusione*

Molteplici sono le proposte *de jure condendo* avanzate per affrontare il problema discusso nel presente lavoro.

[54] Per tutti, H. KRIPKE, *The Myth of the Informed Layman*, in 28.3. *The Business Lawyer* (1973), 631.

[55] S. WACHTER - B. MITTELSTADT - C. RUSSELL, *Do large language models have a legal duty to tell the truth?*, in 11 *R. Soc. Open Sci.* (2024), 28.

Con specifico riferimento all'imputabilità della responsabilità nel caso di diffusione di informazioni false o fuorvianti ad opera di sistemi di IA "forti", l'alternativa a un approccio volto a considerare gli effetti delle loro decisioni (c.d. *outcome-based approach*) consiste nel ricollegare la responsabilità di un soggetto alla violazione di taluni obblighi, con l'obiettivo di innestare nei programmi utilizzabili delle misure di protezione volte a "neutralizzare" possibili *output* contrari agli interessi protetti dall'ordinamento[56]. Un simile modo di procedere può concretizzarsi, alternativamente, nell'imporre una verifica di conformità preventiva affidata a una terza parte oppure a controlli interni del *provider*[57], secondo una strategia già utilizzata, ad esempio, nel regime di MiFID nei confronti di una impresa di investimento che utilizzi algoritmi (art. 17, par. 1, MiFID II; cfr., inoltre, il Considerando n. 10 e gli artt. 5-10 del Regolamento Delegato (UE) 2017/589). Più nel dettaglio, si potrebbe richiedere l'adozione di un metodo per temperare i risultati casuali che possono verificarsi[58]. È vero che nel caso di sistemi di IA autonomi, costruiti come *black box*, non è chiaro se l'autorità di vigilanza disponga delle conoscenze, competente e possibilità necessarie per un adeguato controllo[59]. Allo stesso tempo, è pur vero che la previsione di tali obblighi favorisce l'individuazione (almeno) della negligenza di chi sarebbe preposto a temperare gli *output* casuali.

---

[56] Per un approfondimento teorico F. CONSULICH - M. MAUGERI - C. MILIA - T.N. POLI - G. TROVATORE, *op. cit.*, 11; per l'indicazione al Governo di introdurre fattispecie di reato «incentrate sull'omessa adozione o l'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale», cfr. l'art. 22, co. 5, lett. *b*, DDL IA.

[57] EUROPEAN COMMISSION, *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*, cit., 56 ss.

[58] Sul punto, in via generale, C. NOVELLI - F. CASOLARI - P. HACKER - G. SPEDICATO - L. FLORIDI, *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*, Working Paper, 15 March 2024, disponibile su SSRN: *https://ssrn.com/abstract=4694565*, 6.

[59] Con specifico riferimento alla negoziazione algoritmica e alle imprese di investimento, A. AZZUTTI - W-G. RINGE - H.S. STIEHL, *Machine Learning, Market Manipulation and Collusion on Capital Markets: Why the "Black Box" Matters*, cit., 124.

Intervenendo a prescindere dalla (e, quindi, anche prima della) divulgazione delle informazioni al mercato, questa ipotesi di responsabilità potrebbe essere più efficace a prevenire esternalità negative rispetto alle strategie normative *ex post* e ai poteri di vigilanza che, peraltro, sono esposti ai problemi di avere risorse necessarie[60] e della difficoltà ad individuare pratiche di manipolazione sofisticate[61]. Allo stesso tempo, non mancano controindicazioni. La proposta potrebbe, anzitutto, risultare eccessivamente costosa per il settore privato, rappresentando, per conseguenza, un ostacolo all'innovazione. Il modello di pagamento necessario nel caso di verifica ad opera di una terza parte potrebbe, inoltre, creare possibili conflitti di interesse e quindi compromettere l'efficacia della strategia normativa.

In definitiva, anche alla luce delle criticità sulle eventuali novità normative, la possibilità di irrogare sanzioni amministrative e di esercitare i poteri già attribuiti ai gestori delle sedi di negoziazione e alle autorità di vigilanza può contribuire alla discussione sulla gestione più adeguata del rischio di ledere l'integrità dei mercati e di compromettere la fiducia dei partecipanti a causa dell'utilizzo di sistemi di IA che diffondano informazioni false o fuorvianti.

[60] T.C.W. LIN, *op. cit.*, 1294 ss.
[61] T.C.W. LIN, *op. cit.*, 1296 ss.