Quaderni FinTech

Riflessioni in tema di intelligenza artificiale e attività di vigilanza

P. Deriu, S. Racioppi; con presentazione a cura di A. Lalli

15

agosto 2025

CONSOB
COMMISSIONE NAZIONALE
PER LE SOCIETÀ E LA BORSA

Nella collana dei Quaderni FinTech
sono raccolti lavori di ricerca relativi
al fenomeno «FinTech» nei suoi molteplici aspetti
al fine di promuovere la riflessione e
stimolare il dibattito su temi attinenti
all'economia e alla regolamentazione
del sistema finanziario.

CONSOB

00198 Roma - Via G.B. Martini, 3
t +39.06.84771 centralino
f +39.06.8477612

20121 Milano - Via Broletto, 7
t +39.02.724201 centralino
f +39.02.89010696

h www.consob.it
e studi_analisi@consob.it

Riflessioni in tema di intelligenza artificiale e attività di vigilanza

P. Deriu, S. Racioppi [*]

Sintesi del lavoro

Il presente lavoro analizza le implicazioni connesse all'adozione di sistemi di intelligenza artificiale (IA) nell'ambito dell'attività di vigilanza svolta dalla CONSOB. In assenza di una ricognizione sistematica sull'impiego dell'IA da parte delle amministrazioni pubbliche, si è ritenuto opportuno, in primo luogo, approfondire il quadro normativo di riferimento, nonché esaminare i più recenti orientamenti giurisprudenziali in materia. Successivamente, l'attenzione si è concentrata sul concetto di SupTech, inteso come utilizzo di tecnologie avanzate a supporto delle funzioni di vigilanza, attraverso una prima ricognizione delle principali sperimentazioni condotte da Autorità internazionali, europee e nazionali. In tale contesto, sono state esaminate in dettaglio le iniziative sperimentali avviate dalla CONSOB. Infine, dopo aver delineato i potenziali benefici e i rischi connessi all'impiego di tali tecnologie, le soluzioni SupTech sviluppate sono state analizzate alla luce dei requisiti che emergono dal quadro normativo vigente, al fine di coglierne le principali implicazioni e prospettarne possibili linee evolutive.

JEL Classifications: G18, G28, H83, K23, K24, K30, O32, O33, C55.

Keywords: intelligenza artificiale, SupTech, vigilanza data driven e risk based.

(*) Paola Deriu – Responsabile Divisione Studi e Regolamentazione, CONSOB.

Stefania Racioppi – dottoranda del XXXVIII ciclo, Facoltà di Giurisprudenza, Diritto pubblico, Sapienza Università di Roma, curriculum C - PNRR351 PA, materia di riferimento: diritto amministrativo, NEXT GEN EU, CUP 351: B83C22003030006, Missione: I.4.1 Borse PNRR Pubblica Amministrazione (Missione 4), Componente: 1.

Sono da attribuirsi alla Dott.ssa Stefania Racioppi: il Capitolo I (paragrafi 1, 1.1, 1.2, 1.3, 2, 3, 4) e il Capitolo II (paragrafi 1, 2, 3), mentre il Capitolo II (paragrafo 4), l'intero Capitolo III e le Conclusioni sono il risultato del lavoro congiunto tra le due autrici.

Si ringraziano M. Bellofiore, G. Calanchi, F. Gigante, S. La Civita, A. Limosani, C. Milia, T.N. Poli, A. Raffaelli, A. Russo, G. Trovatore, per il prezioso supporto offerto durante la scrittura e la revisione di questo lavoro. Ogni commento, suggerimento e osservazione ricevuta sono stati di grande valore. Il loro impegno e la loro dedizione ci hanno ricordato quanto sia importante il confronto costruttivo e quanto la ricerca possa beneficiare di uno sguardo critico e attento. Le opinioni espresse nel Quaderno sono attribuibili esclusivamente agli autori e non rappresentano posizioni ufficiali della CONSOB, né impegnano in alcun modo la responsabilità dell'Istituto. Nel citare il presente lavoro non è, pertanto, corretto attribuire le argomentazioni ivi espresse alla CONSOB o ai suoi vertici. Errori e imprecisioni sono imputabili esclusivamente agli autori.

Insights on Artificial Intelligence and Financial Supervision

P. Deriu, S. Racioppi [*]

Abstract

This paper explores the challenges linked to the use of artificial intelligence systems in CONSOB's market surveillance activities. Given the lack of a systematic assessment of AI adoption within public administrations, the analysis begins with an overview of the applicable legal framework and a review of recent case law. It then introduces the concept of SupTech – defined as the use of advanced technologies to enhance supervisory functions – through an initial survey of key initiatives undertaken by international, European, and national authorities. Within this context, particular attention is given to the experimental projects launched by CONSOB. Finally, the paper examines the potential benefits and risks associated with these technologies and assesses the SupTech solutions developed by CONSOB in light of current regulatory requirements, with the aim of identifying their main implications and outlining possible paths for future development.

JEL Classifications: G18, G28, H83, K23, K24, K30, O32, O33, C55.

Keywords: artificial intelligence, SupTech, data-driven and risk-based supervision.

(*) Paola Deriu – Head of the Research and Regulation Department, CONSOB.

Stefania Racioppi – PhD student 38th cycle, Faculty of Law, Public Law, Sapienza University of Rome, curriculum C - PNRR351 PA, subject of reference: administrative law, NEXT GEN EU, CUP 351: B83C22003030006, Mission: I.4.1 PNRR Public Administration Scholarships (Mission 4), Component: 1.

Stefania Racioppi wrote Chapter I (paragraphs 1, 1.1, 1.2, 1.3, 2, 3, 4) and Chapter II (paragraphs 1, 2, 3), both authors jointly wrote Chapter II (paragraph 4), the entire Chapter III, and the Conclusions.

We would like to thank M. Bellofiore, G. Calanchi, F. Gigante, S. La Civita, A. Limosani, C. Milia, T.N. Poli, A. Raffaelli, A. Russo, and G. Trovatore for their valuable support during the drafting and review of this work. All comments, suggestions, and observations received were extremely valuable. Their commitment and dedication reminded us of the importance of constructive dialogue and how research can benefit from a critical and attentive eye. The opinions expressed in this paper are solely those of the authors and do not represent the official position of CONSOB, nor do they in any way engage the responsibility of the Institute. When citing this paper, it is therefore incorrect to attribute the arguments expressed herein to CONSOB or its senior management. Errors and inaccuracies are attributable solely to the authors.

Sommario

PRESENTAZIONE 7

INTRODUZIONE 11

CAPITOLO I Il quadro normativo 15

1 Il Regolamento (UE) 2024/1689 17
- 1.1. La definizione di sistema di intelligenza artificiale 19
- 1.2. *Human centric approach* e *risk-based approach*: gli approcci alla base della disciplina 22
- 1.3. Il perimetro di applicazione, il cosiddetto effetto Brussels e l'efficacia orizzontale 27

2 Le iniziative legislative nazionali in materia di intelligenza artificiale 28

3 L'AI Act e il d.d.l. sull'intelligenza artificiale dalla prospettiva del diritto amministrativo 31

4 Le condizioni della decisione automatizzata secondo la giurisprudenza 35

CAPITOLO II Il SupTech 41

1 SupTech: una possibile definizione 43

2 Le sperimentazioni SupTech a livello nazionale 45

3 Le sperimentazioni SupTech a livello internazionale ed europeo 48

4 Le sperimentazioni SupTech della CONSOB 52

CAPITOLO III Come l'IA può supportare la vigilanza della CONSOB sugli abusi di mercato 55

1 Le fattispecie di abuso di mercato: *insider trading* e manipolazione di mercato 57

2 L'attività di *detection* finalizzata alla individuazione di potenziali casi di abuso di mercato: le cosiddette analisi preliminari 62

3 I *proof of concept* sviluppati dalla CONSOB a supporto della *detection* sugli abusi di mercato 66

4 La compatibilità delle soluzioni SupTech sviluppate dalla CONSOB rispetto al quadro regolatorio in materia di IA 69

CONCLUSIONI 73

BIBLIOGRAFIA 75

RIFERIMENTI GIURISPRUDENZIALI 84

Presentazione

A. Lalli (*)

Il Quaderno raccoglie i risultati di una ricerca su Pubblica amministrazione e tecnologie digitali, avviata nell'ambito del 38° Ciclo del Dottorato di diritto pubblico che ha sede nel Dipartimento di studi giuridici ed economici della Sapienza Università di Roma. La ricerca si è potuta giovare di una convenzione tra il Dipartimento stesso e la CONSOB. Nel panorama nazionale la CONSOB è tra le Istituzioni pubbliche che per prime hanno ritenuto di dedicare risorse umane e finanziarie alla sperimentazione dell'intelligenza artificiale (d'ora in poi anche solo IA) al fine di saggiarne le possibilità di impiego nell'esercizio delle proprie competenze e di valutarne le condizioni di legittimità. Il Quaderno illustra questa esperienza e discute le principali tematiche di rilievo tecnico e giuridico-pubblicistico connesse con l'impiego di questi nuovi strumenti da parte di un'amministrazione pubblica.

Le Autrici muovono dalla considerazione che negli ultimi anni l'IA sia divenuta un fattore trasformativo pervasivo, capace di incidere tanto sulle dinamiche economiche e sociali, quanto sull'organizzazione e sull'operatività delle pubbliche amministrazioni. In ambito finanziario, si è poi osservato che la velocità con cui i mercati evolvono e la mole di dati generata dalle negoziazioni hanno reso urgente la necessità che le autorità di vigilanza si possano dotare di strumenti nuovi, basati su tecniche avanzate di analisi dei dati, al fine di garantire la dovuta tempestività nella tutela dell'integrità dei mercati e degli investitori.

La ricerca esposta nel Quaderno indaga criticamente le opportunità e i rischi connessi all'impiego di sistemi di IA nell'attività di vigilanza della CONSOB, con particolare riguardo al contrasto degli abusi di mercato. Le Autrici percorrono tre direttrici principali esposte in tre distinti capitoli dello scritto.

Il Capitolo I ricostruisce le coordinate giuridiche entro cui si colloca ogni applicazione di IA e quindi anche quelle nel settore pubblico. Si discute in particolare il recente Regolamento (UE) 2024/1689 — l'AI Act — che introduce un modello di regolazione '*human-centric*' e '*risk-based*'. Esso definisce diversi livelli di rischio degli impieghi dell'IA e in relazione a ciascuno stabilisce distinti livelli di tutela. Si codificano

(*) Angelo Lalli - Professore associato di Diritto amministrativo, Dipartimento di Scienze giuridiche, Facoltà di Giurisprudenza, Sapienza Università di Roma.

il principio della sorveglianza umana e alcuni specifici requisiti di trasparenza che devono informare l'intero ciclo di vita dei sistemi di IA. In parallelo, lo scritto prende in esame le disposizioni rilevanti del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR) e il disegno di legge del Governo italiano in materia di intelligenza artificiale (d.d.l. S. 1146-B 'Disposizioni e deleghe al Governo in materia di intelligenza artificiale' approvato dalla Camera con modifiche il 25 giugno 2025). Quest'ultimo, nella versione allo stato approvata in prima lettura dal Parlamento, declina i princìpi delineati dal Regolamento europeo sull'IA nel contesto nazionale, dedicando una disposizione specifica all'uso dell'IA da parte delle amministrazioni pubbliche (l'art. 14). Si prospetta così un doppio binario regolatorio – e di analisi – che deve essere tenuto presente dalle autorità amministrative quando utilizzano l'IA nello svolgimento della propria attività.

Il Capitolo II introduce il concetto di SupTech – l'applicazione della tecnologia all'attività di supervisione – e ne traccia l'evoluzione in quattro generazioni che si susseguono con l'evolversi delle tecnologie (descrittiva, diagnostica, predittiva, prescrittiva). Attraverso un ampio e documentato *excursus* sulle esperienze della Securities and Exchange Commission (SEC), dell'Australian Securities and Investments Commission (ASIC) e della Monetary Authority of Singapore (MAS); della Financial Conduct Authority (FCA) del Regno Unito, dell'Autorité des Marchés Financiers (AMF) francese e del Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) tedesco, viene evidenziata la tendenza generalmente condivisa a impiegare nell'attività di vigilanza sui mercati finanziari *tool* di analisi *data-driven* (quali *natural language processing* NLP, *machine learning*, *web-scraping*), allo scopo di prevenire frodi, individuare schemi manipolativi e ottimizzare l'analisi dei flussi informativi. L'analisi comparata chiarisce che le soluzioni più mature si collocano oggi tra la seconda e la terza generazione e sono caratterizzate dall'ausilio dell'IA per la *detection* e la prioritizzazione del rischio e non viene di solito consentita la sostituzione del controllo umano.

Nel Capitolo III l'attenzione si sposta sui prototipi sviluppati dalla CONSOB in collaborazione con la Scuola Normale Superiore di Pisa. Si tratta di tre *proof of concept* basati su tecniche di *unsupervised machine learning* (*K-means clustering*, *Statistically validated networks*, *Principal component analysis* e *Autoencoder*) che supportano le analisi preliminari di *insider trading*. Questi modelli, incardinati in un impianto *human-in-the-loop*, classificano la discontinuità operativa dei soggetti, identificano '*insider rings*' e rilevano deviazioni anomale nei *pattern* di *trading*. L'adozione sperimentale di questi strumenti – affiancata da una strategia volta a sviluppare solide politiche di *data governance* e dal rafforzamento della Divisione Informatica e IA istituita nel 2024 – testimonia la volontà della CONSOB di coniugare innovazione tecnologica, efficienza istruttoria e tutela dei diritti fondamentali.

Dall'analisi condotta emerge che gli impieghi dell'IA sinora sviluppati dalla CONSOB non rientrerebbero tra i sistemi 'ad alto rischio' per i quali il Regolamento europeo sull'IA pone le più stringenti tutele, trattandosi di soluzioni che supportano (e non sostituiscono) il potere discrezionale dell'Autorità, sempre integralmente riservato all'essere umano. Del resto, gli applicativi impiegati non sono mai abilitati a incidere direttamente sui diritti individuali.

Le Autrici evidenziano come la responsabilità della decisione finale resti sempre in capo all'essere umano che è titolare della funzione amministrativa, escludendo – almeno per il momento – la possibilità di adottare provvedimenti esclusivamente automatizzati. Si sottolinea in modo particolare la necessità di valorizzare il cosiddetto presidio umano (*human-in-the-loop*), che rappresenta una garanzia fondamentale per la legittimità dell'azione amministrativa. Resta, quindi, allo stato confermato che l'utilizzo dell'IA in ambito SupTech ha essenzialmente una funzione diagnostica e predittiva, finalizzata cioè alla prioritizzazione del rischio e all'individuazione di *pattern* irregolari nei mercati finanziari e viene ribadito che la decisione amministrativa di vigilanza (sanzionatoria o conformativa) debba restare di competenza esclusiva del decisore umano. I *proof of concept* elaborati dalla CONSOB operano all'interno della fase preistruttoria del procedimento sanzionatorio in materia di abusi di mercato. Tali strumenti contribuiscono alla raccolta e all'analisi preliminare dei dati, ma non assumono di per sé valore decisorio. Si tratta, quindi, di atti endoprocedimentali, privi di effetti diretti verso i terzi, ma comunque soggetti ai principi di tracciabilità, documentazione e sindacabilità. Il provvedimento amministrativo finale con effetti sui vigilati deve sempre essere espressione di un apprezzamento umano autonomo. L'utilizzo di IA non può mai sostituire l'elemento volitivo proprio del titolare umano della funzione amministrativa.

Infine, si dedica attenzione al problema della tutela giurisdizionale e in tale contesto si afferma opportunamente che l'uso dell'IA non può compromettere il diritto alla difesa o l'accesso alle motivazioni dell'atto. Ed è perciò necessario garantire che gli algoritmi utilizzati siano conoscibili e spiegabili per permettere al giudice amministrativo di esercitare un pieno sindacato di legittimità. Si osserva, ancora opportunamente, che l'impiego di tecnologie di IA da parte delle amministrazioni comporta la necessità di adattamenti organizzativi. Nel caso della CONSOB, come anticipato, si registra la creazione di una Divisione Informatica e Intelligenza Artificiale e il rafforzamento dell'Ufficio Data Governance. Tali modifiche rispondono al principio di buon andamento (art. 97 Cost.) e alla necessità di dotare l'amministrazione delle competenze interdisciplinari necessarie. Il collasso delle competenze tecniche, che ha caratterizzato in genere l'amministrazione pubblica italiana negli ultimi tre decenni, trova in questa virtuosa esperienza una brillante eccezione.

Le Autrici sottolineano, da ultimo, la necessità di consolidare procedure di *human oversight* e *audit* continuo sui modelli usati, di assicurare la qualità e l'assenza di *bias* nei dati utilizzati, di formalizzare atti organizzativi che disciplinino finalità, categorie di dati e misure di sicurezza, in coerenza con il Regolamento GDPR e l'AI Act e di investire nella formazione del personale, affinché le necessarie competenze giuridiche, economiche e cosiddette STEM dialoghino tra loro in un'ottica di vigilanza *evidence-based*.

Nell'ambito della vigilanza finanziaria, in particolare, l'utilizzo di sistemi di IA da parte di autorità indipendenti, come la CONSOB, evidenzia una trasformazione profonda della funzione amministrativa che deve essere pensata alla luce dei principi costituzionali e normativi che ne regolano l'esercizio. L'impiego dei sistemi di IA da parte delle amministrazioni pubbliche' impone la rilettura e l'attualizzazione dei

principi di legalità, di trasparenza, dell'obbligo di motivazione dell'atto e del pieno sindacato giurisdizionale. Questo necessario adeguamento delle regole dell'amministrazione, al fine di mantenere intatti i principi dello Stato di diritto nel contesto tecnologico, deve promanare dall'attento vaglio di esperienze sperimentali concrete e interdisciplinari come quella illustrata nel Quaderno che rappresenta perciò il paradigma di una buona pratica cui anche altre amministrazioni interessate a usare i nuovi strumenti dovrebbero guardare.

Il Quaderno espone un materiale conoscitivo prezioso che arricchisce il dibattitto su questa nuova rivoluzione tecnologica che è in corso.

Introduzione

L'aumento esponenziale dell'impiego dei sistemi di intelligenza artificiale (di seguito, anche IA o intelligenza artificiale) in un'ampia gamma di settori dell'economia e della società ha reso necessaria l'adozione di regole che ne disciplinano lo sviluppo, la commercializzazione e l'uso, in modo da prevenire rischi e pregiudizi dei diritti fondamentali. A livello europeo, il recente Regolamento (UE) 2024/1689 (di seguito anche Regolamento sull'IA o AI Act) e il Regolamento (UE) 2016/679 (d'ora innanzi GDPR) costituiscono i principali riferimenti normativi per garantire che la gestione dei dati e l'uso dei sistemi di IA avvenga nel rispetto dei principi sanciti dagli artt. 2 e 6 del Trattato sull'Unione europea (TUE). Anche a livello nazionale si mostra una crescente attenzione verso la regolamentazione dell'IA, come testimonia il disegno di legge per l'introduzione di disposizioni e la delega al Governo in materia di intelligenza artificiale (d.d.l. 25 giugno 2025, successivamente anche solo d.d.l.).

L'evoluzione tecnologica investe da sempre e in maniera rilevante il settore finanziario[1]. Solo per fare alcuni esempi, l'elaborazione e l'analisi di grandi quantità di dati finanziari[2] consentono nuove e differenti strategie, amplificano le possibilità di *trading cross market* e ultraveloci, permettono di offrire nuovi servizi basati sulla

1 Filippucci, F. *et al.* (2024), The impact of Artificial Intelligence on productivity, distribution and growth: Key mechanisms, initial evidence and policy challenges, *OECD Artificial Intelligence Papers*, n. 15, OECD Publishing, Paris, (https://doi.org/10.1787/8d900037-en); v. anche Fredda, R. (2023), Analisi e proposte normative nella nuova dimensione del capital market, in *CERIDAP*, n. 4, pp. 218 ss., (DOI: 10.13130/2723-9195/2023-4-28), che osserva «*Gli algoritmi in continuo divenire, non solo sono in grado di influenzare l'efficienza nel mercato dei capitali, ma possono anche causarne manipolazioni*». V. anche Commissione europea (2021), Study on the Relevance and Impact of Artificial Intelligence for Company Law and Corporate Governance, (https://op.europa.eu/en/publication-detail/-/publication/13e6a212-6181-11ec-9c6c-01aa75ed71a1/language-en) dove si evidenzia come gli intermediari finanziari e le imprese del settore informatico e delle telecomunicazioni utilizzino strumenti di intelligenza artificiale sia per le loro attività d'impresa, sia per supportare gli assetti organizzativi e di *governance* aziendali; sul punto cfr. Ciocca, P. (2021), Audizione della CONSOB alla Camera dei Deputati, VI Commissione permanente (Finanze) Pacchetto Finanza Digitale, Roma, 8.06.2021 (https://www.consob.it/documents/1912911/1953802/Audizione_Ciocca_20210608.pdf/56379b1b-ef44-a27c-91fd-5c24274236bc).

2 Cfr. Commissione europea (2022), Commission Staff Working Document on Common European Data Spaces, Bruxelles, 23.02.2022, 6532/22, SWD (2022) 45 final, in cui i dati finanziari sono sia le informazioni societarie divulgate pubblicamente e i dati del registro delle imprese, sia i dati comunicati dalle istituzioni finanziarie alle autorità di vigilanza. I dati finanziari sono altresì i dati sui risparmi individuali, i mutui, il credito al consumo, gli investimenti, le pensioni e le assicurazioni. L'innovazione nella finanza si basa inoltre sempre di più anche su dati non finanziari. Proprio in materia di accesso ai dati finanziari, il Parlamento europeo e la Commissione hanno proposto l'adozione di un regolamento relativo a un quadro per l'accesso ai dati finanziari e che modifica i Regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010, (UE) n. 1095/2010 e (UE) 2022/2554, Bruxelles, 28.6.2023 COM (2023), 360 final 2023/0205 (COD), (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0360). Esso è volto a promuovere la creazione di un sistema di finanza aperta (*open finance*), che consenta la condivisione dei dati degli utenti tra i soggetti operanti nel settore bancario, dei servizi di investimento, assicurativi, di pagamento e finanziari, partendo dal *corpus* di norme che disciplinano il fenomeno del cosiddetto *open banking*, introdotte dalla Direttiva (UE) 2015/2366 (PSD2).

gamification (*mirror trading*, *copy-trading*), così come nuovi modelli di consulenza finanziaria automatizzata (*robo-advice*), ma anche di formulare una valutazione del merito creditizio (*credit scoring*). Stante l'impatto dell'IA nelle diverse fasi che compongono la prestazione di servizi ovvero di attività di investimento, il tema può essere analizzato da diverse prospettive.

Il punto di vista che si adotta nel presente lavoro è quello dell'impiego dei sistemi di IA nelle attività di vigilanza[3]. La complessità delle transizioni in corso nei mercati finanziari richiede lo sviluppo di un approccio di vigilanza innovativo, proattivo, *risk-driven* e *data-driven*. Il SupTech[4], letteralmente l'applicazione della tecnologia all'attività di vigilanza, consente di sviluppare *policy* e modelli di vigilanza in grado di sfruttare le capacità di analisi offerte dai sistemi di intelligenza artificiale al fine di ottimizzare le risorse e, al contempo, ridurre al minimo l'onere di segnalazione complessivo.

I sistemi di intelligenza artificiale possono essere utilizzati dalle autorità di vigilanza per analizzare grandi volumi di dati, identificando anomalie che potrebbero integrare condotte illecite, ad esempio riconducibili ad abusi di mercato o all'offerta abusiva di prodotti o servizi. Inoltre, l'IA può essere funzionale all'automatizzazione del processo di verifica della conformità alla normativa di settore in diversi ambiti di vigilanza cartolare, limitando il carico di lavoro manuale e migliorando l'accuratezza. Infine, senza con ciò esaurire l'elenco delle possibilità, i sistemi di IA potrebbero essere usati dalle Autorità in chiave predittiva, intesa quale capacità di analizzare *trend*, attraverso l'esame di serie di dati, e comprendere meglio le dinamiche evolutive dei fenomeni osservati anche in termini prospettici.

Da alcuni anni, la Commissione Nazionale per le Società e la Borsa (d'ora innanzi CONSOB) ha intrapreso un percorso di transizione digitale dei processi e di potenziamento della vigilanza *data driven* e *risk driven*, lungo un duplice fronte: oltre a supportare l'innovazione nei mercati (es. *sandbox*, *liftech*) [5], la CONSOB si è impegnata nell'elaborazione di modelli di vigilanza che sfruttino al meglio gli strumenti di intelligenza artificiale[6]. In questo ambito, grande rilievo ha assunto, da un lato, il

3 Il termine vigilanza è impiegato nel presente lavoro secondo la definizione di Amorosino, S. (2004), Tipologie e funzioni delle vigilanze pubbliche sulle attività economiche, in *Diritto amministrativo*, n. 4, p. 726, come «*tipizzazione dei poteri esercitabili dai vigilanti, che - ovviamente - sono diversi nei vari ambiti di attribuzione o competenza, e non si rinvengono sempre 'tutti insieme' e che - schematizzando - possono esser qualificati come: poteri, ex ante, di regolamentazione secondaria e di porre precetti terziari e di autorizzazione a svolgere attività; poteri continui di informazione ed ispezione (per verificare la rispondenza delle attività alle specifiche regole - giuridiche, tecniche, organizzative - che disciplinano i diversi settori di attività o mercati), e - in prosieguo poteri di conformazione dell'attività degli operatori (al limitato fine di 'rimetterli in carreggiata', cioè ricondurne l'attività nell'ambito della correttezza/conformità alle regole) e, in alcuni casi, sanzionatori, sino all'esclusione autoritativa dal mercato, o agli interventi nelle situazioni di crisi*»; cfr. anche Clarich, M. (2022), Manuale di diritto amministrativo, *Il Mulino*, Bologna, p. 275, secondo cui con il termine vigilanza si fa riferimento a una funzione che include una serie più o meno ampia di poteri istruttori e decisori.

4 Si veda Commissione europea (2020), Comunicazione relativa a una strategia in materia di finanza digitale per l'UE, Bruxelles, 24.9.2020, COM (2020) 591, nella quale il termine SupTech viene impiegato per indicare (testualmente): «la tecnologia applicata alla vigilanza è un sottoinsieme della FinTech che utilizza tecnologie innovative a sostegno dei processi di vigilanza. Aiuta le autorità di vigilanza a digitalizzare i processi di segnalazione e di regolamentazione».

5 Decreto del Ministro dell'Economia e delle Finanze 30 aprile 2021, n. 100, cosiddetto Regolamento Sandbox.

6 CONSOB (2023), Piano Strategico 2022-2024, (https://www.consob.it/web/area-pubblica/piano-strategico); CONSOB (2024), Incontro annuale con il mercato finanziario, (https://www.consob.it/documents/11973/4329955/dsc2024.pdf);

confronto con l'esperienza maturata da omologhe autorità estere nell'esplorazione delle possibilità tecnologiche e di impiego dell'IA, dall'altro lato, l'attitudine a intraprendere attività sperimentali, anche grazie alla collaborazione con il mondo accademico, volte a calare nel contesto domestico nuovi potenziali modelli di vigilanza. In particolare, sono state inizialmente intraprese attività volte a incrementare l'efficienza dei processi di elaborazione e analisi di grandi quantità di dati, dunque in ambiti di vigilanza fortemente *data driven*, tradizionalmente basati in larga parte su dati strutturati o semi strutturati. I primi prototipi sono stati sviluppati in quattro aree di diverse, che hanno riguardato:

1) la vigilanza sulle negoziazioni che hanno luogo sui mercati regolamentati e sulle piattaforme di scambio vigilate dall'Istituto, al fine di ideare strumenti di supporto alla *detection* di possibili casi di abusi di mercato; al riguardo si pone in evidenza come il presente lavoro si focalizza proprio sui prototipi sviluppati in tale ambito[7];

2) la vigilanza sui KID (*Key Information Documents*) dei PRIIPs (*Packaged Retail Investment and Insurance-based Investments Product*), ossia i documenti sintetici che illustrano le caratteristiche chiave dei prodotti finanziari, al fine di automatizzare il processo di estrazione di informazioni dai documenti, tramite tecniche di *Deep Learning* e di *Artificial Neural Networks* (ANN)[8];

3) l'attività di contrasto all'abusivismo, che, negli ultimi anni si manifesta secondo schemi operativi sempre più frequentemente basati sull'utilizzo di internet, sullo sfruttamento di nuove tecnologie e su strategie di *gamification.* Nello specifico, si fa riferimento a condotte abusive attuate tramite piattaforme di *trading*, di servizi di pagamento, di *crowdfunding*, di DLT o di *app* per cellulari;

4) l'individuazione dei casi di *greenwashing* al fine di identificare pratiche in cui affermazioni, dichiarazioni, azioni o comunicazioni relative alla sostenibilità che non riflettono in modo chiaro ed equo il profilo di sostenibilità di un'entità, un prodotto finanziario o un servizio finanziario.

Nel rimandare al Capitolo II, paragrafo 4, per una sintetica descrizione delle direttrici delle sperimentazioni condotte, e al Capitolo III per una disamina più approfondita dei prototipi a supporto della *detection* dei casi di *insider trading*, è utile

CONSOB (2025), Incontro annuale con il mercato finanziario, (https://www.consob.it/documents/d/area-pubblica/dsc2025). Nell'ambito dell'attività di ricerca e analisi della CONSOB, si vedano: Linciano, N. *et al.* (2022), L'intelligenza artificiale nell'asset e nel wealth management, *CONSOB Quaderni FinTech*, n. 9, 2022; Cosulich, F.*et al.* (2023), AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?, *CONSOB Quaderni giuridici*, n. 29; Mazzarisi, P. *et al.* (2022), A machine learning approach to support decision in *insider trading* detection, *CONSOB Quaderni FinTech*, n. 11 (https://www.consob.it/documents/1912911/1933915/FinTech_11.pdf/eebb010d-e5e8-9f75-9e77-b2a1407e418f); Ravagnani, A. *et al.* (2024), Dimensionality reduction techniques to support *insider trading* detection, *CONSOB Quaderni FinTech*, n. 12 (https://www.consob.it/documents/11973/4032571/fintech12.pdf/cc892fa7-816a-0da7-d2ec-8a26e64a6499).

7 In questi termini, CONSOB (2024), Relazione per l'anno 2023, pp. 13 ss. (https://www.consob.it/documents/11973/4329955/ra2023.pdf/ec416168-1a4d-5b3d-55f5-ced625acaa34). Ai *proof of concept* menzionati è dedicato il seguente lavoro a cui si rinvia per gli aspetti più propriamente tecnici: Mazzarisi, P. *et al.* (2022), A machine learning approach to support decision in *insider trading* detection, *CONSOB Quaderni FinTech*, n. 11.

8 Chiti, E. *et al.* (2021), Rapporto 1/2021, L'impiego dell'intelligenza artificiale nell'attività di CONSOB, AGCOM e ARERA, in *BioLaw Journal*, n. 4, pp. 211-227.

focalizzare l'attenzione sul fatto che i differenti progetti intrapresi hanno previsto solitamente quattro fasi: una prima fase di studio e sperimentazione, una seconda fase di sviluppo di casi pilota, una terza fase di attività di *backtesting*, prodromica all'ultima fase, di messa in produzione[9] con l'obiettivo ultimo di incrementare efficacia ed efficienza dell'azione della CONSOB. In generale, i prototipi di IA elaborati mirano a estrarre nuove informazioni dai dati disponibili, lasciando al controllo umano l'assunzione di decisioni volte a orientare le attività di vigilanza (ad esempio: decidere se avviare o meno un'attività istruttoria). L'estrazione di informazioni dai dati disponibili attiene ad attività di vigilanza riconducibili a una fase preistruttoria.

La reingegnerizzazione e la digitalizzazione dei processi operativi è diretta a favorire una più efficiente gestione dei dati di vigilanza. La transizione tecnologica della CONSOB dovrebbe consentire da una parte, la riduzione dei tempi e delle risorse dedicate alle attività istruttorie, dall'altra, lo snellimento dei tempi di elaborazione delle pratiche, migliorando anche i processi di interlocuzione e coordinamento tra unità operative.

In questo percorso incentrato sulla sperimentazione e sul potenziale utilizzo di sistemi di intelligenza artificiale nelle attività di vigilanza della CONSOB, è maturato un quesito di particolare rilievo, al quale il presente lavoro cerca di fornire un indirizzo, circa la compatibilità di tali sistemi con la normativa esistente. A tal fine, nel Capitolo I, è stato esplorato il quadro di riferimento sia normativo – eurounitario e nazionale – sia giurisprudenziale, esaminando i principali profili di criticità che accompagnano, in generale, le amministrazioni pubbliche nell'adozione di soluzioni IA. Il Capitolo II è volto a definire il SupTech e analizzare le principali sperimentazioni avviate a livello internazionale, europeo e nazionale. L'ultimo Capitolo è dedicato all'approfondimento dei prototipi sperimentati dalla CONSOB nell'ambito della prima delle quattro aree sopra indicate, riguardante tecniche di *machine learning* a supporto della *detection* dei casi di *insider trading*[10]. La descrizione dell'esperienza maturata nel corso della sperimentazione e lo svolgimento di osservazioni utili a rispondere al quesito circa la compatibilità di tali sistemi nell'ambito delle attività di vigilanza concludono il Quaderno.

9 Sul tema e anche per una comparazione con le sperimentazioni avviate da altre Autorità indipendenti, Chiti, E. *et al.* (2021), *op. cit.*, pp. 215-216.

10 Si rileva che la ricerca è stata condotta dalla Dott.ssa Stefania Racioppi con il coordinamento della Dott.ssa Paola Deriu non solo a livello teorico, ma anche pratico. Essa è, infatti, il frutto dell'esperienza maturata durante un periodo di sei mesi di tirocinio presso la CONSOB, nell'ambito del percorso di dottorato XXXVIII ciclo, Facoltà di Giurisprudenza, Diritto pubblico, Sapienza Università di Roma, curriculum C - PNRR351 PA della Dott.ssa Racioppi.

CAPITOLO PRIMO

Il quadro normativo

1 Il Regolamento (UE) 2024/1689

Negli ultimi anni a livello sovranazionale sono state intraprese diverse iniziative al fine di sviluppare un quadro normativo diretto a regolamentare i sistemi di IA[11]. Tra queste, il Regolamento (UE) 2024/1689 (nel prosieguo anche AI Act o Regolamento sull'IA) che stabilisce regole armonizzate sull'intelligenza artificiale[12] riveste un ruolo principale e insieme al Regolamento (UE) 2016/679 (GDPR) rappresentano le principali fonti di riferimento volte a garantire che le tecnologie emergenti siano sviluppate e utilizzate in modo etico, sicuro e nel rispetto dei diritti fondamentali.

Proprio come nel caso del GDPR, allo scopo di garantire l'uniformità e, onde evitare che gli Stati membri pregiudichino l'efficacia dell'azione dell'Unione, la scelta è ricaduta sull'adozione di un regolamento e non di una direttiva, in quanto atto avente portata generale, obbligatorio in tutti i suoi elementi e direttamente applicabile. La predilezione dello strumento regolamentare risponde all'esigenza di evitare che normative nazionali diseguali possano frammentare il mercato interno, diminuendo la certezza del diritto per gli operatori economici, la cui fiducia sarebbe così minata[13]. La natura giuridica di questo atto legislativo conferisce inoltre stabilità alla disciplina europea. Posto che la procedura per abrogare un regolamento è spesso lunga e complessa, come previsto dall'art. 294 del Trattato sul Funzionamento dell'Unione Europea (TFUE), e dal momento che l'IA può influenzare in modo significativo aspetti fondamentali della vita quotidiana, se un atto dal contenuto regolatorio fosse facilmente abrogabile, ciò potrebbe creare vuoti normativi o incertezze giuridiche, compromettendo la sicurezza delle persone. In altre parole, senza regole stabili potrebbe essere difficile prevenire e gestire i rischi legati all'uso non etico o pericoloso dell'IA.

11 Solo per citare alcune delle iniziative: Consiglio europeo (2017), Riunione del Consiglio europeo, Conclusioni, Bruxelles; Commissione europea (2018), Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, Piano coordinato sull'intelligenza artificiale, Bruxelles, COM (2018) 795 final; Commissione europea (2019), Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni (2019), Creare fiducia nell'intelligenza artificiale antropocentrica, Bruxelles, COM (2019) 168 final; Commissione europea (2020), Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia, Bruxelles, COM (2020) 65 final; Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM/2021/206 final; Proposta di direttiva del Parlamento europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale), COM/2022/496 final.

12 Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regolamento sull'intelligenza artificiale), GU L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj.

13 Così chiaramente nel considerando n. 3, Regolamento (UE) 2024/1689. Inoltre si consideri che la base legale del Regolamento (UE) 2024/1689, come nel caso del GDPR, è proprio l'art. 114 del TFUE e, secondo il Considerando n. 3, solo «[n]*ella misura in cui il presente regolamento prevede regole specifiche sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, consistenti in limitazioni dell'uso dei sistemi di IA per l'identificazione biometrica remota a fini di attività di contrasto, dell'uso dei sistemi di IA per le valutazione dei rischi delle persone fisiche a fini di attività di contrasto e dell'uso dei sistemi di IA di categorizzazione biometrica a fini di attività di contrasto, è opportuno basare il presente regolamento, per quanto riguarda tali regole specifiche, sull'articolo 16 TFUE*».

Questo aspetto si coglie in particolare ove rapportato allo scenario regolatorio degli Stati Uniti, in cui si è affermato un modello autoregolatorio (*self regulation*) e coregolatorio (*co-regulation*), basato su principi condivisi con le grandi *corporations* americane[14]. L'approccio legislativo statunitense all'intelligenza artificiale vede negli *executive orders* lo strumento principale di regolazione[15]. Gli *executive orders,* nati come direttive amministrative presidenziali, hanno assunto nel tempo un valore legislativo[16]. Guardando alla recente regolamentazione con riferimento alla materia trattata, si può osservare che l'*Executive Order (14110) on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*[17], adottato il 30 ottobre 2023 dall'allora Presidente J. Biden, si esponeva al duplice rischio di essere privato della sua efficacia non solo dal Congresso degli Stati Uniti, che ad esempio poteva rifiutarsi di stanziare il budget necessario a implementare quanto ivi previsto, ma soprattutto dal nuovo presidente eletto, il quale non è vincolato da un *executive order* emanato dal proprio predecessore[18]. Invero, tale ultima ipotesi si è verificata. Il 25 gennaio 2025, il Presidente D. J. Trump, nel revocare l'*Executive Order* (14110), ha adottato un nuovo *Executive Order (14179)* dal titolo *Removing Barriers to American AI Innovation*[19]. A differenza dell'ordine esecutivo del Presidente J. Biden, che mirava a garantire uno sviluppo sicuro, etico e responsabile dell'intelligenza artificiale, attraverso standard e test di sicurezza volti ad assicurare la protezione dalla disinformazione generata dai sistemi di IA e della privacy, nonché a prevenire la discriminazione algoritmica, il nuovo *Executive Order* è incentrato sulla promozione dell'innovazione, perseguita per mezzo della rimozione di qualsiasi controllo. Al di là di ogni considerazione politica, si vuole mettere in luce come il Regolamento sull'IA si pone all'interno di un disegno strategico diretto a far sì che l'Unione europea divenga «*leader mondiale nello sviluppo di un'IA sicura, affidabile ed etica*»[20]. Tale obiettivo viene raggiunto anche assicurando la certezza del diritto, che sembra realizzarsi non attraverso politiche legislative incerte, ma proprio grazie all'adozione di atti giuridici vincolati, come un regolamento.

Il quadro giuridico delineato dal Regolamento (UE) 2024/1689 risponde all'obiettivo di promuovere la diffusione di un'IA antropocentrica e affidabile ed è

14 Finocchiaro, G. (2024), Intelligenza artificiale. Quali regole?, *Il Mulino,* Bologna, p. 108.

15 Si veda l'*Executive Order* (13859), Federal Register (2019), vol. 84, n. 31, pp. 3967 ss. (https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf).

16 Stradella, E. (2018), I poteri normativi dell'esecutivo negli Stati Uniti: alcuni spunti ricostruttivi, in *Rivista AIC*, n. 1, pp. 1-42, in particolare pp. 20 ss.

17 *Executive Order* (14110), Federal Register (2023), Vol. 88, n. 210, pp. 75191 ss. (https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf).

18 Ruggieri, F. *et al.*, Artificial Intelligence Act: un primo sguardo al regolamento che verrà, in *Cassazione penale*, n. 3, pp. 1047-1062.

19 *Executive Order* (14179), Federal Register (2025), vol. 90, n. 20, pp. 8741 ss. (https://www.govinfo.gov/content/pkg/FR-2025-01-31/pdf/2025-02172.pdf).

20 Considerando nn. 2, 8 Regolamento (UE) 2024/1689; cfr. anche Commissione europea (2018), Comunicazione della Commissione europea, Piano coordinato sull'intelligenza artificiale (COM (2018) 795 final), Bruxelles, 7.12.2018 (https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52018DC0795). Si veda da ultimo, Commissione europea (2025), Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, AI Continent Action Plan, COM (2025) 165 final., Bruxelles, 9.4.2025, (https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan), nel quale si afferma (traduzione nostra) «*L'Unione europea è impegnata e determinata a diventare un leader globale nell'intelligenza artificiale, un continente all'avanguardia nell'IA*».

costruito secondo un approccio basato sul rischio, volto ad adattare la tipologia e il contenuto delle norme all'intensità e alla portata dei rischi che potrebbero essere generati dai sistemi di IA[21].

1.1 La definizione di sistema di intelligenza artificiale

Nel 1950 A. Turing scrisse «*I PROPOSE to consider the question, 'Can machines think?' This should begin with definitions of the meaning of the terms 'machine' and 'think'*» [22]. Il primo passo consiste dunque nel definire cosa si intende con l'espressione intelligenza artificiale.

La celerità del progresso tecnologico ha ingenerato una notevole difficoltà da parte degli interpreti nel fornire una definizione di sistema di intelligenza artificiale. Nel considerando n. 4 del Regolamento (UE) 2024/1689 si nota come l'IA consista in una 'famiglia di tecnologie' in rapida evoluzione. Ciò, tuttavia, non fa venir meno l'esigenza di approntare una definizione chiara della nozione di sistema di IA, in quanto finalizzata a garantire la certezza del diritto e ad agevolare la convergenza internazionale[23]. In dottrina è stato osservato come la ragione della difficoltà di fornire un quadro definitorio sia da rintracciare principalmente nel fatto che l'intelligenza artificiale riflette una scienza informatica e non una tecnologia specifica[24].

Di fronte alle incertezze definitorie, le istituzioni europee hanno più volte provato a delineare una nozione di intelligenza artificiale. Nel 2018 la Commissione ha approntato la seguente definizione: «*Artificial Intelligence refers to systems that display intelligent behaviour by analysing their environment and taking action – with some degree of autonomy – to achieve specific goals*»[25].

21 Considerando n. 26, Regolamento (UE) 2024/1689.

22 La storia dell'intelligenza artificiale ha origini nel secolo scorso: cfr. Turing, A.M. (1950), Computing machinery and intelligence, *Mind a Quarterly Review of Psychology and Philosophy*, vol. LIX., n. 236, pp. 433 ss. nel quale viene elaborato un test basato su un giudizio di natura controfattuale, che consente di qualificare 'intelligente' il processo computazionale di sistemi artificiali, guidati da algoritmi, qualora producano il medesimo risultato raggiungibile dall'uomo; cfr. anche Mccarthy, J. *et al.* (1955), A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, *AI Magazine*, 2006, vol. XXVII, n. 4 (https://ojs.aaai.org/aimagazine/index.php/aimagazine/issue/view/165).

23 Considerando n. 12, Regolamento (UE) 2024/1689.

24 Così Proietti, G. (2023), Le definizioni di sistemi di intelligenza artificiale nelle proposte legislative europee. Un'analisi critica, in *Dialoghi di diritto dell'economia*; cfr. Proietti, G. (2024), Definire l'indefinibile? I sistemi di intelligenza artificiale alla ricerca di un inquadramento sistematico, in *Contratto e Impresa*, n. 3, pp. 882 ss.; Consulich, F. *et al.* (2023), AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?, *CONSOB Quaderni giuridici*, n. 29, p. 7, dove si legge che i sistemi di IA si sottraggono a formulazioni linguistiche univoche in ragione della varietà delle configurazioni assunte, rappresentando così il termine intelligenza artificiale un concetto riassuntivo, «*la cui utilità risiede nell'aggregare sul piano lessicale programmi che utilizzano differenti metodi ma che appaiono tutti accomunati dal medesimo elemento funzionale: la capacità di elaborare quantità enormi di dati in tempi estremamente ravvicinati, minimizzando i tempi di latenza e contribuendo così alla soluzione efficiente di problemi che normalmente richiederebbero il concorso di diversi attori umani muniti di competenze eterogenee*». V. anche Wang, P. (2019), On Defining Artificial Intelligence, in *Journal of Artificial General Intelligence*, p. 2 dove sottolinea che senza una chiara definizione del termine è difficile per i *policy makers* valutare cosa i sistemi di IA saranno in grado di fare in futuro.

25 Commissione europea (2018), Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, Piano coordinato sull'intelligenza artificiale, Bruxelles, 7.12.2018, COM (2018) 795 final, in italiano: «*Intelligenza artificiale (IA) indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi*».

Successivamente, nella proposta di regolamento, la definizione è cambiata in favore della seguente versione «*Artificial Intelligence system (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*»[26]. A differenza della precedente, questa definizione appare più strutturata, sebbene venga stabilita una relazione biunivoca tra IA e *software*. Anche tale definizione non è apparsa, però, esaustiva.

Nelle more del procedimento legislativo di adozione del regolamento, l'Organisation for Economic Co-operation and Development (OECD) ha messo a punto la seguente definizione «*an AI system is a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment*» [27]. Tale definizione è stata integralmente ripresa, salvo lievi modifiche, nel Regolamento (UE) 2024/1689. Ai sensi dell'art. 3, par. 1, n. 1) «*AI system means a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*»[28].

Il considerando n. 12 dell'AI Act esplicita la *ratio* della definizione prescelta. La complessità e la rapidità degli sviluppi tecnologici hanno imposto l'adozione di una definizione di IA il più possibile flessibile, volta a ricomprendere al suo interno tutti i sistemi di intelligenza artificiale[29]. Nel medesimo considerando vengono fornite anche indicazioni sulle principali caratteristiche funzionali dell'IA, che la distinguono dai tradizionali sistemi *software* o dagli approcci di programmazione più semplici che utilizzano «*regole definite unicamente da persone fisiche per eseguire operazioni in modo automatico*». Una delle caratteristiche fondamentali dell'IA è la capacità

26 Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione, COM/2021/206 final, in italiano: «*un software sviluppato con una o più delle tecniche e degli approcci elencati nell'Allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono*».

27 OECD (2024), Recommendation of the Council on Artificial Intelligence, (https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449) in italiano (traduzione nostra) «*un sistema di IA è un sistema basato su una macchina che, per obiettivi espliciti o impliciti, deduce, dagli input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali. I diversi sistemi di IA variano nei loro livelli di autonomia e adattabilità dopo l'implementazione*».

28 In italiano «*Sistema di IA: 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*». Si è scelto di riportare la definizione in inglese per uniformità con le precedenti citate, di seguito le citazioni al Regolamento (UE) 2024/1689 saranno in italiano.

29 In particolare, nell'Annesso C (2025) 924 final del 06/02/2025 denominato '*Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)*' vengono ulteriormente specificati tutti i termini utilizzati e i relativi significati in termini legali.

inferenziale, ossia il «*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*»[30]. Le tecniche che consentono l'inferenza nella costruzione di un sistema di IA comprendono approcci di apprendimento automatico (*machine learning*), che imparano dai dati come conseguire determinati obiettivi, e approcci basati sulla logica e sulla conoscenza (*logic-knowledge based*), che inferiscono dalla conoscenza codificata o dalla rappresentazione simbolica del compito da risolvere. La peculiarità dei sistemi basati sull'apprendimento automatico (*machine learning based system*) è rappresentata «*dalla capacità di apprendere in autonomia come raggiungere un dato obiettivo* [...] *e di impararlo in modo sempre più efficiente con il passare del tempo. Questa caratteristica segna un cambio di rotta rispetto alle tecnologie non basate su tecniche di* machine learning*, ossia tradizionalmente operanti con un approccio logico-deduttivo (*rule-based system*)*»[31].

Sia i sistemi di IA *machine learning based*, sia quelli *logic-knowledge based* vengono sviluppati sulla base di set di dati nella fase di *training*. Si parla di *supervised learning* (SL) quando i set di dati sono sottoposti a una procedura di etichettatura (*labelled training data*), «*al fine di indurre nell'algoritmo la capacità di riconoscimento dei criteri attraverso i quali classificare ("etichettare") gli input*»[32]. Qualora invece gli algoritmi siano allenati a riconoscere i criteri rilevanti mediante tentativi ed errori, attraverso premi e punizioni, si parla di *reinforcement learning (RL).* Infine, la tecnica di *training* dell'*unsupervised learning* consente di sviluppare algoritmi che siano in grado di «*individuare i propri criteri di funzionamento direttamente dai dati di carattere non strutturato (*unlabelled training data*) che i sistemi artificiali raccolgono dal loro ambiente circostante*»[33].

La definizione di IA adottata a livello europeo è quindi basata sulle principali caratteristiche dei sistemi di IA[34], onde evitare da un lato che una definizione

30 Considerando n. 12, Regolamento (UE) 2024/1689.

31 Abriani, N., Schneider, G. (2021), Diritto delle imprese e intelligenza artificiale, *Il Mulino*, Bologna, p. 23.

32 Ivi, p. 24.

33 *Ibidem*.

34 Ai sensi dell'art. 96 del Regolamento (UE) 2024/1689, la Commissione ha approvato le Linee guida sulla definizione dei sistemi di intelligenza artificiale, nelle quali si afferma che la definizione di cui all'art. 3, par. 1, n. 1), è volta a comprendere sette elementi principali: (1) un sistema *machine-based*; (2) progettato per funzionare con diversi livelli di autonomia; (3) che può mostrare capacità di adattamento dopo l'implementazione; (4) e che, per obiettivi espliciti o impliciti; (5) deduce, dagli input che riceve, come generare output (6) quali previsioni, contenuti, raccomandazioni o decisioni (7) che possono influenzare ambienti fisici o virtuali. Tale definizione di sistema di IA (traduzione nostra) «*adotta una prospettiva basata sul ciclo di vita che comprende due fasi principali: la fase di pre-implementazione o di "costruzione" del sistema e la fase di post-implementazione o "utilizzo" del sistema. I sette elementi indicati in tale definizione non devono necessariamente essere presenti in modo continuativo in entrambe le fasi del ciclo di vita. La definizione riconosce invece che elementi specifici possono apparire in una fase, ma non necessariamente persistere in entrambe le fasi. Questo approccio alla definizione di un sistema di IA riflette la complessità e la diversità dei sistemi di IA, garantendo che la definizione sia in linea con gli obiettivi dell'*AI Act, in *quanto tiene conto di un'ampia gamma di sistemi di IA*», così Commissione europea (2025), ANNEX to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), Brussels, 6.2.2025, C(2025) 924 final, (https://digital-strategy.ec.europa.eu/it/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application).

eccessivamente ampia ricomprenda anche i *software* tradizionali, dall'altro che una definizione oltremodo ristretta escluda dall'ambito di applicazione alcuni sistemi di IA[35]. Essa appare in linea con l'obiettivo principale dell'AI Act di promuovere l'innovazione, la competitività e la crescita nel mercato unico, tutelando al contempo i diritti fondamentali, attraverso un modello regolatorio che possa rappresentare un archetipo a livello globale.

1.2 *Human centric approach* e *risk-based approach*: gli approcci alla base della disciplina

Gli approcci alla base del Regolamento sono essenzialmente due: *human centric approach* e *risk based approach*.

Il primo mira a garantire che i sistemi di IA siano sviluppati e impiegati come strumenti al servizio delle persone, migliorando il loro benessere, nel rispetto dei diritti fondamentali protetti dalla Convenzione europea sui diritti dell'uomo (CEDU) e dalla Carta dei diritti fondamentali dell'Unione europea[36]. Ciò implica che sin dalle fasi di elaborazione e di apprendimento siano previste norme che proibiscono la violazione diretta o indiretta dei diritti fondamentali[37].

Secondo gli orientamenti e le raccomandazioni del gruppo di esperti ad alto livello sull'IA istituito dalla Commissione (AI HLEG – *High Level Expert Group*)[38], espressamente richiamati nell'AI Act[39], tale approccio comporta, in concreto, che i sistemi di IA siano sviluppati e utilizzati in modo da garantire adeguati meccanismi di controllo e di *governance* dei dati, tenendo conto della qualità e dell'integrità di questi ultimi, consentendo un accesso legittimo alle informazioni. In virtù del principio di trasparenza, gli esseri umani dovrebbero essere informati, in particolare, nel caso di interazione con sistemi di IA destinati alla generazione di contenuti che possono comportare rischi specifici di impersonificazione o inganno, ovvero nelle circostanze in cui risultino esposti a sistemi di IA che, nel trattamento dei loro dati biometrici, possono identificare o inferire le emozioni o intenzioni di tali persone o assegnarle a categorie specifiche. Sarebbe inoltre opportuno adottare misure dirette a evitare distorsioni e

35 Proietti, G. (2024), Definire l'indefinibile? I sistemi di intelligenza artificiale alla ricerca di un inquadramento sistematico, *op. cit.*, 2024, p. 925.

36 Fra i primi documenti in cui si rinviene questo approccio si veda, Commissione europea (2019), Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Creare fiducia nell'intelligenza artificiale antropocentrica, Bruxelles, 8.4.2019, COM (2019) 168 final.

37 In questi termini anche la Carta Etica europea sull'utilizzo dell'Intelligenza Artificiale nei sistemi giudiziari e negli ambiti connessi, adottata dalla CEPEJ, Strasburgo, 3-4 dicembre 2018.

38 Gli orientamenti elaborati dall'AI HLEG partono dal presupposto che per ottenere un'intelligenza artificiale affidabile siano necessari tre elementi: 1) l'IA dovrebbe rispettare la legge, 2) dovrebbe osservare i principi etici e 3) dovrebbe dimostrare robustezza. Sulla base di questi tre elementi, gli orientamenti individuano sette requisiti fondamentali che le applicazioni di IA dovrebbero soddisfare per essere considerate affidabili. Essi sono: intervento e sorveglianza umani; robustezza tecnica e sicurezza; riservatezza e *governance* dei dati; trasparenza; diversità, non discriminazione ed equità; benessere sociale e ambientale; responsabilità. High-Level Expert Group on AI (2019), Ethics Guidelines for Trustworthy AI; cfr. anche i principi elaborati dall'OECD (2019), Recommendation of the council on artificial intelligence, nel quale sono elencati i seguenti principi: *Inclusive growth, sustainable development and well-being; Human-centred values and fairness; Transparency and explainability; Robustness, security and safety; Accountability.*

39 Cfr. Considerando n. 7 e n. 27, Regolamento (UE) 2024/1689.

discriminazioni. Nel promuovere la diversità e l'eguaglianza, i sistemi di IA dovrebbero essere accessibili a tutti, indipendentemente da qualsiasi fragilità e coinvolgere i portatori di interessi pertinenti durante l'intero ciclo di vita. I sistemi di IA dovrebbero essere a beneficio di tutti gli esseri umani, comprese le generazioni future. Infine, dovrebbero essere previsti meccanismi tali da garantire la responsabilità e l'*accountability* dei sistemi di IA e dei loro risultati.

La diffusa consapevolezza dei rischi connessi agli usi dell'IA per i diritti fondamentali, quali meccanismi decisionali opachi, discriminazioni basate sul genere o di altro tipo, intrusioni nelle nostre vite private o utilizzi per scopi criminali, giustifica l'introduzione di un insieme di regole vincolanti secondo un approccio basato sul rischio. Si tratta di un approccio in virtù del quale i *policy makers* identificano il rischio da gestire; selezionano un livello di tolleranza al rischio; valutano i danni e la probabilità che si verifichino; infine assegnano punteggi di rischio alle attività (ad esempio alto, medio o basso)[40].

L'architettura normativa dell'AI Act è costruita proprio partendo dall'idea che «*poiché non tutte le applicazioni di IA sono uguali, e neanche i rischi da queste derivanti lo sono, le misure di mitigazione devono essere diverse a seconda della gravità del rischio*»[41].

Sono così preliminarmente individuati quattro livelli di rischio – inaccettabile, alto, medio o specifico e minimo – in base all'impatto che i sistemi di IA possono avere sulla sicurezza e sui diritti fondamentali, quali a titolo esemplificativo la dignità umana, il rispetto della vita privata e della vita familiare, la protezione dei dati personali, la libertà di espressione e di informazione, il diritto alla non discriminazione, l'uguaglianza di genere, il diritto a un ricorso effettivo e a un giudice imparziale, i diritti della difesa e la presunzione di innocenza e il diritto a una buona amministrazione. In aggiunta e al di fuori di questi livelli di rischio, il Regolamento stabilisce norme specifiche per i «*modelli di IA per finalità generali*»[42] di cui al Capo V.

In caso di rischio inaccettabile, le pratiche di IA sono vietate. Ai sensi dell'art. 5 sono considerati vietati in termini assoluti: l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che, utilizzando tecniche subliminali o volutamente manipolative o ingannevoli oppure facendo leva sulla vulnerabilità, distorcono materialmente il comportamento di una o più persone e ne pregiudicano la capacità decisionale[43]. Sono in linea di principio vietati anche i sistemi di IA che consentono di attribuire un punteggio sociale alle persone, ovvero che permettono di classificare le

40 Kaminski, M.E. (2023), Regulating the risks of AI, in *Boston University Law Review*, vol. 103, pp. 1347-1411, p. 1405, (https://ssrn.com/abstract=4195066 or http://dx.doi.org/10.2139/ssrn.4195066).

41 Lo Sapio, G. (2022), Intelligenza artificiale: rischi, modelli regolatori, metafore, in *Federalismi.it*, n. 27, pp. 232-258, p. 238.

42 Art. 3, par. 1, n. 63) Regolamento (UE) 2024/1689 per modello di IA per finalità generali si intende «*un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato*».

43 Art. 5, par. 1, lett. a) e b); cfr. Considerando n. 29, Regolamento (UE) 2024/1689.

persone per effettuare valutazione del rischio sulla base del loro comportamento sociale o delle caratteristiche personali, quando comportino un trattamento pregiudizievole o sfavorevole[44]. Il suddetto divieto non si applica allorquando i sistemi di IA siano utilizzati a sostegno della valutazione umana circa il coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili connessi alla suddetta attività. La disposizione vieta poi i sistemi che creano o ampliano banche dati di riconoscimento facciale mediante *scraping*, ovvero sistemi di IA per inferire emozioni, a eccezione dell'uso per motivi medici o di sicurezza[45]. I sistemi di identificazione biometrica remota 'in tempo reale' in spazi accessibili al pubblico sono in linea generale vietati, a eccezione delle situazioni elencate in modo tassativo nell'Allegato II, nelle quali l'uso è strettamente necessario per perseguire un interesse pubblico rilevante che prevale sui rischi[46].

In caso di rischio alto, i sistemi di IA possono essere immessi sul mercato o utilizzati subordinatamente al rispetto di determinati requisiti obbligatori (indicati nella Sezione 2 del Capo III), a una valutazione della conformità *ex ante*[47] il cui procedimento è dettagliatamente descritto nelle sezioni 3 e seguenti del suddetto Capo e alla supervisione *ex post* da parte delle autorità nazionali.

I sistemi ad alto rischio, a cui sono dedicate la maggior parte delle disposizioni dell'AI Act, sono suddivisi in due categorie: a) quelli che costituiscono componenti di un prodotto, a prescindere dal fatto che il sistema sia fisicamente incorporato nel prodotto (integrato) o assista la funzionalità del prodotto senza esservi incorporato (non integrato), già soggetti alle normative di armonizzazione settoriali, di cui all'Allegato I (macchine, giocattoli, ascensori, apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva, apparecchiature radio, attrezzature a pressione, attrezzature per imbarcazioni da diporto, impianti a fune, apparecchi che bruciano carburanti gassosi, dispositivi medici e dispositivi medico-diagnostici in vitro); b) quelli che rientrano nell'Allegato III, cosiddetti sistemi '*stand-alone*'[48]. Questi ultimi sono classificati secondo otto aree: biometria, infrastrutture critiche, istruzione e formazione professionale, occupazione, gestione dei lavoratori e accesso al lavoro autonomo, accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi, attività di contrasto,

44 Art. 5, par. 1, lett. c) e d); cfr. Considerando nn. 31, 42, Regolamento (UE) 2024/1689.

45 Art. 5, par. 1, lett. e) e f); cfr. Considerando nn. 43, 44, Regolamento (UE) 2024/1689.

46 Art. 5, par. 1, lett. h); par. 2-7; cfr. Considerando da n. 32 a n. 39, Regolamento (UE) 2024/1689.

47 Tale valutazione della conformità *ex ante* deve poter essere svolta dall'ente (che rivesta il ruolo di fornitore/deployer/distributore) che intende avvalersi del sistema ad alto rischio. Come osservato nella dottrina straniera, Gamero Casado, E. (2021), El enfoque europeo de inteligencia artificial, in *Revista de Derecho Administrativo - CDA*, n. 20, pp. 268-289, in particolare p. 279 «*Estos sistemas no están prohibidos, pero se sujetan a una serie de restricciones y a mecanismos de control ex ante y ex post mediante los que garantizar la aplicación efectiva del Reglamento. Se trata de una luz naranja en el semáforo, puesto que estos sistemas se pueden implantar siempre que se reúnan los requisitos que el propio Reglamento establece*», in italiano (traduzione nostra) «*Questi sistemi non sono vietati, ma sono soggetti a una serie di restrizioni e a meccanismi di controllo ex ante ed ex post per garantire l'effettiva applicazione del regolamento. Si tratta di una luce arancione sul semaforo, in quanto questi sistemi possono essere implementati a condizione che siano soddisfatti i requisiti stabiliti dal regolamento stesso*».

48 Considerando n. 12, Regolamento (UE) 2024/1689.

migrazione, asilo e gestione del controllo delle frontiere, amministrazione della giustizia e processi democratici.

I primi, sistemi che costituiscono componenti di un prodotto, sono già sottoposti a valutazioni di conformità secondo la specifica normativa di settore. Pertanto, i requisiti di conformità previsti dall'AI Act dovranno essere integrati nelle relative procedure, onde evitare duplicazioni di oneri amministrativi[49]. Per i sistemi *stand-alone* si prevedono requisiti obbligatori per tutto il ciclo di vita.

Ai sensi dell'art. 9, par. 1«[i]*n relazione ai sistemi di IA ad alto rischio è istituito, attuato, documentato e mantenuto un sistema di gestione dei rischi*». Secondo il par. 2, il sistema di gestione dei rischi è un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici. Esso consta delle seguenti fasi: a) identificazione e analisi dei rischi noti e ragionevolmente prevedibili che il sistema di IA ad alto rischio, quando utilizzato conformemente alle sue finalità, può generare in relazione alla salute, alla sicurezza e ai diritti fondamentali; b) stima e valutazione dei rischi che possono emergere quando il sistema di IA ad alto rischio è usato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile; c) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato di cui all'art. 72; d) adozione di misure di gestione dei rischi opportune e mirate intese ad affrontare i rischi come sopra individuati. Al fine di individuare le misure di gestione dei rischi più appropriate e mirate, i sistemi ad alto rischio sono inoltre sottoposti a prova (art. 9, par. 6 e 7; art. 60). Tali misure sono dirette a eliminare o ridurre i rischi connessi all'uso del sistema di IA ad alto rischio, al fine di ricondurli entro livelli di rischio accettabili (art. 9, par. 5)[50].

La gestione dei rischi impone l'adozione di adeguate pratiche già a partire dalla progettazione dei processi di raccolta, trattamento e gestione dei dati[51]. Ai sensi dell'art. 10, par. 2 i set di dati di addestramento, convalida e prova sono soggetti a pratiche di *governance* e gestione adeguate alla finalità prevista del sistema di IA ad alto rischio. I dati sono considerati di elevata qualità se «*pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista*» (par. 3). I sistemi di IA ad alto rischio devono essere sviluppati e

49 Cfr. art. 8, par. 2, Regolamento (UE) 2024/1689 «*Se un prodotto contiene un sistema di IA cui si applicano i requisiti del presente regolamento e i requisiti della normativa di armonizzazione dell'Unione elencata nell'Allegato I, sezione A, i fornitori sono responsabili di garantire che il loro prodotto sia pienamente conforme a tutti i requisiti applicabili previsti dalla normativa di armonizzazione dell'Unione applicabile. Nel garantire la conformità dei sistemi di IA ad alto rischio di cui al paragrafo 1 ai requisiti di cui alla presente sezione e al fine di garantire la coerenza, evitare duplicazioni e ridurre al minimo gli oneri aggiuntivi, i fornitori possono scegliere di integrare, se del caso, i necessari processi di prova e di comunicazione nonché le informazioni e la documentazione che forniscono relativamente al loro prodotto nella documentazione e nelle procedure esistenti e richieste in conformità della normativa di armonizzazione dell'Unione elencata nell'Allegato I, sezione A*».

50 Art. 9, par. 5 Regolamento (UE) 2024/1689 «*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*».

51 La definizione di un *framework* sulla gestione del ciclo di vita delle applicazioni di IA da parte di un ente, che includa l'analisi dei rischi in fase progettuale, le funzioni coinvolte sia in fase progettuale sia nelle fasi successive può rappresentare un presidio adeguato.

progettati in modo tale da: i) garantire che il loro funzionamento sia sufficientemente trasparente (art. 13); ii) poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso (art. 14); iii) conseguire un adeguato livello di accuratezza, robustezza e cibersicurezza (art. 15). Per tale ragione, prima dell'immissione sul mercato o della messa in servizio del sistema di IA, viene redatta la documentazione tecnica volta a dimostrare la conformità dello stesso all'AI Act (art. 11).

In caso di rischi specifici, come di impersonificazione o inganno, i sistemi di IA sono soggetti a precisi obblighi di trasparenza. Ai sensi dell'art. 50, i sistemi di IA destinati a interagire direttamente con le persone fisiche devono essere progettati e sviluppati in modo tale che le persone fisiche interessate siano informate del fatto di stare interagendo con un'IA. I *deployer*[52] di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica, ovvero di un sistema di IA che genera o manipola immagini o contenuti audio o video devono informare le persone fisiche di esservi esposte.

In caso di rischio minimo, non vi sono particolari obblighi, tuttavia, ai sensi dell'art. 95, i fornitori o *deployer* dei «*sistemi di IA diversi dai sistemi di IA ad alto rischio*»[53] dovrebbero elaborare codici di condotta per garantire un'IA affidabile ovvero aderire ai codici approntati dalle organizzazioni che li rappresentano.

Ognuna di queste categorie meriterebbe un approfondimento ben più lungo, ma non compatibile con le finalità del presente lavoro. Per quanto di specifico interesse, si rileva sin da ora che nell'Allegato III sono classificati ad alto rischio i sistemi destinati a essere utilizzati per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito creditizio, a eccezione dei sistemi utilizzati allo scopo di individuare frodi finanziarie. Nel rinviare oltre, mentre i sistemi di IA utilizzati ai fini di *scoring* creditizio o assicurativo sono considerati ad alto rischio poiché potenzialmente impattanti sui diritti delle persone (si pensi ad esempio all'impossibilità di ottenere un prestito)[54], i sistemi impiegati per individuare frodi finanziarie non sono classificati come ad alto rischio in quanto fondamentali per mantenere la sicurezza e garantire l'integrità del mercato. Infine, non rientrano in questo elenco i sistemi di consulenza finanziaria, i quali tuttavia, secondo l'art. 6 potranno essere considerati ad alto rischio ove finalizzato a sostituire o influenzare la valutazione umana.

52 Ai sensi dell'art. 3, par. 1, n. 4, Regolamento (UE) 2024/1689 *deployer* è «*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*». Il termine viene impiegato in inglese anche nel testo tradotto del Regolamento (UE) 2024/1689, pertanto nel prosieguo sarà così utilizzato.

53 Locuzione usata dall'art. 95, par. 1 dalla quale si evince come tale categoria di sistemi di IA sia individuata dall'AI Act solo in via residuale.

54 Sul punto si è di recente espressa la Corte di giustizia dell'Unione europea del 7 dicembre 2023, cause riunite C-26/22 e C-64/22 e C-634/21. Sebbene la valutazione del merito creditizio venga effettuata dai creditori al fine di evitare distorsioni della concorrenza, sistemi automatizzati di *credit scoring*, basati non solo su modelli matematici e statistici, ma anche su tecnologie avanzate di *artificial intelligence* e *machine learning* spesso comportano forme di discriminazione. Sul punto si veda anche il recente studio di Bonaccorsi Di Patti, E. *et al.* (2022), Intelligenza artificiale nel credit scoring. Analisi di alcune esperienze nel sistema finanziario italiano, in Banca d'Italia *Questioni di Economia e Finanza (Occasional Papers)*, n. 721.

Per la disamina delle disposizioni del Regolamento dal punto di vista del diritto amministrativa si veda il successivo paragrafo 3.

1.3 Il perimetro di applicazione, il cosiddetto effetto Brussels e l'efficacia orizzontale

Ai sensi dell'art. 2, il Regolamento si applica ai sistemi di IA, i cui output siano utilizzati nell'Unione, a prescindere dalla circostanza che i fornitori, i *deployer* e gli utenti siano stabiliti o si trovino nel territorio dell'Unione ovvero in un paese terzo. Dal momento che l'AI Act prevede specifici requisiti, almeno per i sistemi di IA ad alto rischio, «*sarà pratico e, per economia di scala, anche economico che gli operatori di tale mercato si adeguino agli stessi standard imposti dall'Unione europea anche per rivolgersi a mercati extraeuropei (ai quali resterebbe peraltro difficile spiegare perché lo standard dovrebbe essere diverso, e in termini di sicurezza e protezione dei diritti, magari inferiore)*»[55].

Da tempo si osserva che i grandi mercati hanno un effetto gravitazionale sui produttori, spingendoli verso gli standard normativi prevalenti in questi paesi[56]. Nel momento in cui la forza vincolante delle regole e la globalizzazione dei mercati si incontrano si produce il cosiddetto *effetto Brussels*[57]. Esso si verifica quando gli operatori di un determinato mercato, dopo aver convertito i propri prodotti o le proprie pratiche commerciali per conformarsi a standard rigorosi, decidono di applicare questi nuovi standard alla propria condotta a livello mondiale[58]. Si tratta di una globalizzazione normativa unilaterale che si verifica quando un singolo Stato è in grado di esternalizzare le proprie leggi e regolamenti al di fuori dei propri confini attraverso meccanismi di mercato, dando luogo alla globalizzazione degli standard[59]. Gli standard globali emergono, però, solo quando gli operatori di mercato scelgono in maniera volontaria di conformarsi a un unico standard determinato dal regolatore più severo, rendendo obsoleti gli altri regolatori[60].

L'Unione europea ha sviluppato una vasta capacità di regolamentazione in tutti gli ambiti relativi al mercato interno, diventando l'egemone normativo mondiale, ineguagliato dai suoi rivali geopolitici[61].

55 Lo Sapio, G. (2022), Intelligenza artificiale: rischi, modelli regolatori, metafore, *op. cit.*, p. 241.

56 Drezner, D.W. (2008), All Politics is Global: Explaining International Regulatory Regimes, *Princeton University Press*, pp. 33-62.

57 Lo Sapio, G. (2022), Intelligenza artificiale: rischi, modelli regolatori, metafore, *op. cit.*, p. 241.

58 Bradford, A. (2012), The Brussels Effect, in *Northwestern University Law Review,* vol. 107, n. 1, pp. 2-64, in particolare p. 17.

59 Ivi, p. 3.

60 Ivi, p. 17.

61 Bradford, A. (2020), The Brussels Effect: How the European Union Rules the World, *Oxford University Press*, New York, consultato nell'edizione *online*, Oxford Academic, p. 18, (https://doi.org/10.1093/oso/9780190088583.001.0001).

L'AI Act, anche grazie all'approccio orizzontale e non settoriale adottato[62], favorirà l'Unione in una posizione di '*leadership by example*'[63]. L'Unione aspira, infatti, a stabilire uno standard che si imponga a livello globale, così come avvenuto in passato con il GDPR. Proprio in questo senso sembra porsi la scelta di dettare una disciplina applicabile tanto al settore privato quanto a quello pubblico[64] (si veda il paragrafo 3).

2 Le iniziative legislative nazionali in materia di intelligenza artificiale

Quasi in concomitanza con l'adozione del Regolamento europeo, il Governo ha presentato alle Camere il disegno di legge dal titolo 'Disposizioni e delega al Governo in materia di intelligenza artificiale' (di seguito anche solo d.d.l.), che disciplina l'uso dell'intelligenza artificiale nei settori demandati dal Regolamento all'autonomia normativa degli Stati membri.

Gli Stati membri svolgono un ruolo chiave nell'applicare l'AI Act. Essi devono designare almeno un'autorità di notifica e di vigilanza del mercato come autorità nazionali competenti a controllare l'applicazione e l'attuazione del Regolamento. Sono poi tenuti ad adottare tutte le misure necessarie per assicurare l'attuazione delle disposizioni, sia stabilendo sanzioni effettive, proporzionate e dissuasive in caso di violazione degli obblighi da esso stabiliti, nel rispetto del principio *ne bis in idem,* sia vigilando che le autorità competenti adottino almeno uno spazio di sperimentazione normativa per l'IA. Sul piano del riparto delle competenze, inoltre, ai sensi dell'art. 2, par. 3, il Regolamento «*non si applica a settori che non rientrano nell'ambito di applicazione del diritto dell'Unione e, in ogni caso, non pregiudica le competenze degli Stati membri in materia di sicurezza nazionale, indipendentemente dal tipo di entità incaricata dagli Stati membri di svolgere compiti in relazione a tali competenze*».

Il disegno di legge, approvato dal Senato nella seduta del 20 marzo 2025, modificato dalla Camera dei deputati il 25 giugno 2025, è stato trasmesso nuovamente al Senato il 26 giugno 2025[65]. Il testo contiene da un lato, disposizioni di carattere

62 Rispetto ad altre discipline, l'AI Act si applica trasversalmente a diversi settori e ambiti, non limitandosi a un singolo settore specifico. Questo approccio orizzontale è pensato per garantire che tutti i sistemi di IA rispettino gli stessi standard di sicurezza, trasparenza e protezione dei diritti fondamentali, riducendo i rischi associati all'uso dell'IA e promuovendo la fiducia nell'innovazione tecnologica.

63 Floridi, L. (2021), The European Legislation on AI: a Brief Analysis of its Philosophical Approach, p. 3 (https://ssrn.com/abstract=3873273 o http://dx.doi.org/10.2139/ssrn.3873273).

64 Cfr. art. 3 e considerando n. 13 Regolamento (UE) 2024/1689 in ordine alla definizione di *deployer* come qualsiasi persona fisica o giuridica, «*compresi un'autorità pubblica, un'agenzia o altro organismo, che utilizza un sistema di IA sotto la sua autorità*».

65 D.d.l. Atto Senato n. 1146, presentato in data 20 maggio 2024, annunciato nella seduta n. 191 del 21 maggio 2024. È stato assegnato alle commissioni riunite 8ª (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica) e 10ª (Affari sociali, sanità, lavoro pubblico e privato, previdenza sociale). Lo scorso 20 marzo 2025 è stato approvato dal Senato e il 24 marzo 2025, poi trasmesso alla Camera dei Deputati (Atto Camera n. 2316), assegnato alle commissioni riunite 9ª (Trasporti, poste e telecomunicazioni) e 10ª (Attività produttive, commercio e turismo). Da ultimo, è stato modificato dalla Camera dei deputati il 25 giugno 2025 e trasmesso dal presidente della Camera dei deputati alla Presidenza del Senato il 26 giugno 2025. Nel presente elaborato, ove non diversamente specificato, il riferimento è al d.d.l. approvato con modificazioni dalla Camera dei deputati e trasmesso nuovamente al Senato (S.1146-B).

immediatamente precettivo e, dall'altro, due deleghe al Governo nella medesima materia (art. 24). Esso consta di 28 articoli, che disciplinano l'impiego dell'IA in settori critici quali sanità e disabilità (art. 7), lavoro (art. 11), professioni intellettuali (art. 13), pubblica amministrazione (art. 14), attività giudiziaria (art. 15).

Al pari dell'AI Act, anche il d.d.l. si pone come obiettivo quello di salvaguardare i diritti fondamentali, la democrazia, lo Stato di diritto e la sostenibilità ambientale, promuovendo al contempo l'innovazione per il benessere dei cittadini. Ai sensi dell'art. 1, infatti, l'obiettivo del d.d.l. è la promozione di «*un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità*»[66]. Assumono particolare rilievo le norme che dettano i principi generali che devono presiedere tutto il ciclo di vita dei sistemi e dei modelli di IA, dalla fase della ricerca, sperimentazione e sviluppo fino alla fase dell'applicazione e dell'utilizzo (artt. 3, 4, 5, 6 del d.d.l.). Nel recente parere circostanziato inviato al Governo italiano, la Commissione europea aveva però messo in evidenza alcuni punti di attrito della versione originaria del d.d.l. con il Regolamento sull'intelligenza artificiale[67]. In particolare, la Commissione: aveva suggerito di inserire all'art. 1 un riferimento specifico all'AI Act, segnalando la necessità di una maggiore armonia dal punto di vista definitorio; con specifico riferimento all'utilizzo dei sistemi di IA nelle professioni intellettuali, aveva invitato il legislatore nazionale a eliminare qualsivoglia restrizione all'uso dei sistemi di IA non ad alto rischio; con riguardo agli artt. 18 e 22 del d.d.l., circa la designazione delle autorità nazionali competenti a vigilare sull'applicazione e sull'attuazione della normativa nazionale ed europea in materia di IA, aveva ricordato la necessità che le autorità fossero in possesso dello stesso livello di indipendenza previsto dalla direttiva (UE) 2016/680 per le autorità preposte alla protezione dei dati nelle attività delle forze dell'ordine, nella gestione delle migrazioni e controllo delle frontiere, nell'amministrazione della giustizia e nei processi democratici[68]. Ciò in linea con quanto previsto nel Cons. 159 dell'AI Act, ai sensi del quale «[l]*e autorità di vigilanza del mercato dovrebbero poter esercitare i loro poteri agendo in piena indipendenza. Qualsiasi limitazione del loro accesso ai dati operativi sensibili a norma del presente regolamento dovrebbe lasciare impregiudicati i poteri loro conferiti dalla direttiva (UE) 2016/680*».

Successivamente, la Commissione Giustizia del Senato, nel recepire i rilievi della Commissione europea, aveva espresso parere favorevole al d.d.l. 1146/2024,

66 D.d.l. Disposizioni e deleghe al Governo in materia di intelligenza artificiale, nella versione trasmessa dal Presidente della Camera dei deputati alla Presidenza del Senato il 26 giugno 2025, S. 1146-B (https://www.senato.it/leggi-e-documenti/disegni-di-legge/scheda-ddl?tab=datiGenerali&did=59313).

67 Commissione europea (2024), Parere circostanziato C(2024) 7814, (https://www.altalex.com/documents/news/2024/12/04/intelligenza-artificiale-commissione-ue-richiama-italia-disegno-legge).

68 Si evidenzia come, già in sede di discussione parlamentare, era stata proposta la modifica dell'art. 18 dell'originario d.d.l. a favore (quantomeno) dell'individuazione anche della Banca d'Italia, della CONSOB e dell'IVASS come autorità di riferimento per i settori di competenza, si veda Senato della Repubblica (2024), Parere approvato dalla 4a Commissione permanente sul disegno di legge n. 1146, in *Facicolo Iter D.D.L. S. 1146,* pp. 379 ss. (https://www.senato.it/leg/19/BGT/Schede/Ddliter/58262.htm).

ponendo la condizione che l'impianto normativo favorisse una maggiore libertà di sperimentazione[69].

Nel testo approvato dal Senato lo scorso 20 marzo 2025 e trasmesso alla Camera, le definizioni contenute nell'art. 2 sono state allineate a quelle dell'AI Act, attraverso specifici richiami alle disposizioni di questo. Come osservato, non si tratta solo di una questione formale, ma sostanziale, posto che le incoerenze definitorie avrebbero comportato l'incompatibilità dei relativi articoli con il Regolamento europeo[70]. Circa i principi generali, si segnala che l'art. 6, comma 2 del d.d.l. prescrive che i sistemi di IA «*destinati all'uso in ambito pubblico, fatta eccezione per quelli impiegati all'estero nell'ambito di operazioni militari, devono essere installati su server ubicati nel territorio nazionale, al fine di garantire la sovranità e la sicurezza dei dati sensibili dei cittadini*». La norma così concepita, al fine di non essere ritenuta incompatibile con il diritto sovranazionale, avrebbe richiesto un necessario coordinamento con il principio della libera circolazione dei servizi nel mercato unico e con il *business model* dei grandi fornitori di *cloud*, fondata anche sulla distribuzione più conveniente possibile dei *server*[71]. Per tale ragione – anticipando il contenuto delle modifiche apportate al d.d.l. dalla Camera dei deputati – il comma 2 dell'art. 6 del d.d.l. è stato soppresso. Come detto, il disegno di legge detta poi disposizioni specifiche per diversi settori. Per quanto di interesse, nel rinviare la disamina dell'art. 14 sull'impiego dell'IA da parte delle pubbliche amministrazioni, appare opportuno menzionare l'art. 20. Ai sensi di tale disposizione, l'Agenzia per l'Italia Digitale (AgID) e l'Agenzia per la Cybersicurezza Nazionale (ACN) sono designate quali Autorità nazionali per l'intelligenza artificiale, ferme restando le attribuzioni alla Banca d'Italia, alla CONSOB e all'IVASS del ruolo di autorità di vigilanza del mercato, secondo quanto previsto dall'art. 74, par. 6, del Regolamento sull'IA[72].

Il testo del disegno di legge, come già rilevato, è stato da ultimo modificato dalla Camera dei deputati e trasmesso nuovamente al Senato (S. 1146-B). Nell'ultima versione si segnala la modifica del comma 4 dell'art. 3, recante i principi generali, dove si specifica che l'impiego dei sistemi di IA non deve pregiudicare lo svolgimento con metodo democratico della vita istituzionale e politica e «*non deve altresì pregiudicare la libertà del dibattito democratico da interferenze illecite, da chiunque provocate, tutelando gli interessi della sovranità dello Stato nonché i diritti fondamentali di ogni cittadino riconosciuti dagli ordinamenti nazionale ed europeo*»[73]. Si segnala, inoltre, che

69 Berto, L. (2025), Il parere della Commissione Giustizia del Senato sul disegno di legge sull'intelligenza artificiale, in *Diritto e Giustizia, Il quotidiano dell'Informazione Giuridica.*

70 Berto, L. (2025), Il Senato approva il disegno di legge sull'intelligenza artificiale, in *Diritto e Giustizia, Il quotidiano dell'Informazione Giuridica.*

71 *Ibidem.*

72 Ai sensi dell'art. 74, par. 6 del Regolamento (UE) 1689/2024, per i sistemi di IA ad alto rischio messi in servizio o usati da istituti finanziari, l'autorità di vigilanza ai fini dell'applicazione del regolamento resta l'autorità nazionale pertinente responsabile della vigilanza finanziaria. Per tale ragione in sede di discussione parlamentare è stata proposta la modifica dell'art. 18 dell'originario d.d.l. (si fa riferimento, in questo caso, al d.d.l. S. 1146) a favore dell'individuazione anche della Banca d'Italia, della CONSOB e dell'IVASS come autorità di riferimento per i settori di competenza, v. Senato della Repubblica (2024), Parere approvato dalla 4a Commissione permanente sul disegno di legge n. 1146, in *Fascicolo Iter D.D.L. S. 1146,* pp. 379 ss. (https://www.senato.it/leg/19/BGT/Schede/Ddliter/58262.htm).

73 Art. 3, comma 4, d.d.l. Disposizioni e delega al Governo in materia di intelligenza artificiale, S.1146-B.

al fine di armonizzare la normativa nazionale e quella europea, l'art. 4 contiene uno specifico riferimento al GDPR, nonché al d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali). Proseguendo l'analisi (seppur breve, considerate le finalità del presente Quaderno), l'art. 14 dedicato all'impiego dei sistemi di IA da parte delle pubbliche amministrazioni è rimasto invariato, mentre l'art. 19 istituisce il Comitato di coordinamento delle attività di indirizzo sugli enti, organismi e fondazioni che operano nel campo dell'innovazione digitale e dell'intelligenza artificiale[74]. Ai sensi del neo-introdotto comma 6 dell'art. 19 del d.d.l., alle sedute del Comitato possono prendere parte le Autorità nazionali indicate nell'art. 20 del d.d.l..

Tuttavia, poiché la disposizione richiamata menziona sia le autorità competenti in materia di intelligenza artificiale – come l'Agenzia per l'Italia Digitale (AgID) e l'Agenzia per la Cybersicurezza Nazionale (ACN) – sia altre autorità, quali la Banca d'Italia, la CONSOB, l'IVASS e il Garante per la protezione dei dati personali, potrebbe essere opportuno chiarire con maggiore precisione a quali soggetti ci si riferisce. Da ultimo si rileva che il Comitato svolge sia funzioni di coordinamento che di indirizzo delle politiche di formazione nelle competenze digitali e dell'IA. Infine, in ordine alle Autorità nazionali per l'intelligenza artificiale, l'art. 20 non ha subito modificazioni, attribuendo tale ruolo all'Agenzia per l'Italia Digitale (AgID) e all'Agenzia per la Cybersicurezza Nazionale (ACN), salve le attribuzioni a Banca d'Italia, CONSOB e IVASS quali autorità di vigilanza del mercato.

3 L'AI Act e il d.d.l. sull'intelligenza artificiale dalla prospettiva del diritto amministrativo

Come già evidenziato, il Regolamento sull'IA si fonda sull'art. 114 del TFUE ed è diretto a garantire la libera circolazione dei sistemi di intelligenza artificiale. Le sue disposizioni si applicano tanto ai soggetti privati quanto alle pubbliche amministrazioni[75]. L'AI Act non contiene, però, alcuna disposizione il cui titolo cita espressamente l'uso dei sistemi di intelligenza artificiale da parte delle pubbliche amministrazioni, nonostante queste ultime, a livello sovranazionale e nazionale ne abbiano già sperimentato l'impiego in diversi settori[76].

74 Art. 19, comma 6, d.d.l. Disposizioni e delega al Governo in materia di intelligenza artificiale, S.1146-B, il Comitato è presieduto dal Presidente del Consiglio dei ministri o dall'autorità politica delegata e composto dai seguenti soggetti, o da loro delegati: Ministro dell'economia e delle finanze; Ministro delle imprese e del made in Italy; Ministro dell'università e della ricerca; Ministro della salute; Ministro della Pubblica amministrazione; Autorità politica delegata per la sicurezza della Repubblica e in materia di cybersicurezza; Autorità politica delegata in materia di innovazione tecnologica e transizione digitale.

75 Puigpelat, O.M. (2023), The impact of the AI Act on public authorities and on administrative procedures, in *CERIDAP*, n. 4, pp. 238-252 (DOI: 10.13130/2723-9195/2023-4-6).

76 Cfr. Cavallo Perin, R. (2020), Ragionando come se la digitalizzazione fosse data, *in Diritto amministrativo*, n. 2, pp. 305-328, che parte da questo presupposto. In dottrina amministrativa si v. Galetta, D.U., Corvalan, J.G. (2019), Intelligenza artificiale per una pubblica amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto, in *Federalismi.it*, n. 3 (https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=38014); Galetta, D. U. (2020). Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia, in *Rivista Italiana di Diritto Pubblico Comunitario*, n. 3, pp. 501 ss.; Costantino, F. (2019), Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data, in *Diritto pubblico*, n. 1, p. 43-70;

Al contrario, l'art. 14 del d.d.l. in materia di intelligenza artificiale tratta specificamente dell'uso dell'IA da parte delle pubbliche amministrazioni. Tale disposizione prevede che l'IA deve essere utilizzata allo scopo di incrementare l'efficienza dell'attività amministrativa, ridurre i tempi di definizione dei procedimenti e aumentare la qualità e la quantità dei servizi erogati ai cittadini e alle imprese, assicurando agli interessati la conoscibilità del suo funzionamento e la tracciabilità del suo utilizzo (comma 1). L'impiego dei sistemi di IA deve avvenire in funzione strumentale e di supporto all'attività provvedimentale, nel rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata (comma 2). Infine, dispone che le pubbliche amministrazioni adottino misure tecniche, organizzative e formative finalizzate a garantire un utilizzo dell'IA responsabile e a sviluppare le capacità trasversali degli utilizzatori (comma 3).

Nell'AI Act è comunque possibile rinvenire alcune disposizioni in ordine all'uso dei sistemi di IA da parte delle pubbliche amministrazioni. Ai sensi dell'Allegato III, par. 5, fra i sistemi di IA *stand-alone* ad alto rischio vi sono quelli destinati a essere utilizzati dalle autorità pubbliche, o per conto di esse, per valutare l'accesso a servizi pubblici essenziali o per consentirne la fruizione. Ciò in quanto le persone fisiche che chiedono o ricevono prestazioni e servizi essenziali di assistenza pubblica, come ad esempio servizi sanitari o servizi sociali, si trovano generalmente in una posizione di vulnerabilità e di soggezione rispetto alla decisione assunta dalle autorità pubbliche[77]. Resta fermo, a ogni modo, l'intento perseguito dall'AI Act di non ostacolare «*lo sviluppo e l'utilizzo di approcci innovativi nella pubblica amministrazione, che trarrebbero beneficio da un uso più ampio di sistemi di IA conformi e sicuri, a condizione che tali sistemi non comportino un rischio alto per le persone fisiche e giuridiche*»[78]. In tale direzione depone quanto previsto dall'art. 6, par. 3, comma 1, ai sensi del quale non sono considerati ad alto rischio i sistemi di IA destinati a non influenzare materialmente l'esito del processo decisionale[79]. Tale norma si applica al ricorrere di almeno una delle condizioni previste dal comma 2, ossia il sistema di IA è destinato: a) a eseguire un compito procedurale limitato; b) ovvero a migliorare il risultato di un'attività umana precedentemente completata; c) o a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è finalizzato a sostituire o influenzare

Falcone, M. (2023), Ripensare il potere conoscitivo pubblico tra algoritmi e Big Data, *Editoriale Scientifica*, Napoli; Lalli, A. (2024), La regolazione pubblica delle tecnologie digitali e dell'intelligenza artificiale, *G. Giappichelli*, Torino; Falletti, E. (2023), Mai accettare caramelle né atti amministrativi da sconosciuti, ancorché algoritmi, in *Il diritto dell'informazione e dell'informatica*, n. 1, pp. 97 ss.; Piras, P. (2020). Il tortuoso cammino verso un'amministrazione nativa digitale, in *Diritto dell'informazione e dell'Informatica*, n. 1, pp. 43 ss.; Rangone, N. (2022). Le pubbliche amministrazioni alla prova dell'intelligenza artificiale, in AA.VV., Liber Amicorum per Marco D'Alberti, *G. Giappichelli*, Torino, pp. 494 ss.; Torchia, L. (2022). Lo Stato digitale e il diritto amministrativo in AA.VV., Liber Amicorum per Marco D'Alberti, *G. Giappichelli*, Torino, pp. 477 ss.

77 Considerando n. 58, Regolamento (UE) 2024/1689.

78 Considerando n. 58, Regolamento (UE) 2024/1689.

79 Cfr. anche considerando n. 53, Regolamento (UE) 2024/1689 che definisce un sistema di IA che non influenza materialmente l'esito del processo decisionale come «*un sistema di IA che non ha impatto sulla sostanza, e quindi sull'esito, del processo decisionale umano o automatizzato*». Tali sistemi potrebbero, alternativamente o cumulativamente essere destinati a classificare documenti in entrata per categorie, a rilevare duplicati, ovvero a migliorare il linguaggio in documenti già redatti, oppure a gestire fascicoli.

la valutazione umana precedentemente completa, senza un'adeguata revisione umana; d) oppure a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'Allegato III. La suddetta deroga non trova comunque applicazione nelle ipotesi in cui il sistema effettui la profilazione di persone fisiche (comma 3). La norma, se rapportata alla disciplina del procedimento amministrativo, sembra far riferimento ad almeno due ipotesi. La prima è quella per cui gli output dei sistemi di IA non emergano direttamente dall'atto conclusivo del procedimento, ma costituiscano un atto endoprocedimentale della fase istruttoria[80] (lett. a, b, c). La seconda invece riguarda le fattispecie in cui i sistemi di IA siano impiegati nello svolgimento di attività preistruttorie, dalle quali potrebbero emergere fatti che rendono necessario l'esercizio di un potere (lett. d)[81].

Nel caso in cui le pubbliche amministrazioni impieghino sistemi di IA classificati come ad alto rischio, trova piena applicazione l'apparato normativo previsto dal Regolamento, come prima richiamato.

Se le amministrazioni rivestono la qualità di fornitore[82] devono informare in modo chiaro e comprensibile gli utenti quando l'IA è utilizzata, affinché questi ultimi possano sapere se stanno interagendo con un algoritmo o con un essere umano. Inoltre, sono tenute a fornire dettagli sul funzionamento del sistema, sul suo ruolo nelle decisioni e sul fatto che si tratti di una decisione automatizzata (art. 13). Le amministrazioni sono poi tenute a monitorare l'uso dei sistemi di IA, al fine di prevenire anomalie o danni, intervenendo in caso di malfunzionamenti imprevisti (art. 14). Al precipuo scopo di mantenere la fiducia dei cittadini, i sistemi di IA utilizzati dalle amministrazioni dovrebbero essere addestrati con dati di elevata qualità[83], garantendo un'adeguata progettazione (art. 10). Inoltre, in virtù dei principi di accuratezza o robustezza, prima di essere messi in servizio, i sistemi di IA dovrebbero essere sottoposti a prova[84]. Infine, le amministrazioni sono tenute 'a effettuare una valutazione dei rischi

80 Cfr. sul punto Carullo, G. (2021), *Decisione amministrativa e intelligenza artificiale*, in *Il diritto dell'informazione e dell'informatica*, n. 3, pp. 431 ss., che si chiede quale sia la tutela dei privati in rapporto ai casi in cui le risultanze dell'analisi delegata all'algoritmo non emergano direttamente dall'atto conclusivo del procedimento, ma costituiscano un mero atto endoprocedimentale, pp. 456-457 «*Anche in questo caso sembrerebbe potersi risolvere la questione applicando i principi già noti nel nostro diritto nazionale sulla trasmissione dell'antigiuridicità tra atti. Secondo quanto spiegato in dottrina, si tratterà in particolare di valutare se l'atto endoprocedimentale adottato con un sistema di IA, ed asseritamente lesivo, sia un mero atto preparatorio – e perciò non autonomamente impugnabile –, ovvero presupposto, e perciò direttamente ed immediatamente impugnabile*».

81 Clarich, M. (2022), Manuale di diritto amministrativo, *Il Mulino*, Bologna, p. 238.

82 Art. 3, par. 1, n. 3) Regolamento (UE) 2024/1689 «*fornitore: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito*».

83 Sull'importanza della qualità dei dati di cui si serve la pubblica amministrazione, cfr. Carloni, E. (2021), Qualità dei dati, big data e amministrazione pubblica, in Cavallo Perin, R., a cura di, L'amministrazione pubblica con i Big data: da Torino un dibattito sull'intelligenza artificiale, *Quaderni del dipartimento di giurisprudenza dell'Università di Torino*, n. 20, p.121, «*La qualità dei dati si pone dunque in termini nuovi rispetto ai tradizionali principi di adeguatezza conoscitiva procedimentale e come sfida centrale nel momento in cui le amministrazioni sviluppano i propri processi conoscitivi e decisionali tramite l'acquisizione diretta, ed automatica, di informazioni raccolte altrove o precedentemente: questo determina la perdita di consapevolezza e controllo sulle informazioni utilizzate, e produce la generalizzazione di un'esigenza di qualità "standard" che prima si concentrava solo su alcune specifiche informazioni contenute in determinati archivi pubblici*».

84 Considerando n. 59, Regolamento (UE) 2024/1689.

per i diritti fondamentali, come la possibilità di discriminazioni o violazione della privacy (art. 9).

Quando le amministrazioni ricoprono il ruolo di *deployer*, ossia utilizzano i sistemi di IA, sono soggette a obblighi di conformità relativi alla loro gestione operativa. I *deployer* svolgono un ruolo fondamentale nel garantire la tutela dei diritti fondamentali, integrando gli obblighi del fornitore nello sviluppo del sistema di IA[85]. Pertanto, anche se non obbligatorio come nel caso dei sistemi ad alto rischio, le amministrazioni che utilizzano l'IA sono tenute a supervisionare efficacemente i sistemi durante il periodo in cui sono in uso. Il controllo umano dovrebbe essere previsto in qualsiasi fase critica del processo decisionale (art. 14). Le pubbliche amministrazioni dovrebbero altresì garantire che l'uso dei sistemi di IA non violi i diritti fondamentali, fra i quali anche il diritto alla protezione dei dati personali. Per consentire la valutazione dell'impatto dei sistemi di IA sui diritti fondamentali, in un'ottica di chiarezza e trasparenza, richiamando anche l'art. 6, par. 1, lettera e) e par. 3, 9 del GDPR e gli artt. 2-*ter* e 2-*sexies* del decreto legislativo 30 giugno 2003 n. 196, le pubbliche amministrazioni dovrebbero adottare idonei «*atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*»[86].

Si ribadisce che, anche nelle ipotesi in cui i sistemi di IA non siano ad alto rischio, le pubbliche amministrazioni restano soggette al rispetto delle disposizioni dell'AI Act, che prevede un regime di obblighi modulato secondo il livello di rischio del sistema, ma anche in relazione al ruolo svolto dal soggetto (fornitore, distributore, utilizzatore) e ispirato al principio di gradualità.

Per comprendere la portata di tutte le norme citate, occorre un'attenta navigazione nel panorama legislativo corrente e una previsione strategica delle evoluzioni future in questo ambito. Il processo di digitalizzazione delle pubbliche amministrazioni era già stato innescato dal legislatore nazionale. Ai sensi degli artt. 2, 12, 13, 13-*bis*, 14, 15 e 41 del decreto legislativo 7 marzo 2005, n. 82 (CAD) e dell'art. 3-*bis* della legge 9 agosto 1990, n. 241, le pubbliche amministrazioni, nell'organizzare autonomamente la propria attività e nel gestire i procedimenti amministrativi, utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di eguaglianza e di non discriminazione. Il suddetto processo, dal quale deriva l'espressione 'amministrazione digitale', implica una trasformazione sia dell'organizzazione sia dell'attività dell'amministrazione stessa, che richiede in generale un ripensamento degli schemi operativi e dei processi decisionali tradizionali[87]. Anche l'art. 30 del decreto legislativo

85 Considerando n. 93, Regolamento (UE) 2024/1689.

86 Così testualmente art. 2*sexies* d.lgs. 196/2003.

87 Cfr. Giannini, M.S. (1979), Rapporto sui principali problemi dell'amministrazione dello Stato, nel quale si legge «*i sistemi informativi non servono più alle amministrazioni per fatti di gestione interna, ma servono proprio per amministrare, si proiettano cioè sempre più verso l'esterno*»; cfr. in dottrina Galetta, D.U., Corvalan, J.G. (2019), Intelligenza artificiale per una pubblica amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto, *op. cit.*, p. 12 «*potremmo dunque essere in presenza di una pietra miliare nello sviluppo del settore pubblico: perché, per la prima volta*

31 marzo 2023, n. 36 (codice dei contratti pubblici) affida alle stazioni appaltanti l'onere, «*ove possibile*», di automatizzare le proprie attività ricorrendo a soluzioni tecnologiche, ivi inclusa l'IA. Recentemente, l'art. 9 del decreto legislativo 12 luglio 2024, n. 103, in materia di semplificazione dei controlli sulle attività economiche, impegna le pubbliche amministrazioni ad adottare misure volte ad automatizzare progressivamente le proprie attività ricorrendo a soluzioni tecnologiche, ivi incluse quelle di IA.

In generale, si rileva un consistente *favor* del legislatore nei confronti dell'impiego di sistemi di IA da parte delle amministrazioni sia nell'organizzazione che nello svolgimento delle attività. Come illustrato nel Piano triennale per l'informatica nella PA 2024-2026, l'IA può apportare innumerevoli benefici nel settore pubblico, quali l'automazione di attività di ricerca e analisi, l'aumento delle capacità predittive, con un conseguente miglioramento del processo decisionale basato sui dati, ma anche la personalizzazione dei servizi. L'IA rappresenterebbe «*la risposta alla crescente necessità di migliorare l'efficienza e l'efficacia nella gestione e nell'erogazione dei servizi pubblici*»[88].

Accanto ai benefici, non bisogna comunque tralasciare i rischi dei quali si è occupata anche la giurisprudenza.

4 Le condizioni della decisione automatizzata secondo la giurisprudenza

Le prime pronunce della giurisprudenza amministrativa riguardano una procedura di assunzioni gestita da un sistema informatico per mezzo di un algoritmo,

potrebbe essere avviato un percorso di gestione dei dati e dei documenti in possesso delle pubbliche amministrazioni finalizzato ad automatizzare il processo decisionale applicando l'Intelligenza artificiale a vaste aree di attività di routine, ripetitive e standardizzate». Cfr. anche Cavallo Perin, R. (2020), Ragionando come se la digitalizzazione fosse data, *op. cit.*, p. 305 «*Le prime applicazioni d'informatica pubblica hanno sviluppato due differenti approcci tutt'ora presenti nel dibattito: l'uno che relega la tecnica a strumenti d'ausilio (così in sequenza storica: computer, internet, smartphone); l'altro invece che ritiene che l'innovazione investa la pubblica amministrazione e il procedimento decisionale pubblico, ridisegnandone la forma e la sostanza*»; Rossa, S. (2021), Contributo allo studio delle funzioni amministrative digitali, *CEDAM*, p. 60 «*intendendo per la digitalizzazione della pubblica amministrazione il processo, che si instaura in quell'ambito in cui l'informatica giuridica e il diritto amministrativo si sovrappongono, con il quale le amministrazioni pubbliche agiscono e si organizzano per agire, con l'intento di esercitare funzioni amministrative e prestare servizi pubblici attraverso le tecnologie dell'informazione e della comunicazione, al fine di perseguire due macro obiettivi: da un lato attuare i principi costituzionali sanciti dall'art. 97 Cost., di buon andamento e di imparzialità, nonché dei loro corollari espressamente affermati sul piano costituzionale dalla l. n. 241/1990, vale a dire efficacia, efficienza ed economicità; dall'altro concretizzare la strategia dell'Open Government dando attuazione ai suoi principi di trasparenza, di partecipazione e di collaborazione*». Si veda ancora, Marchetti, B. (2021), The algorithmic administrative decision and the human in the loop, in *BioLaw Journal*, n. 2, pp. 381 ss. Nella dottrina straniera, cfr. Arenilla Sáez, M. (2021), La administración digital : los riesgos de la desintermediación, las escisiones y las centralizaciones, *Instituto Nacional de Administración Pública*, Madrid, pp. 167-168; Neves, A.F. (2023), A necessidade de reescrever o direito administrativo, in *Estudos em homenagem ao Professor Doutor Fernando Alves Correia*, vol. I, Almedina, Coimbra, pp. 555-592, che rileva come l'impiego delle *ICTs* altera il modo in cui le amministrazioni si organizzano, esercitano la propria attività e si relazionano con i propri interlocutori. La digitalizzazione richiede quindi di ripensare al quadro organizzativo della pubblica amministrazione, i cui principi cardine devono rintracciarsi nella collaborazione, cooperazione, coordinamento e interoperabilità.

88 AgID (2023), Piano Triennale per l'informatica nella pubblica amministrazione 2024- 2026, (https://www.agid.gov.it/sites/agid/files/2024-06/piano_triennale_per_linformatica_nella_pa_2024-2026.pdf).

che avrebbe disposto i trasferimenti del personale docente, senza tenere in considerazione le preferenze indicate nelle rispettive domande di trasferimento. Superato un preliminare atteggiamento di chiusura del T.A.R. Lazio, secondo cui nessuna complicatezza o ampiezza di un procedimento amministrativo può legittimare la sua devoluzione a un meccanismo informatico o matematico[89], il Consiglio di Stato ha sottolineato gli indubbi vantaggi che derivano dalla automazione del processo decisionale dell'amministrazione[90]. A ogni modo, l'utilizzo non può costituire motivo di elusione dei principi che regolano l'attività amministrativa[91]. Infatti, «*la regola tecnica che governa ciascun algoritmo resta pur sempre una regola amministrativa generale, costruita dall'uomo e non dalla macchina, per essere poi (solo) applicata da quest'ultima, anche se ciò avviene in via esclusiva*»[92]. Da ciò deriva che «*l'algoritmo, ossia il software, deve essere considerato a tutti gli effetti come un 'atto amministrativo informatico'*»[93]. Pertanto, il meccanismo attraverso il quale si concretizza la decisione automatizzata deve rispondere al principio della conoscibilità, quale declinazione rafforzata del principio di trasparenza. La regola algoritmica deve essere anche soggetta alla piena cognizione e al pieno sindacato del giudice amministrativo, al fine di poter valutare come il potere sia stato concretamente esercitato.

L'ammissibilità del procedimento di formazione della volontà amministrativa affidato a un *software*, «*nel quale vengono immessi una serie di dati così da giungere, attraverso l'automazione della procedura, alla decisione finale*»[94], non ha fatto venir meno l'esigenza di leggere in maniera critica le potenzialità della rivoluzione digitale del settore pubblico. Se è vero che le nuove tecnologie possono correggere i pregiudizi dei processi cognitivi umani, appare altrettanto vero che l'impiego delle stesse comporta una serie di scelte tutt'altro che neutre[95].

89 Cfr. *ex multis* T.A.R. Lazio Roma, sez. III *bis,* sent. 10 settembre 2018, n. 9224; sent. 10 settembre 2018, n. 9227; sent. 10 settembre 2018, n. 9230; sent. 27 maggio 2019, n. 6606; sent. 13 settembre 2019 n. 10964, nella quale si afferma che alla «*deleteria prospettiva orwelliana di dismissioni delle redini della funzione istruttoria e di abdicazione a quella provvedimentale*», osterebbero i valori costituzionali di cui agli artt. 3, 24 e 97.

90 Sentenza Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270.

91 Sentenza Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270.

92 *Ibidem.*

93 Sentenza Consiglio di Stato, sez. VI, 13 dicembre 2019, 8472.

94 Sentenza Consiglio di Stato, sez. VI, 13 dicembre 2019, nn. 8473 e 8474.

95 Il riferimento implicito nelle pronunce nn. 8472, 8473 e 8474 del 2019, ma esplicito nella sentenza n. 881/2020, è al caso *State v. Loomis (881* N. *W.2d 749 (Wis. 2016).* Il caso origina dalla condanna inflitta al sig. Eric L. Loomis con sentenza del Tribunale circondariale di La Crosse. La pena era stata determinata sulla scorta dei risultati elaborati dal programma COMPAS (*Correctional offender management profiling for alternative sanctions*) di proprietà della società Northpointe (ora Equivant), secondo cui Loomis era da identificarsi quale soggetto ad alto rischio di recidiva. La Corte suprema del Wisconsin, pur negando nel caso di specie la violazione del diritto al *due process*, ha affermato che i giudici possono ricorrere allo strumento di *risk assessment* nel processo valutativo di una condanna ai seguenti limiti: i) i tribunali non dovrebbero utilizzare il risultato prodotto dall'algoritmo come unico fattore determinante la decisione di condanna o meno; ii) i giudici sono poi obbligati a fornire una motivazione per la decisione assunta che vada oltre la mera indicazione del risultato prodotto dal software; da ultimo, iii) le corti non possono determinare la severità della pena sulla base del *risk assessment* (https://www.biodiritto.org/AI-Legal-Atlas/AI-Giurisprudenza/Wisconsin-USA-Supreme-Court-of-Wisconsin-State-v.-Loomis-sull-impiego-nell-ambito-di-un-giudizio-penale-del-software-di-calcolo-del-rischio-di-recidiva-COMPAS). In argomento sulla presenza di *bias* cognitivi nel *tool* COMPAS, cfr. Larson, J. *et al.* (2016), How We Analyzed the COMPAS Recidivism Algorithm, (https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm), «*Our analysis of Northpointe's tool, called COMPAS (which stands for Correctional Offender Management Profiling for Alternative Sanctions), found that black defendants were far more*

Il Consiglio di Stato[96] ha così formulato i principi di piena conoscibilità, di non esclusività della decisione algoritmica e di non discriminazione, a cui deve conformarsi la decisione automatizzata per poter essere considerata legittima[97].

Il principio di conoscibilità viene definito come il diritto di ciascuno di conoscere l'esistenza di processi decisionali automatizzati che lo riguardino e, nel caso, di ricevere informazioni significative sulla logica utilizzata. Esso corrobora l'idea dell'amministrazione come '*casa di vetro*'[98] e costituisce una declinazione rafforzata del principio di trasparenza che si inquadra nel diritto a una buona amministrazione, sancito dall'art. 41 della Carta europea dei diritti fondamentali[99]. Si tratta di un principio in parte già affermato nel considerando n. 63 del GDPR, in base al quale ogni interessato dovrebbe avere il «*diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento*».

Il lodevole sforzo di dare rilievo al principio di conoscibilità collide però con la tendenziale opacità che contraddistingue alcuni dei sistemi di intelligenza artificiale, i cui risultati richiederebbero esperienza e processi specializzati per essere compresi e controllati[100]. Proprio a tal fine, non solo gli artt. 13 e 50 dell'AI Act impongono

likely than white defendants to be incorrectly judged to be at a higher risk of recidivism, while white defendants were more likely than black defendants to be incorrectly flagged as low risk».

96 Sentenza Consiglio di Stato, sez. VI, 4 febbraio 2020, n. 881.

97 Si tratta di principi che attualmente ricevono pieno riconoscimento nell'ordinamento positivo. L'art. 30 del codice dei contratti pubblici prevede che le stazioni appaltanti, nell'automatizzare la propria attività, anche attraverso sistemi di IA, devono: a) assicurare la disponibilità del codice sorgente, della relativa documentazione, nonché di ogni altro elemento utile a comprenderne le logiche di funzionamento; b) introdurre negli atti di indizione delle gare clausole volte ad assicurare le prestazioni di assistenza e manutenzione necessarie alla correzione degli errori e degli effetti indesiderati derivanti dall'automazione. Inoltre proprio nel comma 3 sono richiamati i principi di conoscibilità, per cui ogni operatore economico ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino e, in tal caso, a ricevere informazioni significative sulla logica utilizzata; di non esclusività della decisione algoritmica, per cui nel processo decisionale vi deve essere un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata; di non discriminazione algoritmica, per cui il titolare deve mettere in atto misure tecniche e organizzative adeguate al fine di impedire effetti discriminatori nei confronti degli operatori economici.

98 Così Turati, F. (1908), Atti del Parlamento italiano, Camera Dei Deputati, sess. 1904-1908, Legislatura XXII, 1° sessione, 2° tornata del 17 giugno 1908, Pres. Marcora, «*dove un superiore, pubblico interesse non imponga un momentaneo segreto, la casa dell'amministrazione dovrebbe essere di vetro*». Cfr. sentenza Cons. Stato, Ad. Plen., 2 aprile 2020, n. 10, punto 22.6 nella quale è stata ribadita l'importanza del principio di trasparenza, in quanto fondamento della democrazia amministrativa in uno Stato di diritto; v. anche Corte costituzionale, sentenza 21 febbraio 2019, n. 20.

99 L'art. 41 della Carta europea dei diritti fondamentali testualmente prevede che «*Ogni persona ha diritto a che le questioni che la riguardano siano trattate in modo imparziale ed equo ed entro un termine ragionevole dalle istituzioni, organi e organismi dell'Unione. 2. Tale diritto comprende in particolare: a) il diritto di ogni persona di essere ascoltata prima che nei suoi confronti venga adottato un provvedimento individuale che le rechi pregiudizio; b) il diritto di ogni persona di accedere al fascicolo che la riguarda, nel rispetto dei legittimi interessi della riservatezza e del segreto professionale e commerciale; c) l'obbligo per l'amministrazione di motivare le proprie decisioni. 3. Ogni persona ha diritto al risarcimento da parte dell'Unione dei danni cagionati dalle sue istituzioni o dai suoi agenti nell'esercizio delle loro funzioni, conformemente ai principi generali comuni agli ordinamenti degli Stati membri. 4. Ogni persona può rivolgersi alle istituzioni dell'Unione in una delle lingue dei trattati e deve ricevere una risposta nella stessa lingua*».

100 Consiglio dell'Unione europea (2020), La Carta dei diritti fondamentali nel contesto dell'intelligenza artificiale e della trasformazione digitale; cfr. in dottrina, Carloni, E. (2022), Le intelligenze artificiali nella pubblica amministrazione e la sfida della trasparenza gli algoritmi, in Lalli, A., a cura di, L'amministrazione pubblica nell'era digitale, *G. Giappichelli*, Torino, pp. 45 ss.; Foà, S. (2023), Intelligenza artificiale e cultura della trasparenza amministrativa. Dalle 'scatole nere'

specifici obblighi di trasparenza in capo ai *deployer*, ma l'art. 86 prevede anche il diritto alla spiegazione dei singoli processi decisionali, ossia il diritto di qualsiasi persona di «*ottenere dal* deployer *spiegazioni chiare e significative sul ruolo dei sistemi di IA nella procedura decisionale e sui principali elementi della decisione adottata*»[101].

Il principio di non esclusività della decisione algoritmica fa riferimento alla necessità che nel processo decisionale sia garantito un contributo da parte dell'uomo di controllare, validare o anche smentire la decisione automatica. La sorveglianza può essere declinata in vari modi. Questa può avvenire con meccanismi di *governance* che consentano un approccio con intervento umano in ogni ciclo decisionale del sistema (*human-in-the-loop* – HITL); con supervisione umana (*human-on-the-loop* – HOTL) che prevede l'intervento umano durante il ciclo di progettazione del sistema e il monitoraggio del funzionamento del sistema; ovvero con controllo umano (*human-in-command* – HIC) che prevede il controllo dell'attività del sistema di IA nel suo complesso e la capacità di decidere quando e come utilizzare il sistema in qualsiasi particolare situazione.

Ai sensi dell'art. 14 dell'AI Act, le misure di sorveglianza umana sono commisurate ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA ad alto rischio. La sorveglianza umana richiede comunque il possesso di specifiche competenze in capo alle persone all'uopo preposte, in particolare un livello appropriato di alfabetizzazione, formazione e autorità in materia di IA per svolgere adeguatamente tali compiti, come previsto dall'art. 4[102]. Tali disposizioni pongono delicati problemi nel settore pubblico.

In primo luogo, sembra delinearsi una diligenza qualificata del personale, con conseguenti profili di *culpa in eligendo* in capo alla persona deputata alla sorveglianza qualora difetti la professionalità richiesta e di *culpa in vigilando* nei casi in cui il sorvegliante non individui e affronti tempestivamente i segnali di anomalie[103]. Ai sensi del paragrafo 4 dell'art. 14, la persona fisica cui è affidata la sorveglianza, oltre a dover comprendere correttamente le capacità e i limiti pertinenti del sistema di IA, deve essere in grado di monitorarne il funzionamento anche per individuare e affrontare anomalie, disfunzioni e prestazioni inattese, intervenendo sul funzionamento del sistema o interrompendolo mediante il pulsante di arresto.

In secondo luogo, la disposizione citata richiede che la persona fisica a cui è affidata la sorveglianza sia consapevole della possibile tendenza di fare

alla "casa di vetro"?, in *Diritto amministrativo,* n. 3, pp. 515 ss.; Lo Sapio, G. (2021), La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione, in *Federalismi.it*, n. 16, pp. 114 ss.

101 L'art. 86, par. 1 del Reg. (UE) 2024/1689 prevede testualmente che «*Qualsiasi persona interessata oggetto di una decisione adottata dal* deployer *sulla base dell'output di un sistema di IA ad alto rischio elencato nell'Allegato III, ad eccezione dei sistemi elencati al punto 2 dello stesso, e che produca effetti giuridici o in modo analogo incida significativamente su tale persona in un modo che essa ritenga avere un impatto negativo sulla sua salute, sulla sua sicurezza o sui suoi diritti fondamentali ha il diritto di ottenere dal* deployer *spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata*».

102 Cfr. anche Considerando n. 91 Reg. (UE) 2024/1689; in ordine alla definizione di alfabetizzazione in materia di IA, art. 3, par. 1, n. 56 Reg. (UE) 2024/1689.

103 Così Foà, S. (2023), Intelligenza artificiale e cultura della trasparenza amministrativa. Dalle "scatole nere" alla "casa di vetro"?, *op. cit.*, p. 527.

automaticamente affidamento, ovvero eccessivo affidamento, sull'output prodotto dal sistema (cosiddetta distorsione dall'automazione). Resta dunque salvo il potere/dovere di decidere di non usare il sistema di IA oppure di ignorare, annullare o ribaltare l'output del sistema, salvo la sua corretta interpretazione. Nel settore pubblico, però, la scelta di non usare o di ignorare, annullare o ribaltare l'output del sistema comporta da un lato, un onere motivazionale rafforzato, dovendo il funzionario spiegare la suddetta decisione; dall'altro lato, indubbi profili di responsabilità per il mancato adeguamento all'output[104]. Si aggiunga che un funzionario pubblico, anche solo per mere ragioni di convenienza pratica, difficilmente non seguirà l'output del sistema. È stato osservato che così facendo si realizzerebbe un indebolimento della capacità di giudizio del decisore pubblico, con contestuale sua deresponsabilizzazione e demansionamento di fatto[105]. Infine, anche dal punto di vista degli assetti organizzativi, la scelta di ignorare o annullare l'output dovrebbe competere allo stesso funzionario deputato alla sorveglianza, con l'urgenza di una previa definizione della *governance* del processo[106].

La possibilità che i dati impiegati dai sistemi di AI contengano, già in fase di *training,* errori di valutazione o pregiudizi (*bias*), producendo e/o amplificando fenomeni di esclusione di interi gruppi sociali o episodi individuali di discriminazione, è alla base del principio di non discriminazione[107]. Il Regolamento (UE) 2024/1689 prevede che i sistemi di IA vengano sviluppati e utilizzati in modo da includere soggetti diversi e promuovere la parità di accesso, l'uguaglianza di genere e la diversità culturale, evitando allo stesso tempo effetti discriminatori e pregiudizi ingiusti vietati dal diritto dell'Unione o nazionale[108].

La pronuncia del Tribunale dell'Aja in merito al sistema di profilazione SyRI (*System Risk Indication*) testimonia come i sistemi di IA, se progettati e utilizzati in modo inadeguato, possono risultare particolarmente intrusivi e perpetuare modelli storici di discriminazione. SyRI veniva utilizzato dal governo olandese allo scopo di valutare l'attitudine a commettere frodi o abusi da parte di coloro che percepivano

104 In materia di responsabilità, si veda la recente Proposta di Direttiva del Parlamento europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale) COM/2022/496 final. L'intento è quello di semplificare l'onere della prova per qualunque soggetto promuova un'azione per danni causati da sistemi di IA in uno Stato membro, al fine di superare le principali criticità riscontrate in materia di responsabilità civile, ossia: i) antieconomicità (in quanto le norme nazionali in materia di responsabilità civile risultano spesso di difficile applicazione alla materia dell'IA, con particolare riferimento all'identificazione del soggetto responsabile); ii) incertezza (le norme nazionali spesso possono essere interpretate diversamente in base all'apprezzamento del giudice nazionale); iii) frammentazione normativa.

105 Del Gatto, S. (2020), Potere algoritmico, digital welfare state e garanzie per gli amministrati. I nodi ancora da sciogliere, in *Rivista italiana di diritto pubblico comunitario*, n. 6, pp. 829 ss.

106 Cfr. Foà, S. (2023), Intelligenza artificiale e cultura della trasparenza amministrativa. Dalle "scatole nere" alla "casa di vetro"?, *op. cit.*, p. 528.

107 Si tratta di un principio già enunciato dal Considerando n. 71 del GDPR, ai sensi del quale il titolare del trattamento dovrebbe porre in essere le misure tecniche e organizzative adeguate al fine di garantire che siano rettificati i fattori che comportino inesattezze dei dati e sia minimizzato il rischio di errori e allo scopo di impedire, tra l'altro, effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero un trattamento che comporti misure aventi tali effetti.

108 Considerando n. 27.

sussidi o altre forme di assistenza pubblica[109]. Il sistema è stato ritenuto discriminante in quanto, mediante un meccanismo mai rivelato, attingeva a dati sensibili da diciassette *database* riguardanti cittadini delle aree più problematiche del Paese, contribuendo così a promuovere stereotipi. Il sistema si poneva, dunque, in contrasto con il principio di eguaglianza sostanziale che avrebbe dovuto essere perseguito anche attraverso la spiegazione delle modalità di funzionamento del sistema[110].

In conclusione, i sistemi di IA possono essere utilizzati nel settore pubblico, purché siano rispettati specifici principi giuridici, oltre alla disciplina generale del diritto amministrativo e di settore. L'uso dell'IA appare legittimo ove siano garantiti la conoscibilità, la sorveglianza umana e la non discriminazione. L'adozione dell'IA nel settore pubblico deve essere implementata con attenzione e deve essere accompagnata da un'idonea formazione dei dipendenti pubblici e da un'adeguata considerazione in ordine ai rischi legati ad esempio alla presenza ovvero al diritto di difesa dei cittadini[111].

109 Tribunale distrettuale dell'Aja, 5 febbraio 2020, C-09-550982-HA ZA 18-388, (http://www.europeanrights.eu/public/sentenze/The_Netherlands-05.02.2020_ECLI_NL_RBDHA_2020_865.pdf).

110 Cfr. punto 6.92 della sentenza; v. Avanzini, G. (2022), Intelligenza artificiale e nuovi modelli di vigilanza pubblica in Francia e Olanda, in *Giornale di diritto amministrativo*, n. 3, pp. 316 ss.

111 Cfr. Considerando n. 59, Reg. (UE) 2024/1689.

CAPITOLO SECONDO

Il SupTech

1 SupTech: una possibile definizione

Si è già osservato come oggi possa darsi per scontato che nel settore pubblico vengano impiegati sistemi di IA. L'assenza di una 'mappatura degli usi'[112] impone, però, di considerare le diverse iniziative sviluppate dalle singole amministrazioni, per capire se siano *compliant* con il quadro normativo sopra descritto.

Data la trasformazione tecnologica dei mercati[113], le autorità di vigilanza hanno sviluppato un approccio di vigilanza innovativo, proattivo e *data-driven*. La tecnologia applicata alla vigilanza prende il nome di SupTech[114]. Secondo l'OECD, con il termine SupTech si indica «*the use of digital tools and solutions including hardware and software by public sector regulators and supervisors to carry out their responsibilities*»[115]. L'impiego da parte delle autorità di vigilanza di sistemi di IA e di strumenti avanzati di raccolta e analisi di dati risponde all'esigenza di rendere maggiormente efficiente ed efficace l'attività amministrativa di vigilanza.

A livello globale, già nel 2017, il Basel Committee on Banking Supervision (BCBS) invitava le autorità di vigilanza a sperimentare le potenzialità delle nuove tecnologie, fra le quali i sistemi di intelligenza artificiale che avrebbero permesso di vagliare grandi e complesse quantità di dati, non altrimenti analizzabili dagli esseri umani in maniera altrettanto rapida ed efficiente[116]. La necessità di utilizzare strumenti digitali per rafforzare le capacità di supervisione delle autorità di vigilanza emerge, in realtà, con la crisi finanziaria del 2008[117]. Tale evento ha incrementato notevolmente la complessità e i volumi delle informazioni da processare nell'attività di vigilanza e di regolamentazione dei mercati.

Nello studio del 2019 del Financial Stability Institute, come riportato dall'OECD, le iniziative SupTech sono classificate secondo quattro generazioni che si susseguono con l'evolversi delle tecnologie[118]. La prima generazione, 'descrittiva', prevede un uso limitato dei dati che vengono preparati e validati per compiere analisi prevalentemente manuali. La seconda, 'diagnostica', prevede maggior livelli di automazione per facilitare l'analisi e la rappresentazione dei dati utili alle attività di

112 Rangone, N. (2022), Le pubbliche amministrazioni alla prova dell'intelligenza artificiale, *op. cit.*, p. 496; cfr. anche Marchetti, B. (2021), *The algorithmic administrative decision and the human in the loop*, *op. cit.*

113 Si v. nota 1, Introduzione.

114 Il termine SupTech viene utilizzato per la prima volta da Ravi Menon all'Australian Securities and Investments Commission (ASIC) Annual Forum 2017, Singapore, 20 marzo 2017 (https://www.bis.org/review/r170328a.htm). Il termine è stato successivamente definito da Broeders, D., Prenio, J. (2018), Innovative technology in financial supervision (suptech) – the experience of early users, *FSI Insights on policy implementation*, n. 9, (https://www.bis.org/fsi/publ/insights9.pdf) «*the use of innovative technology by supervisory agencies to support supervision*».

115 OECD (2021), Business and Finance Outlook 2021: AI in Business and Finance, *OECD Publishing*, Paris, (https://doi.org/10.1787/ba682899-en), p. 122. In italiano (traduzione nostra): «*l'uso di strumenti e soluzioni digitali, compresi hardware e software, da parte delle autorità di regolamentazione e supervisione del settore pubblico per svolgere le proprie responsabilità*».

116 Basel Committee on Banking Supervision (2017), Consultative Document, Sound Practices: Implications of fintech developments for banks and bank supervisors, (https://www.bis.org/bcbs/publ/d415.htm).

117 FSB (2020), The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions, (https://www.fsb.org/wp-content/uploads/P091020.pdf).

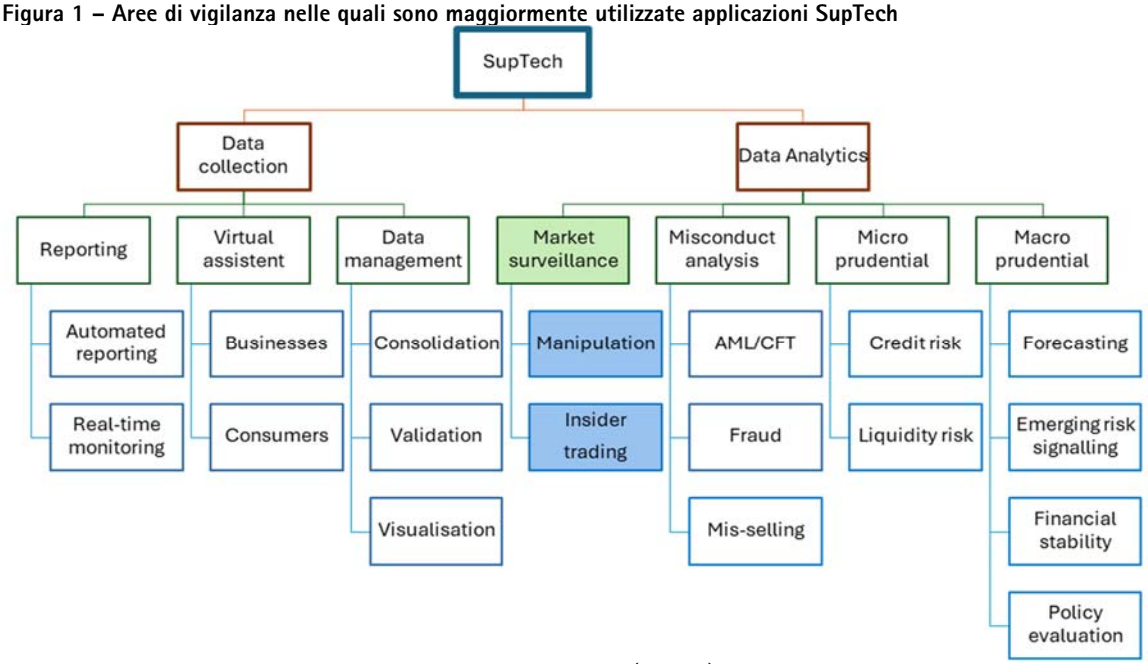
118 OECD (2021), Business and Finance Outlook 2021, *op. cit.*

regolamentazione. La terza, 'predittiva', implica il coinvolgimento massivo di sistemi e architetture in grado di gestire *big data* per restituire esiti predittivi. La quarta generazione, 'prescrittiva', impiega sistemi di intelligenza artificiale capaci di fornire anche piani di azione.

Al di là dell'evoluzione in senso cronologico, questa classificazione può risultare utile per ragionare sullo stato di avanzamento delle iniziative di vigilanza intraprese dalle autorità. Si potrebbe arrivare a sostenere che l'impiego di IA non faccia ricadere necessariamente l'attività dell'autorità nella terza o quarta generazione, dovendone valutare le concrete modalità di utilizzo.

Alla luce della definizione di SupTech e delle 'generazioni' concepite in relazione al progresso tecnologico, si richiama lo schema (di seguito riformulato) dello studio del Financial Stability Institute per approfondire le possibili attività ricomprese in tale concetto.

Figura 1 – Aree di vigilanza nelle quali sono maggiormente utilizzate applicazioni SupTech



Fonte: Broeders, D., Prenio, J., Innovative technology in financial supervision (SupTech) – the experience of early users, *FSI Insights on policy implementation*, n. 9, luglio 2018.

La Figura 1 suddivide le applicazioni SupTech nelle aree di *data collection* e di *data analytics*, all'interno della quale è ricompresa l'attività di vigilanza dei mercati. Soluzioni SupTech permetterebbero applicazioni più performanti di *detection* e *surveillance* dell'*insider trading* e della manipolazione di mercato. Proprio nella repressione di tali fenomeni, la CONSOB ha sviluppato dei *proof of concept*. Prima di analizzarli, è utile passare in rassegna alcune iniziative SupTech sviluppate in ambito nazionale e internazionale.

2 Le sperimentazioni SupTech a livello nazionale

A livello nazionale si osservano diversi esperimenti. La Banca d'Italia, ad esempio, sta lavorando sullo sviluppo di un sistema di IA di tipo *machine learning* per individuare le società di capitali potenzialmente connesse a contesti di criminalità organizzata. Come riportato nella Figura 1 (Capitolo II, paragrafo 1), i sistemi di IA possono rendere più efficace ed efficiente l'azione di contrasto al crimine finanziario, contribuendo a una più accurata e tempestiva identificazione dei rischi di riciclaggio e di finanziamento del terrorismo (ML/TF) e a una gestione automatizzata dei flussi di lavoro sottostanti[119]. Il modello sviluppa un algoritmo di *machine learning* per individuare aziende potenzialmente collegate alla criminalità organizzata; esso consente di calcolare un indicatore di rischio (*score*) compreso fra 0 e 1 che indica la probabilità che la singola impresa sia connessa o meno a contesti di criminalità organizzata. Utilizzando un dataset di oltre 28.000 imprese italiane, l'algoritmo identifica con successo circa il 76% delle aziende collegate alla criminalità organizzata e il 74% delle aziende presumibilmente 'sane'. Il punteggio di rischio che scaturisce dall'algoritmo potrebbe essere utilizzato a livello operativo per supportare l'azione delle autorità antiriciclaggio e delle forze dell'ordine (come strumento di *screening* preliminare).

Il modello, addestrato utilizzando un *dataset* relativo al periodo 2010–2021, ha prodotto i seguenti risultati in fase di test: «[il] *78,3% delle società di capitale ha uno score inferiore a 0,50; tra il restante 21,7% delle aziende con un punteggio superiore a tale soglia, l'1,8% ha uno score superiore a 0,95*»[120]. L'indicatore di rischio, ancora in fase sperimentale, presenta diverse potenziali applicazioni. Come riportato nello studio, esso può contribuire al patrimonio informativo che supporta le funzioni istituzionali dell'UIF; ovvero potrebbe fungere da strumento preliminare di *screening* per contribuire a orientare l'azione degli organi investigativi.

Dal 2021 la Banca d'Italia ha, inoltre, iniziato a impiegare sistemi di IA, basati sulla ricerca testuale e sulla clusterizzazione, per migliorare l'analisi del patrimonio informativo desumibile dagli esposti privatistici[121]. Fra i benefici dell'impiego di sistemi di IA, la Banca d'Italia menziona la riduzione delle tempistiche di verifica, l'accrescimento delle possibilità di identificare in anticipo fenomeni rilevanti. Proprio in ordine alla gestione degli esposti, anche attraverso sistemi di IA, la Banca d'Italia ha adottato un regolamento, nel cui Allegato sono enumerate le operazioni svolte nella trattazione degli esposti e specificato l'uso delle informazioni estratte da questi tramite

119 Cariello, P. *et al.* (2024), A machine learning approach for the detection of firms linked to organised crime in Italy, based on balance sheet data, *Banca d'Italia Quaderni dell'antiriciclaggio*, n. 22.

120 *Ivi*, p. 26.

121 Banca d'Italia (2022), Relazione sugli esposti dei clienti delle banche e delle finanziarie dell'anno 2021 (https://www.bancaditalia.it/pubblicazioni/relazione-esposti/2022/relazione-sugli-esposti-sul-2021.pdf). L'esperienza di *EspTech* sugli esposti privatistici, durante il 10° Workshop Innovazione IT e banche: l'Intelligenza Artificiale nel settore bancario - Stato dell'arte e prospettive, 29 gennaio 2021 (https://www.cipa.it/attivita/workshop/2021/index.html), nonché dalla ricostruzione analitica di Franca, S. (2022), Il trattamento di dati nelle sperimentazioni dell'IA riguardanti le pubbliche amministrazioni, in Donati, F. *et al.*, a cura di, Intelligenza artificiale e diritto: una rivoluzione?, vol. II, *Il Mulino*, Bologna, pp. 155-186, in particolare, pp.160-161.

strumenti di IA[122]. Nell'attività di analisi degli esposti, che in ingenti quantità vengono trasmessi alle filiali della Banca d'Italia, viene utilizzato un motore di ricerca *full text* in grado di ricercare tutte le informazioni riconducibili a un determinato servizio o prodotto finanziario. In questo modo, non solo, è possibile individuare le fattispecie che presentano elementi di similarità, ma anche trarre informazioni utili per la trattazione dell'esposto e per l'attività di vigilanza. Allo stesso scopo di supportare le attività di analisi degli esposti e di identificare precocemente potenziali casi di abuso, la Banca d'Italia utilizza tecniche di analisi e algoritmi di *machine learning* (ML) in grado di estrarre e rappresentare gli elementi e i documenti che, sulla base della normativa di settore, risultino maggiormente rilevanti. La logica alla base delle tecniche utilizzate consiste «*nell'aggregare gli esposti in* cluster*, per similitudine semantica, apprendendo elementi informativi e rappresentazioni gerarchiche dall'aggregazione dei dati*»[123]. In conclusione, l'uso dei sistemi di IA in tale ambito è «*esclusivamente preordinato ad effettuare un'analisi dell'andamento spazio-temporale relativo al diffondersi di fattispecie ricorrenti o potenzialmente anomale negli esposti*»[124].

L'IVASS, in collaborazione con la BCE e la Banca d'Italia, ha sviluppato tecniche di IA sugli archivi dei sinistri allo scopo di prevenire frodi, facilitare la consultazione dei documenti assicurativi, arricchire gli indicatori sulla stabilità delle imprese assicurative e classificare i reclami consentendone una più agevole trattabilità[125].

L'AGCOM, nell'ambito del progetto di ricerca europeo dal titolo '*Innovative Monitoring Systems and Prevention Policies of Online Hate Speech*' (IMSyPP)[126], sta sviluppando un sistema di prevenzione e *detection* algoritmica dell'*hate speech* sui servizi media e piattaforme *online* mediante l'impiego di strumenti e metodi afferenti agli ambiti dell'intelligenza artificiale, *machine learning* e *data science*[127]. Inoltre, l'AGCOM si è dotata di una piattaforma che consente di estrarre la ricorrenza di qualsiasi parola chiave e di esaminare il testo di interi documenti riconducibili a notizie su qualsivoglia argomento e accadimento, al fine di individuare *fake news*. La piattaforma si avvale di due algoritmi rilevanti[128]. Il primo è un algoritmo di *stemming*, che consente di estendere la ricerca alle diverse varianti di un termine prescelto. Il secondo è un algoritmo di intelligenza artificiale ad apprendimento automatico di tipo

122 Banca d'Italia (2022), Regolamento concernente il trattamento dei dati personali effettuato dalla Banca d'Italia nell'ambito della gestione degli esposti riguardanti la trasparenza delle condizioni contrattuali, la correttezza dei rapporti tra intermediari e clienti e i diritti e gli obblighi delle parti nella prestazione dei servizi di pagamento, GU Serie Generale n. 75 del 30 marzo 2022. In dottrina, sul regolamento si veda Armiento, M.B. (2023), Prove di regolazione dell'intelligenza artificiale: il Regolamento della Banca d'Italia sulla gestione degli esposti, in *Giornale di diritto amministrativo*, n. 1, pp. 105- 115.

123 Allegato del Regolamento, p. 5.

124 *Ibidem.*

125 IVASS (2024), Relazione sull'attività svolta dall'Istituto nell'anno 2023.

126 Progetto iscritto inscritto nel Programma della Commissione europea e allineato al Testo Unico dei servizi di media audiovisivi (d.lgs. 208/2021).

127 Chiti, E. (2021), Rapporto 1/2021, L'impiego dell'intelligenza artificiale nell'attività di CONSOB, AGCOM e ARERA, *op. cit.*, pp. 222-223.

128 AGCOM (2018), Interim Report indagine conoscitiva del. 309/16/CONS, News vs. Fake nel sistema dell'informazione, (https://www.agcom.it/sites/default/files/migration/attachment/Allegato%2022-11-2018_0.pdf).

supervisionato attraverso il quale avviene la classificazione automatica di ogni notizia rispetto a una categoria di argomenti predefiniti (quali cronaca, politica, esteri, economia, esteri, scienza e tecnologia, cultura, spettacolo e sport). Alla prima fase di *training*, in cui il sistema viene addestrato a partire da dati di input, segue la fase operativa, nella quale il sistema è in grado, per ogni nuovo documento ricevuto, di effettuare una predizione della categoria di appartenenza.

Infine, l'INPS, sin dal 2012, utilizza un modello statistico predittivo di *data mining* denominato SAVIO che consente di selezionare i certificati medici presentati dai lavoratori per cui risulta più opportuno predisporre controlli, in ragione della maggiore probabilità che alcuni eventi di malattia possano risolversi prima del previsto ovvero della possibilità che si verifichino comportamenti opportunistici. Si tratta di uno strumento a supporto istruttorio i cui input si inseriscono in un procedimento nel quale l'intervento umano è a più riprese garantito (decisione su come utilizzare le indicazioni circa i certificati da verificare, effettuazione del controllo, assunzione delle decisioni conseguenti)[129]. Il sistema SAVIO costituisce un esempio pionieristico di utilizzo di modelli predittivi nella pubblica amministrazione italiana. Considerato il rapidissimo progresso tecnologico, un arco temporale superiore al decennio, in termini digitali, appare lontano quanto un'era geologica; nondimeno l'esperienza di SAVIO assume rilevanza non solo sotto il profilo metodologico, ma anche per il contributo offerto al dibattito sulla legittimità dell'uso algoritmico da parte di enti pubblici. Infatti, sulla legittimità del sistema si è recentemente espressa la Corte di Cassazione[130] con un'ordinanza rilevante sotto un duplice profilo. Da un lato, posto che l'attività di controllo condotta dall'Istituto trova diretto fondamento nella legge, non è necessario il consenso dell'utente[131]; dall'altro lato, l'attribuzione agli operatori dell'INPS di specifici compiti di verifica del sistema comporta la classificazione di quest'ultimo «*in termini di modulo organizzativo, interamente svolto all'epoca in forza della legislazione attributiva del potere e delle finalità assegnate all'organo pubblico titolare del potere*»[132]. Il ritardo, pur fisiologico, con cui le pronunce giurisprudenziali intervengono a valutare soluzioni tecnologiche già in uso, come dimostra il caso SAVIO, evidenzia l'importanza di un dialogo costante tra innovazione amministrativa, normazione e controllo giurisdizionale, affinché l'evoluzione tecnologica proceda in un quadro di garanzie consolidate.

129 Ponti, B. (2023), Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità, *FrancoAngeli s.r.l.*, Milano, pp. 161 ss.

130 Cass. civ., Sez. I, Ord., 01 marzo 2023, n. 6177.

131 Ciò è peraltro espressamente previsto dall'art. 6, par. 1, lettera e) del GDPR, che consente il trattamento dei dati quando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio dei pubblici poteri di cui è investito il titolare del trattamento.

132 Così anche T.A.R. Lazio, Roma, sez. III *bis*, sent., 22.03.2017, n. 3769 «*quanto alla decisione di fare ricorso all'elaborazione elettronica ai fini della definizione del contenuto dell'atto, la predetta decisione si sostanzia, in realtà, esclusivamente nella metodologia prescelta dall'amministrazione ai fini dell'articolazione e dello svolgimento del procedimento amministrativo, che si presenta alternativa rispetto a quella tradizionale della materiale acquisizione al procedimento caso per caso di tutti gli elementi decisivi ai fini dell'assunzione della decisione finale e, pertanto, la decisione al riguardo dell'amministrazione assume essenzialmente una valenza di tipo organizzativo dell'attività amministrativa*».

Il panorama descritto, in parte riconducibile a iniziative non particolarmente recenti, risente della difficoltà nel reperire informazioni sulle sperimentazioni delle pubbliche amministrazioni, principalmente a causa della mancanza di una ricognizione sistematica delle pratiche adottate. Tuttavia, il recente quadro normativo ha innescato una tendenza innovativa: le amministrazioni, spinte anche dal principio di trasparenza, stanno iniziando a divulgare le sperimentazioni in cui sono coinvolte. Al riguardo, il Piano triennale per l'informatica nella PA 2024-2026[133] rappresenta un primo passo ricognitivo; nel medesimo solco può essere ricondotta l'iniziativa promossa dalla Banca d'Italia nell'ambito dello Strumento di sostegno tecnico (TSI),[134] in cooperazione con l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), dedicata all'utilizzo dell'intelligenza artificiale (IA) nei mercati finanziari italiani[135].

Obiettivo del progetto è esaminare in modo sistematico le opportunità e i rischi associati all'impiego dell'IA nei mercati finanziari italiani, fornendo raccomandazioni volte a supportare le autorità finanziarie nazionali nella definizione di misure concrete. Tali misure dovranno facilitare l'adozione responsabile dell'IA, mitigarne i potenziali rischi e, al contempo, promuovere l'innovazione e il contributo del settore finanziario alla crescita economica del Paese. Al termine dei lavori, previsti entro la prima metà del 2026, l'OCSE curerà un rapporto finale[136].

3 Le sperimentazioni SupTech a livello internazionale ed europeo

Guardando al di là del panorama nazionale, le prime Autorità a utilizzare e sperimentare il SupTech sono state la Securities and Exchange Commission (SEC), l'Australian Securities and Investments Commission (ASIC) e la Monetary Authority of Singapore (MAS) e la Financial Conduct Authority (FCA). Anche a livello europeo, come di seguito rilevato, l'Autorité des Marchés Financiers (AMF) e la Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hanno iniziato a impiegare sistemi di IA.

Negli Stati Uniti, la SEC, già dopo la crisi finanziaria del 2008, ha sperimentato per la prima volta semplici metodi di analisi del testo. In uno dei primi test sono stati esaminati i documenti degli emittenti aziendali per determinare se l'Autorità avrebbe potuto prevedere alcuni dei rischi derivanti dall'aumento e dall'uso di contratti di *credit default swap* [CDS] che hanno portato alla crisi finanziaria. Si trattava di una sperimentazione rudimentale che non ha prodotto gli esiti sperati, ma che ha dimostrato che i metodi di analisi del testo potevano essere facilmente applicati ai

133 Già citato in nota n. 88.

134 Programma dell'Unione europea volto a promuovere le riforme strutturali negli Stati membri, attuato tramite la Commissione europea - SG Reform.

135 Allo sviluppo del progetto collaborano il Ministero dell'Economia e delle Finanze (MEF), la CONSOB, la COVIP e l'IVASS.

136 Allo stato attuale è stata ultimata la fase di raccolta di dati, tramite questionario inviato a un'ampia platea di istituzioni finanziarie attive in Italia: banche, investitori istituzionali, infrastrutture dei mercati finanziari. Sono inoltre stati svolti *workshop* tra rappresentanti selezionati delle istituzioni e dell'industria, italiani ed esteri.

documenti depositati presso la SEC[137]. Successivamente, sono stati applicati metodi di *topic modeling*, che misurano la probabilità di parole all'interno dei documenti e tra i documenti, al fine di definire gli argomenti univoci che rappresentano. Si tratta di modelli di apprendimento non supervisionato che oggi sono ampiamente utilizzati dalla Commissione[138].

L'australiana ASIC utilizza l'intelligenza artificiale e l'apprendimento automatico per mappare il *trading* azionario in tempo reale, grazie ai dati dell'Australian Taxation Office (ATO). Identificate le connessioni tra *trader* e familiari, colleghi, vicini etc., il sistema avvisa in caso di operazioni che potrebbero essere sospette. L'impiego di questi sistemi ridurrà significativamente il lavoro manuale associato all'identificazione dell'*insider trading*, garantendo un'azione di contrasto più mirata[139].

In risposta a un'interrogazione parlamentare sull'uso dei sistemi di IA nella vigilanza degli istituti finanziari, l'autorità di Singapore MAS ha dichiarato di aver adottato un approccio basato sul rischio nell'attività di supervisione[140]. In primo luogo, la MAS ha sviluppato strumenti che utilizzano l'apprendimento automatico per migliorare il *targeting* del rischio per azioni di vigilanza o di esecuzione. Ad esempio, la MAS ha addestrato un modello di apprendimento automatico, utilizzando tratti identificati da esperti umani, per analizzare i dati di *trading* di mercato per aiutare i funzionari a identificare e dare priorità a potenziali collusioni o manipolazioni di mercato per le indagini. La MAS impiega, inoltre, l'apprendimento automatico per aiutare i supervisori a identificare i rappresentanti di consulenza finanziaria che potrebbero presentare rischi più elevati di esibire comportamenti scorretti, come la vendita scorretta di prodotti di investimento o assicurativi. Le istituzioni finanziarie con un numero maggiore di rappresentanti che presentano rischi più elevati di coinvolgimento in vendite scorrette vengono considerate prioritarie per un impegno di vigilanza più approfondito. La MAS impiega poi il *natural language processing* (NLP) per aiutare i supervisori a lavorare in modo più efficiente. Invece di far setacciare manualmente ai supervisori voluminosi dati testuali, come i report inviati dagli istituti finanziari, la MAS usa il NLP per analizzare i testi e segnalare problemi all'attenzione

137 Bauguess, SW. (2017), The Role of Big Data, Machine Learning, and AI in Assessing Risks: a Regulatory Perspective, New York, (https://www.sec.gov/newsroom/speeches-statements/bauguess-big-data-ai) il quale sul punto rileva che «*Our analysis showed that the first mention of CDS contracts in a Form 10-K was by three banks in 1998. By 2004, more than 100 corporate issuers had mentioned their use. But the big increase in CDS disclosures came in 2009. This was, of course, after the crisis was in full swing. And identification of those issues by the press wasn't much earlier. We analyzed headlines, lead paragraphs, and the full text of articles in major news outlets over the years leading up to the financial crisis and found that robust discussions of CDS topics did not occur until 2008. During that year, we found a ten-fold increase in CDS articles relative to the prior year*». Tuttavia, si noti che, anche se l'aumento delle tendenze di divulgazione dei CDS fosse stato precedente alla crisi, comunque sarebbe stato necessario saper dove e cosa cercare. Non si può eseguire un'analisi su un rischio emergente se non si sa che sta emergendo. Questa limitazione ha fornito la motivazione per la fase successiva di elaborazione del linguaggio neurale.

138 Di Castri, S. *et al.* (2019), The suptech generations, *FSI Insights on policy implementation*, n. 19, (https://www.bis.org/fsi/publ/insights19.pdf).

139 ASIC (2022), Discorso tenuto da Chair Joseph Longo al Corporate Counsel Association's Executive Committee webinar (https://asic.gov.au/about-asic/news-centre/speeches/chair-s-remarks-at-corporate-counsel-association-event/).

140 MAS (2023), Risposta scritta all'interrogazione parlamentare sull'uso dell'IA nella vigilanza (https://www.mas.gov.sg/news/parliamentary-replies/2023/written-reply-to-parliamentary-question-on-use-of-artificial-intelligence-in-supervision-of-fis).

dei supervisori. L'Autorità utilizza il NLP anche per analizzare i *social media,* tramite tecniche di *web scraping,* ed estrarre contenuto da testi che potrebbero giustificare l'attenzione della vigilanza. Infine, la MAS utilizza analisi avanzate di dati per identificare reti di attività sospette che potrebbero indicare riciclaggio di denaro, finanziamento del terrorismo o altri reati finanziari. Il *Managing Director*, nella conferenza per la presentazione del Report annuale 2023/2024, ha dichiarato, riservandosi di rivelare di più «*a tempo debito*», che la MAS ha avviato un nuovo programma chiamato *AI Collider*, come spazio di sperimentazione finalizzato a incentivare lo sviluppo e l'adozione di soluzioni basate su IA attraverso collaborazione tra istituzioni finanziarie, aziende tecnologiche e organismi di ricerca. Il programma si pone l'obiettivo di i) facilitare la condivisione sicura di dati e modelli di IA tra gli attori del sistema finanziario, ii) promuovere l'adozione responsabile dell'IA in conformità al *framework* FEAT (*Fairness*, *Ethics, Accountability, Transparency*), iii) supportare l'utilizzo di tecnologie innovative come *federated learning* e *privacy-preserving analytics*, iv) accelerare la sperimentazione congiunta di algoritmi IA per casi d'uso specifici (es. gestione del rischio, antiriciclaggio, ESG. Il primo progetto pilota ha identificato il rilevamento di truffe e frodi come caso d'uso: «*By pooling data across banks, suspicious movement of money across bank accounts of multiple banks can be detected, and prompt action taken to investigate and stop these scams*»[141].

La britannica FCA, nel *Data strategy update 2022*[142], ha dichiarato di aver utilizzato il *web scraping* per identificare potenziali abusi. In media vengono analizzati 100.000 siti web creati ogni giorno, per identificare i nuovi domini registrati che mostrano le caratteristiche che potrebbero essere utilizzate per truffe o frodi. Una volta identificati come fraudolenti o illegali, la FCA pubblica un avviso per i consumatori e chiede la rimozione al *website's registrar*. È stato poi sviluppato il *Single View Analytics Tool* (SVAT) che fornisce uno 'sportello unico' di dati e indicatori chiave su ogni azienda e fornisce un contesto per le decisioni sui rischi e su dove intervenire[143]. Il risparmio stimato dalla FCA grazie all'utilizzo di nuovi *tool* in sostituzione di vecchi sistemi inefficienti è pari a complessivamente 20 milioni di sterline. Data la complessità delle dinamiche di mercato e le più complesse forme che possono assumere gli abusi di mercato, è intenzione della FCA utilizzare l'IA come supporto nell'individuazione di tali fenomeni[144].

141 MAS (2024), Annual Report 2023/2024 Media Conference (https://www.mas.gov.sg/news/speeches/2024/mas-annual-report-media-conference-2023-2024), in italiano (traduzione nostra): «*Mettendo in comune i dati delle varie banche, è possibile individuare movimenti sospetti di denaro tra conti bancari di più istituti e intervenire tempestivamente per indagare e fermare queste truffe*».

142 FCA (2022), Data strategy update 2022 (https://www.fca.org.uk/publications/corporate-documents/data-strategy-update-2022).

143 In termini semplificati lo SVAT non è un sistema AI in sé, piuttosto uno strumento di integrazione e visualizzazione dei dati, che può incorporare o essere collegato a moduli analitici avanzati, inclusi quelli basati su AI. È parte di un ecosistema SupTech in cui l'AI è uno degli strumenti a disposizione, ma non l'elemento fondante del SVAT stesso.

144 FCA (2024), Artificial Intelligence (AI) update – further to the Government's response to the AI White Paper Corporate (https://www.fca.org.uk/publications/corporate-documents/artificial-intelligence-ai-update-further-governments-response-ai-white-paper). È interessante osservare che la stima di risparmio di circa 20 milioni di sterline pare collegata principalmente alla riduzione del tempo e delle risorse umane impiegate nei processi di selezione e di revisione delle segnalazioni, nonché a una più efficiente allocazione dei controlli di vigilanza. La stima va collocata nel

Nel contesto europeo, l'Autorité des Marchés Financiers (AMF), al pari della FCA, dal 2019 sfrutta algoritmi di *natural language processing* (NLP) per individuare siti che possano offrire investimenti potenzialmente fraudolenti. L'autorità francese, inoltre, ha sviluppato un sistema di supervisione denominato *Outil de Profilage des Intermédiaires Financiers* (OPIF), volto a rafforzare l'azione preventiva nei confronti degli intermediari operanti nel mercato finanziario. Lo strumento consente all'Autorità di attribuire a ciascun intermediario un 'profilo di rischio regolamentare', sulla base di un set di indicatori strutturati e criteri qualitativi. L'approccio si fonda principalmente su regole predefinite e modelli deterministici, risultando così pienamente conforme a un quadro regolatorio prudente, ma al contempo più contenuto dal punto di vista dell'innovazione tecnologica[145].

Di segno più marcatamente tecnologico è invece l'approccio seguito dalla tedesca Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), nel quadro dello sviluppo della *Digitale Aufsichtsplattform*, piattaforma digitale pensata per accompagnare la trasformazione del proprio modello di vigilanza. Il progetto si inserisce in una strategia di lungo periodo orientata alla digitalizzazione dei processi di supervisione e alla progressiva automazione della gestione dei flussi informativi tra autorità e soggetti vigilati. La piattaforma è concepita per integrare strumenti di *machine learning*, applicati all'analisi di grandi volumi di dati (*big data*) provenienti da banche, assicurazioni e altre istituzioni finanziarie. L'obiettivo dichiarato è quello di rafforzare la capacità della BaFin di individuare tempestivamente *pattern* di rischio e comportamenti anomali, incluse ipotesi di abusi di mercato[146] [147].

Dalla breve ricognizione effettuata è possibile trarre alcune indicazioni circa le tendenze in atto. Le iniziative intraprese dalle Autorità a livello globale ed europeo mostrano una crescente propensione verso l'implementazione dei sistemi di intelligenza artificiale. Alla luce dello studio del 2019 del Financial Stability Institute, sopra citato, anche a fronte dei diversi e non assimilabili impieghi e/o sperimentazioni, potremmo dire che le autorità si trovano nella seconda o terza categoria, ossia in quella diagnostica o al massimo predittiva.

contesto di un budget complessivo annuale della FCA pari a circa 762 milioni di sterline (esercizio 2023/24), di cui circa 38 milioni destinati a investimenti tecnologici.

145 Si tratta di uno strumento che – allo stato attuale - non incorpora moduli di IA o machine learning, pur rappresentando un progresso nel monitoraggio sistematico dei soggetti vigilati. La finalità principale resta quella di fornire un supporto alla vigilanza ex ante, utile alla calibrazione degli interventi ispettivi e all'allocazione efficiente delle risorse di controllo. AMF (2024), Vérifications à faire concernant votre intermédiaire financier (https://www.amf-france.org/fr)

146 BaFin (2022). Machine learning in risk models (https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2022/fa_bj_2202_Maschinelles_Lernen_en.html); Sims, T. (2025), German financial watchdog: AI is helping to catch market abuse, in *Reuters.com* (https://www.reuters.com/sustainability/boards-policy-regulation/german-financial-watchdog-ai-is-helping-catch-market-abuse-2025-06-02).

147 Carini, V. (2024), Authority Ue e Borse: così l'IA è alleata contro gli abusi, in *Il Sole 24 Ore*, 20 marzo 2024 p. 46.

4 Le sperimentazioni SupTech della CONSOB

Con specifico riferimento alla CONSOB, come indicato in premessa, nel contesto dell'adozione di strumenti SupTech per il rafforzamento dell'attività di vigilanza sono stati sviluppati diversi prototipi.

Un primo gruppo di sperimentazione ha riguardato una delle aree di vigilanza più massivamente caratterizzate dall'analisi di dati (*data driven*), ovvero la vigilanza sulle transazioni sui mercati regolamentati e sulle piattaforme di scambio vigilate dall'Istituto. L'obiettivo dei prototipi è stato quello di ideare strumenti di supporto alla analisi per la *detection* di possibili casi di abusi di mercato; al riguardo si pone in evidenza come il presente lavoro si focalizza proprio sui prototipi sviluppati in tale ambito, ai quali sarà dedicata un'ampia rassegna al successivo Capitolo III.

Un secondo tipo di sperimentazione è stata applicata a supporto della vigilanza dei documenti cosiddetti KID (*Key Information Document*) che illustrano le caratteristiche principali dei prodotti finanziari pre-assemblati destinati agli investitori al dettaglio (PRIIPs – *Packaged Retail and Insurance-based Investment Products*). Il produttore di un PRIIP deve predisporre un documento standardizzato contenente le informazioni chiave relative al prodotto di investimento, ad esempio la struttura di *pay off*, gli obiettivi di investimento, i costi, i guadagni e le perdite potenziali ai sensi del Regolamento (UE) 1286/2014. Le informazioni contenute nei KID, in formato testo o tabulare, devono rispettare i *template* e le metodologie previste dal Regolamento Delegato dell'Unione europea n. 653/2017. La numerosità dei documenti notificati alla CONSOB ne rende impossibile lo scrutinio completo da parte dei funzionari e richiede l'utilizzo di criteri di selezione basati su parametri di rischio. Tale sperimentazione, sviluppata in collaborazione con l'Università La Sapienza, si basa su tecniche di *information extraction,* ossia di un processo automatico che struttura e combina selettivamente i dati che si trovano nei testi o in sorgenti di dati semi-strutturati, con approccio *pattern based* e *learning based.* Il primo approccio consente di classificare i prodotti in macro classi, dal livello più specifico a quello più generale, attraverso un'attività di estrazione e selezione dei dati, dopo la trasformazione dei KID dal formato pdf in testo. Il secondo approccio presuppone, invece, la trasformazione dei KID in immagine da cui poter estrarre informazioni quantitative attraverso l'uso di reti neurali addestrate a riconoscere tabelle. L'interazione fra la parte narrativa e numerica dei KID necessita infatti di due diversi modelli fra loro complementari al fine di costruire in maniera automatica un *dataset* strutturato che può essere processato sia da sistemi automatici sia da persone, con potenziali e significativi benefici di analisi in termini di prioritizzazione delle azioni di vigilanza attraverso uno *screening* automatico dei KID[148].

Una sperimentazione più recente riguarda l'attività di contrasto agli abusivismi finanziari, fenomeno in espansione e sempre più radicato nell'ambiente digitale, soprattutto in relazione all'offerta illecita di cripto-attività e servizi

148 Lembo, D. *et al.* (2022) Information Extraction through AI techniques: The KIDs use case at CONSOB, in *arXiv,* pp. 1-4 (https://doi.org/10.48550/arXiv.2202.01178).

d'investimento. In tale ambito, è stato avviato un percorso di collaborazione con due istituzioni accademiche, finalizzato alla realizzazione di un prototipo informatico basato sull'impiego di tecnologie di IA, capace di affiancare e potenziare le capacità di *detection* dell'Autorità. Il sistema è concepito per automatizzare le attività di analisi e verifica che attualmente caratterizzano il processo di gestione degli esposti. A partire dai contenuti delle segnalazioni ricevute, il modello è in grado di estrarre in modo automatico informazioni strutturate relative ai soggetti coinvolti, ai siti web indicati, alla presenza di strumenti finanziari o cripto-asset, nonché ad altri elementi significativi per la qualificazione del comportamento segnalato. Sulla base di tali dati, il sistema procede a una navigazione automatica delle fonti *online*, eseguendo il *download* e l'analisi dei contenuti rilevanti, al fine di ricostruire le modalità operative dei soggetti e di verificare eventuali profili di illiceità.

Il cuore tecnologico del prototipo risiede nell'impiego di modelli linguistici di grandi dimensioni (LLM, *Large Language Models*), anche nella loro forma multimodale, in grado di processare input testuali e visivi. Tali modelli sono addestrati per eseguire operazioni di classificazione e sintesi delle informazioni, con riferimento ai quadri regolatori di MiFID e MiCAR, e generare report automatizzati destinati a supportare il lavoro degli uffici nella predisposizione di atti formali, come relazioni, delibere e provvedimenti di oscuramento. L'intero processo prevede una fase di validazione e *backtesting*, nella quale i risultati prodotti dal sistema vengono confrontati con l'analisi condotta da operatori umani. In caso di disallineamento, il *prompt* di sistema viene modificato e l'inferenza ripetuta, con l'obiettivo di raffinare progressivamente l'accuratezza e l'affidabilità dell'output.

Infine, in collaborazione con l'Università di Trento è stata avviata una sperimentazione con l'obiettivo di sviluppare un sistema di supporto alla vigilanza sui *green bond* europei, attraverso l'impiego di tecniche di IA e *Natural Language Processing* (NLP). Alla luce del crescente ricorso a etichette ESG – *Environmental, Social and Governance* nelle emissioni obbligazionarie e dell'aumento delle controversie legate a potenziali casi di *greenwashing*, l'esigenza regolatoria si concentra sulla verifica dell'effettiva coerenza tra le dichiarazioni di sostenibilità contenute nei documenti ufficiali e le reali pratiche attuate dagli emittenti. Il cuore del progetto, in questo caso, consiste nella costruzione di un prototipo informatico in grado di analizzare automaticamente la documentazione testuale associata alle emissioni di *green bond* – in particolare prospetti, *sustainability reports* e documentazione di *marketing* – con l'obiettivo di individuare frasi rilevanti dal punto di vista ambientale, etichettarle in funzione del loro contenuto (menzione ambientale, *claim* ambientale), associarvi un giudizio di *sentiment* (neutrale, opportunità, rischio) e verificare la presenza o l'assenza di riferimenti agli obiettivi di sviluppo sostenibile (SDG - *Sustainable Development Goals*). Particolare rilievo è attribuito alla misurazione dello scostamento (*mismatch*) tra gli SDG dichiarati formalmente dall'emittente e quelli effettivamente rilevabili nei documenti, considerato potenziale indicatore di *greenwashing*. Dal punto di vista tecnico, il prototipo utilizza modelli avanzati di NLP basati, ottimizzati per la comprensione contestuale del linguaggio finanziario e ambientale. L'analisi è articolata in diverse fasi: pulizia e segmentazione del testo, identificazione delle frasi ambientali e dei *claims*, assegnazione del *sentiment* e infine

mappatura degli SDG. I risultati vengono restituiti in forma strutturata, consentendo un'analisi scalabile e sistematica di migliaia di frasi in tempi significativamente ridotti rispetto alla lettura umana. Il valore aggiunto del modello risiede nella possibilità di generare '*alert*' di vigilanza su documenti e soggetti che presentano caratteristiche potenzialmente anomale – ad esempio, un elevato *mismatch* tra SDG dichiarati e riscontrati, o un *sentiment* prevalentemente opportunistico in assenza di riscontri concreti – che possono orientare l'attività degli uffici verso indagini più approfondite. Anche in questo caso, il modello – promettente – richiede ulteriori fasi di addestramento, prima di poter essere pienamente integrato nei sistemi di vigilanza. Alla luce della rapidissima evoluzione del settore, risulta particolarmente complesso monitorare in modo sistematico gli sviluppi in corso presso le diverse autorità di vigilanza dei mercati finanziari. Ciononostante, si ritiene utile proporre una ricognizione delle principali evidenze sinora emerse, con specifico riferimento al contesto europeo, pur senza alcuna pretesa di esaustività.

Tavola 1 – Principali applicazioni SupTech adottate da autorità europee di vigilanza sui mercati finanziari

autorità	strumento / iniziativa	obiettivo principale	tecnologie adottate	grado di maturità
FCA (UK)	- Single View Analytics Tool (SVAT) - Web scraping	Vista integrata e dinamica dei soggetti vigilati, identificazione truffe/frodi	Data integration, dashboarding, moduli AI opzionali NLP, LLM	Operativo e in aggiornamento
AMF (Francia)	- Outil de Profilage des Intermédiaires Financiers (OPIF) - Web scraping	Profilazione del rischio degli intermediari, identificazione truffe/frodi	Rule-based profiling, indicatori deterministici NLP, LLM	Stabile ma non AI-based
BaFin (Germania)	- Digitale Aufsichtsplattform - AI Monitoring Systems	Digitalizzazione della vigilanza; detection automatica di rischi	ML, AI per abusi di mercato, big data analytics	In espansione, con adozione concreta di AI
CONSOB (Italia)	Prototipi SupTech - Greenwashing Alert - Insider Trading - Web scraping	Individuazione automatica di greenwashing e abusi di mercato; identificazione truffe/frodi	ML e rule-based AI; NLP, LLM (es. ClimateBERT, ESG-BERT)	Sperimentale avanzato

In generale, tutte le sperimentazioni condotte rappresentano un tentativo avanzato di integrare soluzioni di intelligenza artificiale all'interno dei processi di vigilanza tradizionali, con l'obiettivo di aumentarne tempestività, efficienza e capacità analitica. L'implementazione, tuttavia, solleva anche importanti questioni organizzative e metodologiche, legate alla necessità di garantire un equilibrio tra automazione e controllo umano, nonché alla ridefinizione dei flussi operativi e delle competenze richieste agli operatori coinvolti.

È giunto quindi il momento di approfondire le sperimentazioni condotte dalla CONSOB in ambito SupTech con particolare riferimento all'area della repressione delle fattispecie di abuso di mercato e, in particolare, dell'*insider trading*.

CAPITOLO TERZO

Come l'IA può supportare la vigilanza della CONSOB sugli abusi di mercato

1 Le fattispecie di abuso di mercato: *insider trading* e manipolazione di mercato

Prima di affrontare il tema di come l'IA possa essere di supporto all'attività di vigilanza che la CONSOB svolge sugli abusi di mercato appare utile tratteggiare – senza pretesa alcuna di esaustività – il quadro normativo che definisce le condotte oggetto di analisi.

La cornice normativa eurounitaria in materia di abusi di mercato, risultante anche dal Regolamento (UE) MAR e dalla Direttiva (UE) MAD II, è articolata sulla possibilità di configurazione di un doppio binario sanzionatorio di illeciti penali e illeciti amministrativi, in quanto lascia agli Stati membri la facoltà di punire le violazioni di *market abuse*, oltre che con sanzioni penali per le condotte ritenute più gravi, anche con sanzioni amministrative. Il che delinea non solo discipline nazionali non armonizzate ma, com'è stato notato, possibili difficoltà di coordinamento tra i procedimenti dell'autorità di vigilanza e i processi dell'autorità giurisdizionale e il rischio di violazione del principio eurounitario (art. 50 Carta dei diritti fondamentali UE) e convenzionale (art. 7 CEDU) del *ne bis in idem*[149].

Nell'ordinamento italiano, in attuazione delle regole, anche non direttamente applicabili perché non *self-executing*, provenienti dall'UE[150], il decreto legislativo 24 febbraio 1998, n. 58 (di seguito, anche solo TUF), attualmente in vigore, prevede un doppio binario sanzionatorio di illeciti penali e amministrativi. Le fattispecie penali (artt. 184 e 185 TUF), sanzionate con pene detentive e pecuniarie, intendono prevenire e reprimere le condotte abusive più gravi, unicamente a carattere doloso, mentre le fattispecie d'illecito amministrativo (artt. 187-*bis* e 187-*ter* TUF) comprendono anche le condotte abusive meno gravi, tanto a titolo di dolo quanto a titolo di colpa, che trovano la propria risposta sanzionatoria in misure pecuniarie e interdittive[151].

149 Su quest'ultima questione la legislazione europea incarica gli Stati membri di garantire che l'irrogazione di sanzioni penali per i reati ai sensi della Direttiva (UE) MAD II e di sanzioni amministrative ai sensi del Regolamento (UE) MAR non violino il divieto del doppio processo per l'*idem factum* (considerando n. 23 della Direttiva MAD II), questione poi che, come si vedrà *infra*, è stata amplificata dalla natura sostanzialmente penale delle sanzioni amministrative e dalla relativa estensione dei principi del processo equo al procedimento. Su alcune proposte di soluzione, a legislazione vigente e *de iure condendo*, v. Deodato, C. (2019), Sanzioni formalmente amministrative e sostanzialmente penali: i problemi procedurali connessi all'applicazione delle sanzioni CONSOB in materia di materia di market abuse (e alcune soluzioni), in *federalismi.it*, n. 23, 2019, pp. 28 ss.

150 In principio, la Direttiva 89/592/CEE del 13 novembre 1989 (*Coordinating Regulations on insider trading*) aveva previsto unicamente il divieto di *insider trading*. Soltanto con la Direttiva CE/6/2003 (Market Abuse Directive – MAD I) è stata inclusa, nell'ambito delle fattispecie di *market abuse*, quella di manipolazione del mercato, imponendo agli Stati membri l'obbligo di adottare le sanzioni amministrative e lasciando libertà ai legislatori nazionali quanto all'introduzione delle sanzioni penali per entrambe le fattispecie. Successivamente, il legislatore eurounitario ha adottato due nuovi strumenti normativi (il Regolamento (UE) 596/2014, Market Abuse Regulation – MAR, e la Direttiva 2014/57/UE, Criminal Sanctions Market Abuse Directive – CSMAD, o Market Abuse Directive 2 – MAD II). Con il Regolamento (UE) MAR, che si applica dal 2 luglio 2016, è stato perseguito l'obiettivo di massima e immediata armonizzazione delle fattispecie in analisi, è stato esteso l'ambito di applicazione e sono stati definiti nel dettaglio i limiti edittali e non delle sanzioni amministrative; con la Direttiva MAD II è stato previsto l'obbligo (e non più la facoltà) degli Stati membri UE di introdurre sanzioni penali.

151 La fattispecie di manipolazione del mercato può essere realizzata mediante più condotte differenti: le condotte di cosiddetta manipolazione informativa per la diffusione di notizie false e le condotte di cosiddetta manipolazione operativa tramite il conferimento di ordini o l'esecuzione di operazioni secondo una varietà di strategie, alcuni delle quali esemplificativamente indicate. Si tratta di comportamenti che possono alterano la trasparenza e la correttezza

Le fattispecie di abusi di mercato di divieto di *insider trading* e di manipolazione di mercato intendono tutelare beni giuridici differenti: il divieto di *insider trading* salvaguarda la parità di accesso alle informazioni sensibili e contrasta lo sfruttamento illegittimo di informazioni privilegiate[152]; il divieto di manipolazione del mercato protegge l'andamento degli scambi dalla diffusione di informazioni false, da comportamenti simulati o altri artifici da parte di coloro che sono in grado di influire sul processo di formazione dei prezzi degli strumenti finanziari.

La disciplina penale sull'illecito di abuso di informazioni privilegiate riguarda anzitutto gli '*insider* primari' e, precisamente, chiunque, essendo in possesso delle stesse in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio, o per il fatto di essere coinvolto in attività criminali:

«*a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;*

b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato effettuato ai sensi dell'art. 11 del Regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014;

c) raccomanda o induce altri, sulla base di tali informazioni, al compimento di taluna delle operazioni indicate nella lettera a)» (art. 184 TUF).

delle negoziazioni in ambito finanziario. L'eventuale realizzazione di due o più delle condotte darà sempre luogo a una sola sanzione penalmente rilevante e non a un concorso di illeciti.

152 La normativa ruota intorno a due principali obblighi: uno di *disclosure* in quanto impone alle società quotate di comunicare immediatamente al mercato tutte le informazioni privilegiate di cui vengono a conoscenza e che le riguardano; un divieto di operare e anche di rivelare in modo selettivo ad alcuni soggetti queste informazioni privilegiate o dare consigli di investimento. In base all'art. 7 del Regolamento (UE) *MAR*, l'informazione è privilegiata quando ricorrono quattro elementi: a) l'informazione riguarda uno o più emittenti (cosiddetta *corporate information*) o uno o più strumenti finanziari (cosiddetta *market information*), b) l'informazione non è pubblica, ovvero un'informazione non disponibile alla generalità degli investitori sul mercato, c) l'informazione ha carattere «*preciso*», d) l'informazione è *price sensitivity*, ossia è un'informazione che, se resa pubblica, «*potrebbe avere un effetto significativo sui prezzi di tali strumenti finanziari*». In particolare, l'informazione ha carattere preciso se i) «*fa riferimento a una serie di circostanze esistenti o che si può ragionevolmente ritenere che vengano a prodursi o a un evento che si è verificato o del quale si può ragionevolmente ritenere che si verificherà*» e se ii) «*è sufficientemente specifica da permettere di trarre conclusioni sul possibile effetto di detto complesso di circostanze o di detto evento sui prezzi degli strumenti finanziari*». Inoltre, nel caso di un «*processo prolungato che è inteso a concretizzare, o che determina, una particolare circostanza o un particolare evento, tale futura circostanza o futuro evento, nonché le tappe intermedie di detto processo che sono collegate alla concretizzazione o alla determinazione della circostanza o dell'evento futuri, possono essere considerati come informazioni aventi carattere preciso*». E ancora, è chiarito nello stesso articolo che una «*tappa intermedia in un processo prolungato*» può costituire, a sua volta, un'informazione privilegiata. Riguardo alla *price sensitivity*, per «*informazione che, se comunicata al pubblico, avrebbe probabilmente un effetto significativo sui prezzi degli strumenti finanziari (...) s'intende un'informazione che un investitore ragionevole probabilmente utilizzerebbe come uno degli elementi su cui basare le proprie decisioni di investimento*». L'accertamento della consumazione dell'abuso di informazione privilegiata è di difficile individuazione ed è necessario il ricorso a presunzioni che consentano di risalire al fatto ignoto (*factum probandum*) desumendolo da fatti noti gravi, precisi e concordanti (indizi o fonti della presunzione) alla stregua di canoni di ragionevole probabilità e secondo regole di esperienza. Sull'evoluzione della nozione di informazione privilegiata, sia in ambito normativo sia in quello giurisprudenziale, si veda Seminara, S. (2020), L'informazione privilegiata, in Cera M., Presti, G., a cura di, Il testo unico finanziario, Zanichelli, Bologna, pp. 2124 ss.

L'illecito è esteso anche ai cosiddetti '*insider* secondari', intendendosi per tali coloro che entrano in possesso di informazioni privilegiate per altre circostanze sapendo, o comunque dovendo sapere, che si tratta di informazioni privilegiate.

La disciplina penale sulla manipolazione del mercato punisce invece chiunque diffonda notizie false o ponga in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari (art. 185 TUF).

Con riferimento agli illeciti amministrativi, la Corte EDU ha proceduto alla loro riqualificazione come sostanzialmente penali a causa del livello di severità delle sanzioni (pecuniarie, interdittive e ablatorie)[153], applicando i criteri elaborati nella sentenza *Engel*[154]. Tale interpretazione è stata poi condivisa dalla Corte di giustizia UE[155] e dalla Corte costituzionale[156], suscitando perplessità sulla presunta violazione di alcuni principi fissati dalla CEDU e dalla Carta dei diritti fondamentali UE[157].

Anzitutto, con particolare riguardo alla violazione del diritto a un processo equo, la sentenza *Grande Stevens* ha chiarito che, nell'ambito del procedimento sanzionatorio CONSOB[158], le garanzie del giusto processo sono comunque

153 Corte EDU, 4 marzo 2014, ric. n. 18640/2010, Grande Stevens e altri c. Italia. Su questa decisione si vedano *ex multis* i commenti di Flick G.M, Napoleoni, V. (2014), Cumulo tra sanzioni penali e amministrative: doppio binario o binario morto? "Materia penale", giusto processo e ne bis in idem nella sentenza della Corte Edu, 4 marzo 2014, sul market abuse, in *Riv. AIC* (*rivistaaic.it*), n. 3, 11 luglio 2014, nonché in *Riv. soc.*, n. 5, 2014, pp. 953 ss.; Viganò, F. (2014), Doppio binario sanzionatorio e ne bis in idem: verso una diretta applicazione dell'art. 50 della Carta?, in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*), n. 3, pp. 219 ss.; Montalenti, P. (2015), Abusi di mercato e procedimento CONSOB: il caso Grande Stevens e la Sentenza CEDU, in *Giur. comm.*, n. 3, pp. 478 ss.; Genovese, A. (2017), Il controllo del giudice sulla regolazione finanziaria, in *Banca borsa tit. cred.*, n. 1, pp. 49 ss.; Ventoruzzo, M. (2014), Abusi di mercato sanzioni CONSOB e diritti umani: il caso Grande Stevens e altri c. Italia, in *Riv. soc.*, n. 4, pp. 693 ss.

154 Corte EDU, 8 giugno 1976, ric. n. 5100/71, *Engel e altri c. Paesi Bassi*, ha definito tre criteri per la qualificazione sostanzialmente penale delle sanzioni amministrative: la qualificazione giuridica dell'illecito nel diritto nazionale; la natura dell'illecito e la finalità repressiva della sanzione; la natura punitiva e il grado di severità della sanzione; il collegamento con una violazione penale. Dopo questa sentenza, la Corte EDU, 28 novembre 1999, *Escobet c. Belgio*, ha sostenuto che «*in ogni caso la nozione di pena contenuta nell'art. 7 della Convenzione come quella di accusa in materia penale che figura nell'art. 6 hanno portata autonoma* [...] *la Corte non è vincolata dalle qualificazioni del diritto interno, che hanno valore relativo*». Sui criteri sviluppati dalla vicenda *Engel* si è espressa in senso sostanzialmente conforme alla Corte EDU la Corte di giustizia UE, sentenze del 5 giugno 2012, *Bonda*, C-489/10, EU:C:2012:319, punto 37, e del 26 febbraio 2013, *Åkerberg Fransson*, C-617/10, EU:C:2013:105, punto 35.

155 Rispettivamente con riferimento alla fattispecie di manipolazione del mercato, prevista dall'art. 187-*ter* TUF, e alla fattispecie di abuso di informazione privilegiata, prevista dall'art. 187-*bis* TUF, la Corte di giustizia UE, sentenza del 20 marzo 2018, *Garlsson Real Estate SA c. Consob*, C-537/16, EU:C:2018:193, punto 33, e sentenza del 20 marzo 2018, *Di Puma c. Consob*, C-596/16 e C-597/16, EU:C:2018:192, punto 35, qualifica le sanzioni sostanzialmente penali sulla base della natura dell'illecito e della gravità della sanzione.

156 Corte cost., sentenza 21 marzo 2019, n. 63, sulla retroattività *in mitius* delle sanzioni amministrative, sulla quale si rinvia al commento di Bindi, E., Pisaneschi, A. (2019), La retroattività in mitius delle sanzioni amministrative CONSOB, in *Giur. comm.*, n. 5, pp. 1015 ss., e Corte cost., ordinanza 10 maggio 2019, n. 117, sul diritto al silenzio (*nemo tenetur se detegere*), sulla quale si rinvia ai commenti di Logli, A. (2020), Poteri istruttori della CONSOB e nemo tenetur se detegere, in *Giur. comm.*, n. 2, pp. 230 ss.; Caneschi G. (2020), Nemo tenetur se detegere anche nei procedimenti amministrativi sanzionatori? La parola alla Corte di giustizia, in *Cass. pen.*, n. 2, pp. 579 ss. In generale sul tema si rinvia ad allena, M., Vaccari, S. (2022), Diritto al silenzio e autorità di vigilanza dei mercati finanziari, in *Riv. dir. banc.* (*rivista.dirittobancario.it*), n. 3, pp. 689 ss.

157 Su tutte queste questioni si veda Deodato, C. (2019), *op. cit.*, pp. 1 ss.

158 La presunta violazione si riferiva al previgente Regolamento sul procedimento sanzionatorio CONSOB 19 dicembre 2013, n. 18750, nella misura in cui il procedimento non garantiva il rispetto di un contraddittorio adeguato, non prevedeva un'udienza pubblica e non assicurava l'imparzialità dell'organo giudicante. In particolare, il procedimento,

salvaguardate dalla previsione del giudizio di opposizione davanti alla Corte d'Appello, per motivi anche di merito, e dal giudizio di legittimità dinnanzi alla Corte di Cassazione, per soli motivi di legittimità, contro i medesimi provvedimenti sanzionatori dell'autorità di vigilanza. Secondo la Corte EDU lo Stato è infatti libero di scegliere dove collocare le garanzie dell'equo processo, nella fase amministrativa o nella fase giurisdizionale, in quanto trattasi di decisione rimessa all'apprezzamento delle autorità nazionali[159].

In secondo luogo, la Corte EDU ha riconosciuto la legittimità di una duplice risposta sanzionatoria e di una pluralità di procedimenti riguardanti il medesimo fatto qualora vi sia una «*connessione sostanziale e temporale sufficientemente stretta*», ravvisabile in presenza di alcuni determinati criteri[160]. Sul medesimo profilo, la Corte di giustizia UE ha ribadito la legittimità del doppio binario sanzionatorio lasciando agli Stati membri facoltà di scelta nell'individuazione delle sanzioni applicabili che possono avere la consistenza di sanzioni amministrative, di sanzioni penali o di una

così come era articolato, era in contrasto con il principio di parità delle armi di accusa e difesa in quanto non consentiva all'interessato un'interlocuzione sulla Relazione conclusiva prima della determinazione finale della Commissione.

159 Dopo la sentenza Grande Stevens della Corte EDU il Consiglio di Stato (sentenze 26 marzo 2016, n. 1595 e n. 1596) ha ravvisato l'incompatibilità del procedimento sanzionatorio CONSOB con il principio del contraddittorio sancito dall'art. 195 TUF poiché la Relazione conclusiva dell'Ufficio Sanzioni Amministrative «*non è oggetto di comunicazione (o di altre forme di conoscenza) e rispetto ad esso non vi è alcuna possibilità di controdeduzione*». Tuttavia, queste pronunce non hanno ravvisato alcun contrasto con la CEDU ma unicamente i principi del contraddittorio 'rinforzato' sanciti dall'art. 187-*septies* TUF. Oltre a queste pronunce della giustizia amministrativa, anche decisione della giustizia ordinaria hanno pronunciato la legittimità del procedimento sanzionatorio della CONSOB (Corte d'Appello di Roma, decreto 30 maggio 2014; Corte d'Appello di Roma, sentenza 1° luglio 2014; Corte d'Appello di Bologna, sentenza 3 marzo 2015, n. 199). La CONSOB ha comunque modificato il Regolamento sul Procedimento Sanzionatorio, con delibera n. 19521 del 24 febbraio 2016, introducendo il diritto dei destinatari della lettera di contestazione degli addebiti, che abbiano presentato deduzioni scritte o abbiano partecipato all'audizione, di ricevere la relazione finale e di presentare le proprie controdeduzioni rispetto alle conclusioni raggiunte dall'ufficio entro trenta dalla ricezione della stessa.

160 Corte EDU, sentenza 15 novembre 2016, ric. nn. 24130/11 e 29758/11, *A. e B. c. Norvegia*, ha elaborato alcuni criteri per individuare una siffatta connessione dal punto di vista sostanziale e temporale. Con riferimento ai primi la connessione sussiste «– *whether the different proceedings pursue complementary purposes and thus address, not only in abstracto but also in concreto, different aspects of the social misconduct involved; – whether the duality of proceedings concerned is a foreseeable consequence, both in law and in practice, of the same impugned conduct ("in idem"); – whether the relevant sets of proceedings are conducted in such a manner as to avoid as far as possible any duplication in the collection and in the assessment of the evidence, notably through adequate interaction between the various competent authorities to ensure that the establishment of the facts in one set of proceedings is replicated in the other; – and, above all, whether the sanction imposed in the proceedings which become final first is taken into account in those which become final last, so as to prevent the situation where the individual concerned is in the end made to bear an excessive burden, this latter risk being least likely to be present where there is in place an offsetting mechanism designed to ensure that the overall quantum of any penalties imposed is proportionate*». Con riguardo alla connessione temporale «*the two sets of proceedings have to be conducted simultaneously from beginning to end. […] the connection in time must be sufficiently close to protect the individual from being subjected to uncertainty and delay and from proceedings becoming protracted over time*». Per alcuni commenti sulla sentenza si rinvia a Viganò, F. (2016), La Grande Camera della Corte di Strasburgo su ne bis in idem e doppio binario sanzionatorio, in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*), e a Tripodi, A.F. (2018), Corte europea dei diritti dell'uomo e sistemi sanzionatori in materia di abusi di mercato e di violazioni tributarie: la quiete dopo la tempesta, in *Soc.*, n. 1, pp. 80 ss.

combinazione di entrambe[161] purché le sanzioni complessivamente irrogate rispettino il principio di proporzionalità[162].

Inoltre, la Corte costituzionale ha esteso al procedimento sanzionatorio in materia di abusi di mercato le garanzie convenzionali del *favor rei* e della retroattività della *lex mitior*[163]. In particolare, con la sentenza n. 63 del 2019, è stato dichiarato incostituzionale l'art. 6, comma 2, del decreto legislativo n. 72 del 2015 nella parte in cui escludeva l'applicazione retroattiva della legge successiva più favorevole. In tale circostanza, i giudici costituzionali hanno affermato l'applicazione dei principi elaborati in materia penale qualora il fatto non sia più considerato illecito o sia mutato l'apprezzamento della gravità di esso da parte dell'ordinamento, salvo che vi siano

161 Corte di giustizia UE, sentenza 20 marzo 2018, C-524/15, *Menci*, par. 47; Corte di giustizia UE, sentenza 20 marzo 2018, C-537/16, *Garlsson Real Estate SA e altri*, punto 49; Corte di giustizia UE, sentenza 20 marzo 2018, C-596/16 e C-597/16, *Di Puma c. Consob*, punto 26. Su queste tre decisioni si rinvia a Consulich, F. (2018), Il prisma del ne bis in idem nelle mani del Giudice eurounitario, in *Dir. pen. proc.*, n. 7, 2018, pp. 949 ss.

162 Corte di giustizia UE, sentenza 20 marzo 2018, C-537/16, *Garlsson Real Estate SA e altri*, punto 60, aveva manifestato perplessità sull'efficacia del principio di proporzionalità, considerato il tenore previgente dell'art. 187-*terdecies* TUF che sembrava fare riferimento soltanto al cumulo di pene pecuniarie e non anche al cumulo di una sanzione amministrativa pecuniaria di natura penale e di una pena della reclusione. L'art. 187-*terdecies* TUF vigente stabilisce, in applicazione di detto principio, che l'autorità, giudiziaria o amministrativa, che si pronuncia per seconda sullo stesso fatto, debba tenere conto, al momento dell'irrogazione delle sanzioni di proprio competenza, delle misure già irrogate. Questo controllo di proporzionalità può condurre, come affermato dalla giurisprudenza di legittimità, a disapplicare, totalmente o parzialmente, la sanzione che debba essere applicata per ultima qualora la prima sia commisurata al disvalore del fatto o comunque a modulare la seconda tenendo conto della prima. Sul controllo di proporzionalità si veda Corte di Cassazione penale, Sez. V, sentenza 15 aprile 2019, n. 3999. Si veda Pagella, C. (2020), L'inafferrabile concetto di «*connessione sostanziale e temporale sufficientemente stretta*»: la Cassazione ancora sul ne bis in idem e *insider trading*, in *Sistema penale* (*sistemapenale.it*). Si è avuta applicazione dell'art. 187-*terdecies* TUF da parte della Corte d'Appello di Milano, Sez. II, sentenza 15 gennaio 2019 (dep. 15 aprile 2019), n. 284, sulla quale si rinvia al commento di Pagella, C. (2019), Riflessi applicativi del principio di proporzione del trattamento sanzionatorio complessivamente irrogato per i fatti di market abuse e punibilità dell'insider di sé stesso: la Corte di Appello di Milano sul caso Cremonini, in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*). Un siffatto scrutinio di proporzionalità della complessiva risposta sanzionatoria, tuttavia, potrebbe non essere sufficiente dopo la sentenza della Corte EDU, 6 giugno 2019, ric. n. 47342/14, *Nodet c. Francia*, che – pur esplicitamente estendendo i criteri di *A/B c. Norvegia* agli abusi di mercato – aderisce a una interpretazione restrittiva dei criteri, che riguarderebbe non solo il piano sanzionatorio ma il diritto a non essere sottoposto a due procedimenti per il medesimo fatto, con conseguente valutazione di tutti i parametri della cosiddetta «*close connection*» per escludere la violazione del *ne bis in idem*. Sulla sentenza si veda la nota di Scoletta, M. (2019), Il ne bis in idem 'preso sul serio': la Corte EDU sulla illegittimità del doppio binario francese in materia di abusi di mercato (e i possibili riflessi nell'ordinamento italiano), in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*). Sul doppio binario sanzionatorio è intervenuta da ultimo la Corte costituzionale, sentenza 16 giugno 2022, n. 149, in materia di violazione dei diritti d'autore. La Corte ha reputato fondata la questione di illegittimità costituzionale dell'art. 649 c.p.p. nella parte in cui non prevede che il giudice pronunci il proscioglimento o il non luogo a procedere nei confronti di un imputato per un delitto in materia di diritto d'autore che, in relazione allo stesso fatto, sia già stato sottoposto a un procedimento sanzionatorio, ormai concluso. In questa circostanza i giudici hanno altresì rivolto un monito al legislatore per superare la disarmonia e rimeditare complessivamente i sistemi di doppio binario sanzionatorio ancora vigenti.

163 Il fondamento del principio di retroattività *in mitius* ha ricevuto un fondamento costituzionale nell'art. 3 Cost.: il principio di eguaglianza «*impone, in linea di massima, di equiparare il trattamento sanzionatorio dei medesimi fatti, a prescindere dalla circostanza che siano stati commessi prima o dopo l'entrata in vigora della norma che ha disposto l'*abolitio criminis *o la modifica mitigatrice*» (Corte costituzionale, sentenza 27 luglio 2011, n. 236). Invero, tale principio è entrato a fare parte dell'ordinamento nazionale con la pronuncia della Corte EDU (sentenza 17 settembre 2009, ric. n. 10249/03, *Scoppola c. Italia*) che, per il tramite della norma di apertura all'ordinamento convenzionale dell'art. 117 Cost., ha ricevuto un nuovo fondamento con l'interposizione dell'art. 7 CEDU, salvo disconoscere la sua natura assoluta qualora il legislatore individui deroghe o limitazioni sorrette da una valida giustificazione.

ragioni di tutela di interessi di rango costituzionale tali da resistere al medesimo vaglio di ragionevolezza[164].

Da ultimo, nei procedimenti amministrativi in materia di *market abuse* davanti alla CONSOB sono state estese le garanzie concernenti l'applicazione del diritto di non cooperare alla propria incriminazione (cosiddetto *nemo tenetur se detegere*) e del diritto al silenzio da parte dell'incolpato. La questione è stata oggetto di un dialogo giurisprudenziale tra Corte costituzionale[165] e Corte di giustizia UE[166], a seguito di un incidente di costituzionalità sollevato dalla Corte di Cassazione[167]. In particolare, i giudici di Lussemburgo, partendo dalla considerazione che il diritto al silenzio è garantito dagli artt. 47 e 48 della Carta dei diritti fondamentali UE, escludono che una persona possa essere sanzionata in siffatte circostanze. Condividendo questo assunto iniziale – e tenuto conto della natura punitiva delle sanzioni amministrative in materia di abusi di mercato – la Corte costituzionale ha dichiarato l'illegittimità dell'art. 187-*quinquesdecies* TUF, nella parte in cui sanziona chi si sia rifiutato di rispondere alle domande di Banca d'Italia e CONSOB nell'esercizio del diritto al silenzio. Questo principio, tuttavia, non viene considerato assoluto in quanto la decisione precisa che «*il diritto al silenzio non giustifica comportamenti ostruzionistici che cagionino indebiti ritardi allo svolgimento dell'attività di vigilanza della CONSOB, come il rifiuto di presentarsi a un'audizione prevista da tali autorità, ovvero manovre dilatorie miranti a rinviare lo svolgimento dell'audizione stessa. Né il diritto al silenzio potrebbe legittimare l'omessa consegna di dati, documenti, registrazioni preesistenti alla richiesta della CONSOB*»[168].

2 L'attività di *detection* finalizzata alla individuazione di potenziali casi di abuso di mercato: le cosiddette analisi preliminari

La CONSOB ha adottato un assetto organizzativo fondato su divisioni operative, ciascuna delle quali è responsabile di specifiche aree di intervento. In tale

164 Corte cost., sentenza 21 marzo 2019, n. 63. Sul punto si rinvia ai commenti di Provenzano, P. (2020), Illecito amministrativo e retroattività '*in bonam partem*': da eccezione alla regola a regola generale, in *Banca borsa tit. cred.*, n. 1, pp. 52 ss., e Tiganò, V. (2020), L'estensione del principio costituzionale della retroattività favorevole in materia penale alle sanzioni amministrative punitive contro gli abusi di mercato, in *ivi*, pp. 62 ss.

165 Corte cost., ordinanza 10 maggio 2019, n. 117. Su questa ordinanza si rinvia al commento di Fares, G. (2020), Diritto al silenzio, soluzioni interpretative e controlimiti: la Corte costituzionale chiama in causa la Corte di giustizia, in *dirittifondamentali.it*, n. 1, pp. 57 ss.

166 Corte di giustizia UE, sentenza del 2 febbraio 2021, *DB c. CONSOB, C-481/19*, EU:C:2021:84. Si veda il commento di Coduti, D. (2021), Il diritto al silenzio nell'intreccio tra diritto nazionale, sovranazionale e internazionale: il caso D.B. c. CONSOB, in *federalismi.it*, n. 22, pp. 121 ss.

167 Corte di Cassazione civile, Sez. II, ordinanza 16 febbraio 2018, n. 3831, con nota di Gatta, G.L. (2018), "Nemo tenetur se detegere" e procedimento amministrativo davanti alla CONSOB per l'accertamento dell'abuso di informazioni privilegiate: la Cassazione solleva questione di legittimità costituzionale dell'art. 187-quinquiesdecies T.U.F., in *Dir. pen. cont.* (*dirittopenalecontemporaneo.it*).

168 Corte cost., sentenza 30 aprile 2021, n. 84. Michetti, M. (2021), Diritto al silenzio e *insider trading*: il confronto tra Roma e Lussemburgo prosegue sulla via del dialogo (Corte costituzionale, sentenza n. 84/2021), in *Consulta online* (*giurcost.org*), n. 3, pp. 758 ss., e Catalano, S. (2021), La vicenda decisa dalla sentenza n. 84 del 2021 della Corte costituzionale: un esempio di "buon dialogo" fra Corti, in *Forum di Quad. cost.* (*forumcostituzionale.it*), n. 4, pp. 295 ss.

contesto, le attività di prevenzione e rilevazione delle condotte riconducibili agli abusi di mercato sono attribuite alla Divisione Mercati, nell'ambito del più ampio mandato volto a garantire la trasparenza, il regolare svolgimento delle negoziazioni e l'integrità complessiva del mercato. La vigilanza si estende alle infrastrutture di mercato, sia di *trading* sia di *post-trading*, ai soggetti che le gestiscono, alla trasparenza delle informazioni diffuse al pubblico e al rispetto della disciplina in materia di abusi di mercato, nonché alla regolarità degli scambi.

In estrema sintesi, relativamente alle infrastrutture di mercato, l'attività di vigilanza operativa è rivolta ai meccanismi di gestione delle volatilità, alle condizioni di accesso agli scambi, ai partecipanti ai mercati e ai *liquidity providers*, nonché alle misure e ai presidi adottati per mitigare i rischi collegati alla resilienza operativa e alla sicurezza informatica. La vigilanza sulle informazioni di mercato riguarda sia la diffusione di informazioni da parte degli emittenti o da altri soggetti, sia gli studi e le raccomandazioni di investimento diffuse da dagli intermediari, sia i giudizi contenuti nelle *rating action* diffusi dalle agenzie di *rating* concernenti società italiane con titoli quotati o negoziati su MTF o il debito sovrano italiano.

Uno specifico Ufficio è incaricato di vigilare sulla regolarità dell'andamento dei mercati *cash* e derivati e sul loro contesto informativo, di gestire e analizzare i dati degli ordini e delle operazioni concluse sui mercati così come i dati rivenienti dal flusso di *transaction reporting* che includono sia le operazioni concluse sulle *trading venue* (mercati regolamentati e piattaforme multilaterali di negoziazione) sottoposte alla vigilanza della CONSOB sia i dati delle operazioni concluse fuori mercato sugli strumenti finanziari per i quali la stessa CONSOB sia l'autorità competente[169]. Il medesimo Ufficio gestisce le istruttorie preliminari su ipotesi di abusi di mercato. Obiettivo di tale attività operativa è la protezione del corretto meccanismo di determinazione dei prezzi degli strumenti finanziari, dunque dell'efficienza e integrità dei mercati.

L'attività di monitoraggio viene svolta sia in tempo reale sia in fase *ex post* (detta anche in differita), attraverso l'analisi di volumi rilevanti di dati relativi – come sopra indicato – sia agli ordini immessi sia ai contratti conclusi sui mercati, con attenzione costante all'evoluzione del contesto informativo. La vigilanza in tempo reale si fonda su una pluralità di fattori, selezionati in funzione delle specifiche circostanze e del mutare delle condizioni di mercato. Tra le variabili analizzate, a titolo esemplificativo, rientrano l'andamento dei prezzi degli strumenti finanziari, la dinamica dei *book* di negoziazione, le aste di volatilità, le posizioni *long* e *short*, l'individuazione di strategie di *trading* potenzialmente anomale, nonché l'analisi delle *quote di mercato* e dei principali risultati economici ottenuti dagli operatori. Una quota significativa delle attività di negoziazione è inoltre riconducibile a imprese di investimento che

169 Il *transaction reporting* previsto dalla MiFID II è disciplinato principalmente dall'Art. 26 del Regolamento (UE) n. 600/2014, noto come MiFIR (Markets in Financial Instruments Regulation), che richiede alle imprese di investimento di segnalare i dettagli delle transazioni alle autorità competenti. Le informazioni da riportare comprendono l'identificazione delle controparti, i dettagli del prezzo, il volume delle transazioni, il tipo di operazione e l'identificazione degli strumenti finanziari. I requisiti tecnici per il *transaction reporting*, compresi i dettagli su quali informazioni devono essere incluse nei report e le modalità di trasmissione, sono disciplinati dal Regolamento Delegato (UE) 2017/590.

adottano modelli di *trading algoritmico*, inclusi quelli ad *alta frequenza*, e/o che svolgono funzioni di *market making*.

La vigilanza *ex post* è finalizzata principalmente alla comprensione di dinamiche osservate in tempo reale, che plasticamente in un orizzonte temporale più ampio possono acquisire maggiore interesse, anche ai fini della *detection* di potenziali condotte di abusi di mercato. Una delle caratteristiche principali di tale tipo di attività è quello di essere *event driven*, sebbene non in via esclusiva. In altri termini l'analisi in differita scatta tutte le volte che si verificano impatti sul prezzo degli strumenti finanziari non spiegati dal contesto informativo; ovviamente questo tipo di analisi può trarre origine anche da altri tipi di input, ad esempio sia da *alert* generati giornalmente dai sistemi di vigilanza dell'Istituto che raccolgono, classificano ed elaborano il flusso di dati relativi agli ordini e alle transazioni, fornite quest'ultime dagli intermediari e dalle autorità estere nell'ambito del *transaction reporting*.

All'attività di *detection* di condotte potenzialmente anomale contribuiscono, oltre agli approfondimenti autonomamente condotti, anche l'analisi degli esposti qualificati presentati dagli investitori, gli input provenienti dall'autorità giudiziaria e, in misura preponderante, l'esame delle segnalazioni di ordini e operazioni sospetti (cosiddette STORs) trasmesse alla CONSOB dai soggetti obbligati ai sensi dell'art. 16, parr. 1 e 2, del Regolamento MAR, tramite l'apposita procedura *on-line*. In tale ambito, l'Ufficio è altresì competente a verificare l'efficacia e la proporzionalità dei presìdi adottati dagli intermediari e dagli operatori di mercato per l'adempimento degli obblighi di segnalazione delle STORs.

Le attività di vigilanza finalizzate alla individuazione di potenziali casi di abuso di mercato, definite 'analisi preliminari', sono condotte per gli aspetti di rispettiva competenza dagli uffici preposti e sono dirette a selezionare i casi in relazione ai quali sia appropriato dare luogo all'avvio di un'indagine finalizzata all'apprensione materiale dei fatti dai quali possono scaturire elementi di prova della commissione dell'illecito che rendono necessario, in forza del principio di doverosità, l'esercizio del potere sanzionatorio.

L'avvio del procedimento sanzionatorio avviene, quindi, all'esito della fase di accertamento, attraverso la quale la CONSOB esercita un'attività a carattere tecnico-discrezionale, volta a colmare lo iato, dovuto alla opinabilità degli esiti connessi alla valutazione del fatto alla sua eventuale riconducibilità nella fattispecie normativa[170]. Qualora dalle analisi preliminari gli uffici rilevino la sussistenza di condotte potenzialmente integranti fattispecie di abuso di mercato, il Responsabile della Divisione dispone l'avvio di un'indagine e il caso viene trasmesso a un diverso Ufficio specificamente incaricato di svolgere indagini approfondite. Qualora dalle analisi preliminari emergano condotte potenzialmente riconducibili a ipotesi di abuso di mercato, il Responsabile della Divisione dispone formalmente l'avvio di un'indagine, affidando il caso a un Ufficio distinto, specificamente incaricato di svolgere approfondite attività istruttorie. Se, all'esito di tale fase di vigilanza approfondita,

170 Fratini, M. (2012), Articolo 195, in Fratini M., Gasparri M., a cura di, Il testo unico della finanza, *UTET*, Torino, pp. 2657 ss.

emergono elementi di prova idonei a sostenere l'ipotesi di illecito, viene avviato il procedimento sanzionatorio, assicurando al destinatario della contestazione il pieno esercizio del diritto di difesa. Come noto, il procedimento sanzionatorio può assumere natura amministrativa – con attivazione dell'Ufficio Sanzioni Amministrative – e/o penale, mediante l'inoltro di una segnalazione all'Autorità Giudiziaria competente.

La fase delle analisi preliminari si svolge senza l'instaurazione del contraddittorio con il presunto autore della violazione, in conformità all'art. 13 della legge 24 novembre 1981 n. 689. Per controbilanciare questa mancanza, la legge generale sulle sanzioni prevede una limitazione rigida del periodo intercorrente fra l'accertamento e la contestazione (90 giorni), onde evitare che il ritardo nell'instaurazione del contraddittorio possa pregiudicare l'esercizio del diritto di difesa.

In ordine alla definizione del momento di conclusione della fase di accertamento e, dunque, della durata della preistruttoria, la Corte di Cassazione è costante nell'affermare che «*il momento dell'accertamento, dal quale decorre il termine di decadenza per la contestazione, non coincide necessariamente e automaticamente né col termine dell'attività ispettiva né con la data di deposito della relazione né con quella in cui la Commissione si è riunita per prenderla in esame, poiché la pura 'constatazione' dei fatti non coincide necessariamente con l''accertamento'*»[171].

In sede di revisione del regolamento sul procedimento sanzionatorio, la CONSOB ha sostenuto che l'indeterminabilità *ex ante* della durata della fase di accertamento e l'impossibilità di standardizzare le attività precedenti alla contestazione degli addebiti fossero di ostacolo all'adozione di una regolamentazione analitica[172]. La recente giurisprudenza della Corte di Cassazione[173] ha ritenuto che, nel giudizio di opposizione alle sanzioni amministrative previste dal TUF, il giudice, chiamato a pronunciarsi sulla tempestività della contestazione dell'illecito e, quindi, sulla individuazione del momento in cui il medesimo è stato o poteva essere accertato, ha la possibilità di sindacare la necessità o l'opportunità della protrazione dell'attività istruttoria da parte dell'Amministrazione e, dunque, di apprezzare la irragionevolezza della prosecuzione di una istruttoria inutile o divagante. Il sindacato sulle scelte istruttorie dell'Amministrazione deve comunque: a) essere svolto *ex ante*, ossia prendendo in considerazione l'utilità potenziale delle ulteriori iniziative istruttorie e non i concreti esiti che tali iniziative abbiano effettivamente prodotto; b) tener conto dell'interesse dell'Amministrazione a pervenire all'accertamento complessivo di tutti gli aspetti di vicende che possono essere anche molto complesse e svilupparsi in periodi temporali non brevi, che va salvaguardato dal rischio che l'efficacia delle indagini dell'Autorità di vigilanza venga posta a repentaglio da una *discovery* prematura.

171 Così Cass. civ., Sez. II, Sentenza, 16 aprile 2018, n. 9254; cfr. *ex multis* Cass. Civ., Sez. Un., 09 marzo 2007, n. 5395; Cass. civ., Sez. II, 06 febbraio 2009, n. 3043; Cass. civ., Sez. II, Sentenza, 02 dicembre 2011, n. 25836; Cass. civ., Sez. II, Sentenza, 08 agosto 2019, n. 21171; Cass. civ., Sez. II, Sentenza, 19 febbraio 2019, n. 4820.

172 Esiti della consultazione del 29 maggio 2015, Modifiche al regolamento sul procedimento sanzionatorio della CONSOB.

173 Cass. civ., Sez. II, Sent., 31 maggio 2022, n. 17673.

3 I *proof of concept* sviluppati dalla CONSOB a supporto della *detection* sugli abusi di mercato

Proprio nella fase delle analisi preliminari che caratterizza la vigilanza sulle contrattazioni al fine di individuare possibili casi di abusi di mercato, la CONSOB ha avviato una delle prime sperimentazioni dell'utilizzo di sistemi di intelligenza artificiale, ideando alcuni *proof of concept* (PoC). Si tratta di sperimentazioni ideate in collaborazione con la Scuola Normale Superiore di Pisa per la progettazione e realizzazione di strumenti di intelligenza artificiale da poter implementare nell'attività di vigilanza – fortemente *data driven*, dunque, basata sull'analisi di volumi di dati particolarmente rilevante – finalizzata alla *detection* di posizioni riconducibili a investitori per i quali il sospetto che abbiano realizzato condotte illecite è particolarmente elevato. Si sottolinea che tali strumenti affiancano, supportano e corroborano il controllo umano, ma non lo sostituiscono. Nel Capitolo I, paragrafo 4, si è già avuto modo di mettere in evidenza come la sorveglianza umana può essere declinata attraverso un modello che preveda l'essere umano nel ciclo decisionale (*human-in-the-loop* - HITL), l'essere umano 'sopra' al ciclo decisionale (*human-on-the-loop* - HOTL), ovvero l'essere umano al comando (*human-in-command* - HIC).

Il primo, HITL, indica un modello in cui l'essere umano è parte integrante del processo decisionale: l'IA fornisce output o suggerimenti, ma è l'essere umano a prendere la decisione finale o a validarla prima che venga attuata. Il secondo, HOTL, rappresenta un modello a controllo umano sovraordinato, nel quale l'essere umano mantiene una funzione di supervisione esterna, intervenendo a posteriori o in presenza di anomalie, senza partecipare attivamente a ogni singola decisione responsabilità decisionali, anche nei casi in cui l'operatività quotidiana sia fortemente automatizzata[174]. Il terzo modello, HIC, è complementare ai primi due e introduce una prospettiva più ampia sul ruolo dell'essere umano rispetto ai sistemi di IA, volto a garantire che l'intero ciclo di vita del sistema – dalla progettazione all'impiego, fino alla disattivazione – rimanga sottoposto alla responsabilità e alla volontà umana[175].

La distinzione assume particolare rilievo nei contesti a elevato impatto regolamentare, come quello finanziario, in cui l'adeguatezza del coinvolgimento umano rappresenta un elemento centrale per la valutazione del rischio e la conformità alle disposizioni dell'AI Act. Come osservato anche in dottrina, al fine di mitigare i timori legati all'automazione, il modello di sorveglianza HITL garantisce che i risultati forniti da un sistema di IA non siano l'unico motivo alla base del processo decisionale, poiché l'operatore umano può intervenire e modificare i criteri del sistema sino al momento

174 Le definizioni dell'*EU High Level Expert Group on AI* (AI HLEG), contribuiscono a cogliere le differenze, ponendo in evidenza come l'HITL richieda una capacità di intervento umano in ogni ciclo decisionale del sistema, mentre l'HOTL punti invece all'intervento umano attraverso la progettazione e il monitoraggio del sistema in quanto tale. High-Level Expert Group on AI (2019), Ethics Guidelines for Trustworthy AI (https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai).

175 Diversamente dai modelli HITL e HOTL, che si concentrano sulla fase operativa della decisione, il paradigma HIC mira ad assicurare la *governance* complessiva del sistema, in linea con i principi di autonomia, accountability e controllo democratico. In ambito finanziario, il modello HIC si traduce nell'adozione di meccanismi organizzativi, normativi e tecnici che attribuiscano chiaramente le responsabilità decisionali, anche nei casi in cui l'operatività quotidiana sia fortemente automatizzata.

della decisione finale[176]. In questo modo, il modello HITL «*has increasingly become a standard solution for solving the issues of transparency, bias, legal security and systemic risks relating to automation*»[177]. Alla luce di ciò, sembra opportuno rilevare che nelle sperimentazioni condotte dalla CONSOB è stato privilegiato il modello HITL, con una tendenza evolutiva alla definizione di un quadro di *governance* complessiva dei sistemi di IA, che conduce all'integrazione di modelli di tipo modello HIC.

Sia concesso un ulteriore chiarimento. Nel presente lavoro, il PoC identifica uno studio funzionale a dimostrare la fattibilità tecnica di un'idea o tecnologia in modo limitato e sperimentale, senza coinvolgere dati e/o utenti reali. In caso di esito positivo, segue un progetto pilota, che rappresenta una sperimentazione in scala ridotta di una soluzione già funzionante, testata in un contesto operativo reale, con l'obiettivo di valutarne l'efficacia prima dell'adozione su larga scala. In sintesi, il PoC verifica *se si può fare*, mentre il progetto pilota verifica *se funziona davvero* nel mondo reale.

In particolare, sono stati elaborati tre *proof of concept* nell'ambito dell'attività di vigilanza volte alla *detection* di potenziali condotte di *market abuse* basati su metodi di IA di tipo *unsupervised machine learning* il cui funzionamento è dettagliatamente descritto rispettivamente nei Quaderni FinTech n. 11[178] e n. 12[179].

In sintesi, nel Quaderno FinTech n. 11 vengono presentati due metodi che mirano a valutare la continuità o discontinuità del comportamento degli investitori, sia in termini assoluti che relativi. Le due *proof of concept* sono state elaborate allo scopo di fornire all'operatore umano incaricato di eseguire le verifiche, un supporto nelle analisi preliminari per l'individuazione di soggetti sospettati di condotte di *insider trading*. Come descritto nel precedente paragrafo 2, la prima individuazione di posizioni sospette attiene a una fase preistruttoria, alla quale segue una fase di approfondimento e una successiva fase di indagine, essenziale sia per confermare gli esiti dell'analisi preliminare, sia per raccogliere elementi di prova in relazione alla concreta realizzazione della fattispecie di abuso di informazioni privilegiate.

176 Lazcoz Moratinos, G. (2025), Human Oversight or Monitoring in Article 14 of the Artificial Intelligence Act: a mere mandatory requirement for High-Risk Systems?, in Cotino Hueso, L. & Galetta, D.U., The European Union Artificial Intelligence Act. A Systematic Commentary, *Editoriale Scientifica,* Napoli, pp. 717-739, in particolare p. 733.

177 Enarsson, T., Enqvist, L., e Naarttijärvi, M. (2021), Approaching the human in the loop – legal perspectives on hybrid human/algorithmic decision-making in three contexts, *Information & Communications Technology Law*, vol 31, n. 1, pp. 123-153, in particolare p. 149 (https://doi.org/10.1080/13600834.2021.1958860), in italiano (traduzione nostra): «*è diventata sempre più una soluzione standard per risolvere le questioni di trasparenza, parzialità, sicurezza giuridica e rischi sistemici legati all'automazione*». Gli Autori rilevano che anche tale meccanismo presenta criticità, in quanto il ruolo che i decisori umani devono svolgere può anche essere conflittuale: da un lato, ci si aspetta che essi esercitino (o siano tenuti per legge a esercitare) un'effettiva autonomia, mantenendo il controllo delle decisioni e vigilando sulla legittimità, sulla proporzionalità, sull'accuratezza e sulla qualità delle decisioni o delle raccomandazioni generate dalla macchina (e potenzialmente dai dati sottostanti); dall'altro lato, ci si conta sul fatto che lo facciano in relazione a sistemi decisionali progettati per prendere decisioni su larga scala, confrontandosi con restrizioni sia in termini di tempo che di risorse. Inoltre, devono affrontare un contesto giuridico complesso che richiede loro di interpretare la legge e di esprimere un giudizio sensibile.

178 Mazzarisi, P. *et al.* (2022), A machine learning approach to support decision in *insider trading* detection, *CONSOB Quaderni FinTech*, n. 11 (ttps://www.consob.it/documents/1912911/1933915/FinTech_11.pdf/eebb010d-e5e8-9f75-9e77-b2a1407e418f).

179 Ravagnani, A. *et al.* (2024), Dimensionality reduction techniques to support *insider trading* detection, *CONSOB Quaderni FinTech*, n. 12 (https://www.consob.it/documents/11973/4032571/fintech12.pdf/cc892fa7-816a-0da7-d2ec-8a26e64a6499).

Il primo modello si basa su una tecnica di *clustering analysis*, denominata *k-means clustering*. In termini estremamente semplificati, il modello è stato sviluppato a partire dalla considerazione che, in corrispondenza di un evento *price sensitive*, l'analisi delle attività di *trading* nel cosiddetto *periodo sospetto* – ossia le giornate e/o le ore precedenti la diffusione pubblica dell'informazione – evidenzi inevitabilmente un certo numero di investitori in posizione premiante. Tale numero risulta naturalmente proporzionato alla liquidità dello strumento finanziario oggetto di analisi: si consideri, ad esempio, quanti investitori potrebbero aver acquistato titoli di una *blue chip* a elevata liquidità nel corso di una settimana (nell'ordine di decine di migliaia), rispetto al numero sensibilmente inferiore di investitori attivi su un titolo caratterizzato da bassi volumi di scambio (poche unità). Tuttavia, anche nell'ipotesi di un'azione altamente liquida, un'analisi retrospettiva che tenga conto sia delle abitudini individuali di *trading* di ciascun investitore, sia delle modalità operative di gruppi di investitori accomunati da comportamenti simili (*peers*), consente di interpretare in maniera più articolata le operazioni effettuate nel periodo sospetto. Tali operazioni, infatti, potranno risultare coerenti con i comportamenti pregressi del singolo investitore e/o del gruppo di riferimento (*peer group*), oppure discostarsene, evidenziando livelli di discontinuità operativa con una intensità maggiore o minore.

A titolo esemplificativo, un investitore attivo nel periodo sospetto – e dunque in posizione premiante – che tuttavia opera abitualmente su quello specifico strumento e/o settore, e che ha assunto una posizione significativa in termini assoluti ma proporzionata rispetto al proprio patrimonio complessivo, sarà considerato tendenzialmente meno sospetto. Al contrario, un investitore che abbia effettuato un'unica operazione nella giornata immediatamente precedente l'evento *price sensitive*, investendo l'intero patrimonio su uno strumento sul quale non aveva mai operato in precedenza – né su strumenti analoghi – e la cui operatività risulti difforme rispetto a quella del proprio gruppo di *peers*, sarà qualificato come fortemente discontinuo. L'analisi di tali elementi per ciascuna posizione rilevata nel periodo sospetto può certamente essere svolta da un analista umano; si tratta tuttavia di un'attività estremamente onerosa in termini di tempo, in particolare nei casi che riguardano strumenti finanziari a elevata negoziazione.

Sulla base del modello di analisi realizzato, l'algoritmo permette di identificare quei gruppi di investitori la cui attività di *trading*, in prossimità di un evento *price sensitive*, risulta non solo orientata alla realizzazione di un profitto privo di rischio, ma anche caratterizzata da una discontinuità operativa rispetto alla precedente storia di *trading* e all'operatività tipica del gruppo di appartenenza. In particolare, la *clustering analysis* modella il comportamento di *trading* di ciascun investitore sulla base di parametri quantitativi selezionati (saldo netto tra acquisti e vendite, concentrazione del *trading* ed esposizione). Elaborando questi parametri, la metodologia *k-means clustering* identifica gruppi omogenei di investitori in un determinato orizzonte temporale. Infine, l'analisi valuta l'evoluzione nel tempo della posizione di ogni investitore, distinguendo quelli che hanno modificato il proprio comportamento di *trading* in prossimità di un evento *price sensitive* (i cosiddetti investitori discontinui).

Il secondo modello si propone di individuare gruppi di investitori che operano in modo sincronizzato e con direzionalità favorevole in prossimità di un evento *price sensitive* (i cosiddetti *insider ring*). La metodologia impiegata, denominata *Statistically Validated Networks*, dopo aver caratterizzato l'attività di *trading* di ogni investitore in tre possibili stati (acquisto, vendita, acquisto-vendita), costruisce una rete di investitori che mostrano attività sincronizzata in termini di stati e tempistiche di *trading*. Partendo da una rete di investitori statisticamente validata, il modello identifica gruppi omogenei di soggetti con attività simile, che hanno operato in direzione favorevole rispetto a un evento *price sensitive*.

Il Quaderno FinTech n. 12 introduce un approccio innovativo rispetto ai due studi precedenti che utilizzano tecniche di *Unsupervised Machine Learning*, applicando una tecnica che prevede la decomposizione e successiva ricostruzione di una serie temporale di dati attraverso l'analisi delle 'componenti principali' (PCA, *Principal Component Analysis*) e l'uso di *autoencoder*, in relazione alle posizioni assunte da gruppi di investitori su un determinato titolo azionario in prossimità di un evento *price sensitive*. L'unico input richiesto dal metodo è la posizione di *trading* di ciascun investitore attivo sull'*asset* interessato dall'evento *price sensitive*. Dopo aver calcolato gli errori di ricostruzione associati ai profili di *trading*, vengono applicate diverse condizioni per identificare gli investitori il cui comportamento potrebbe risultare sospetto di *insider trading* in relazione all'evento *price sensitive*. In termini pratici, la logica seguita nella procedura di identificazione di comportamenti anomali considera la posizione media ricostruita attraverso la tecnica PCA come rappresentativa di un comportamento operativo normale. Qualsiasi deviazione significativa nell'operatività di un singolo investitore rispetto al comportamento medio ricostruito durante il periodo di osservazione (che superi una certa soglia di sensibilità) viene segnalata dall'algoritmo come anomala e potenzialmente meritevole di ulteriori indagini attraverso metodi 'tradizionali'.

L'approccio sottostante ai modelli è risultato di grande utilità e, con particolare riferimento al primo di essi sono state avviate analisi funzionali a integrarne l'utilizzo nei sistemi di vigilanza utilizzati dagli Uffici incaricati.

4 La compatibilità delle soluzioni SupTech sviluppate dalla CONSOB rispetto al quadro regolatorio in materia di IA

Come si è avuto modo di osservare, la CONSOB ha avviato lo sviluppo di diversi prototipi che integrano soluzioni di tipo SupTech. L'intelligenza artificiale può offrire contributi rilevanti all'attività di vigilanza, sia in termini di efficienza operativa che di capacità di individuazione tempestiva di potenziali abusi di mercato. Questo approccio si inserisce nel solco tracciato dall'art. 14 del d.d.l. sull'intelligenza artificiale, che disciplina l'utilizzo dell'intelligenza artificiale da parte delle pubbliche amministrazioni, delineandone finalità, limiti e presìdi organizzativi. Come già illustrato, la norma prevede che l'IA sia impiegata con funzione strumentale e di supporto, con l'obiettivo di migliorare l'efficienza amministrativa, ridurre i tempi dei procedimenti e accrescere

la qualità dei servizi offerti. L'impiego dell'IA deve garantire la conoscibilità e la tracciabilità dei sistemi, nel rispetto del principio di trasparenza. È espressamente ribadita la centralità della decisione umana: ogni provvedimento amministrativo resta nella piena responsabilità dell'agente pubblico, la cui autonomia decisionale non può essere sostituita da sistemi automatizzati. Infine, il legislatore impone alle amministrazioni l'adozione di misure tecniche, organizzative e formative per promuovere un uso responsabile dell'IA e lo sviluppo delle competenze trasversali degli operatori coinvolti.

L'esperienza maturata dalla CONSOB dimostra come l'intelligenza artificiale possa rappresentare uno strumento strategico per rafforzare risorse limitate e migliorare il processo decisionale. Tuttavia, tali benefici devono essere accompagnati da un solido impianto di regole e garanzie, in grado di bilanciare le opportunità dell'innovazione con il rispetto dei principi di legalità, trasparenza e proporzionalità. È dunque fondamentale disporre di un *framework* che consideri sia i rischi tecnici e organizzativi, sia le implicazioni per i diritti fondamentali e per il corretto esercizio dei poteri pubblici.

Alla luce dell'art. 6 e dell'Allegato III del Regolamento (UE) 2024/1689, appare plausibile ritenere, allo stato attuale[180], che i prototipi sviluppati dalla CONSOB per il supporto delle analisi volte a rilevare abusi di mercato, descritti al Capitolo III, non rientrino tra quelli ad alto rischio. Infatti, sono esclusi da tale classificazione i sistemi destinati a individuare frodi nei servizi finanziari o a fini prudenziali, così come quelli che non influenzano in modo significativo l'esito dei processi decisionali né pongono rischi per i diritti fondamentali. Anche una valutazione dal punto di vista tecnico consente di ritenere che tutte le componenti che hanno caratterizzato lo sviluppo dei prototipi (assenza di *bias* nei dati, trasparenza degli algoritmi e dello sviluppo del codice) siano prive di elementi atti a connotarne l'alto rischio.

Proprio circa il processo decisionale, è opportuno sottolineare che i prototipi di IA sperimentati dalla CONSOB sono ben lontani dal sostituire l'attività di vigilanza preordinata all'accertamento di potenziali casi di abuso di mercato. La funzione di *detection* di condotte abusive resta saldamente affidata ai funzionari, mentre i sistemi di IA si limitano ad analizzare grandi volumi di dati, contribuendo a rendere più efficiente la fase istruttoria.

In ordine alla sinergia realizzabile fra IA ed esseri umani, la dottrina distingue tra diverse forme di interazione tra IA e decisore umano: i) intelligenza assistita (*assisted intelligence*), in cui gli individui mantengono il pieno controllo dei processi decisionali; ii) intelligenza aumentata *(augmented intelligence*), in cui l'IA è in grado di fornire risposte a problemi complessi e viene sovente utilizzata nel processo istruttorio, anche per evitare errori umani; iii) intelligenza amplificata (*amplified intelligence*), in

180 La precisazione è d'obbligo poiché anche se ai sensi dell'art. art. 6 e dell'Allegato III non sono classificati come sistemi ad alto rischio quelli volti a individuare frodi nell'offerta dei servizi finanziari, ex art. 6, par. 6, resta salvo il potere della Commissione europea di adottare atti delegati al fine di modificare il par.3, 2 comma, del medesimo articolo, aggiungendo nuove condizioni a quelle stabilite, oppure modificandole, «*qualora vi siano prove concrete e affidabili dell'esistenza di sistemi di IA che rientrano nell'ambito di applicazione dell'Allegato III ma non presentano un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche*».

cui l'IA è in grado di emettere vere e proprie raccomandazioni; iv) intelligenza autonoma (*autonomous intelligence*), nella quale l'IA assume decisioni in maniera indipendente, operando in via autonoma; v) intelligenza autopoietica (*autopoietic intelligence*), in cui l'IA è in grado di espandere le sue capacità in settori diversi[181].

Nel caso di specie, i *proof of concept* sviluppati dalla CONSOB potrebbero rientrare nella categoria dell'intelligenza aumentata. Con la conseguenza che tali iniziative potrebbero essere collocate nella seconda generazione, cosiddetta diagnostica, fra quelle viste in materia SupTech (si veda Capitolo II, paragrafo 1). Questa configurazione è coerente con quanto previsto dal comma 2 dell'art. 14 del d.d.l. sull'intelligenza artificiale che prevede che l'utilizzo dell'IA nella pubblica amministrazione debba avvenire «*in funzione strumentale e di supporto all'attività provvedimentale, nel rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale*».

Una volta implementati operativamente, tali sistemi dovranno essere sottoposti a monitoraggio continuo, anche in assenza di un obbligo esplicito previsto per i sistemi ad alto rischio. Sarà essenziale garantire, lungo tutto il ciclo di vita dell'IA, il rispetto di requisiti quali affidabilità, accuratezza, robustezza, sicurezza informatica, qualità dei dati, sorveglianza umana e tutela dei diritti fondamentali, inclusa la protezione dei dati personali.

In questa prospettiva, l'adozione di atti amministrativi in grado di chiarire finalità, categorie di dati trattabili e misure di salvaguardia, conformemente a quanto previsto dagli artt. 6 e 9 del GDPR e dagli artt. 2-*ter* e 2-*sexies* del d.lgs. 196/2003 appare idonea a rafforzare i principi di trasparenza, non esclusività algoritmica e non discriminazione, sanciti anche nell'art. 14 del d.d.l. IA e peraltro ribaditi come principi ispiratori con riferimento all'utilizzo di sistemi di intelligenza artificiale nelle indagini preliminari *ex* art. 24 del d.d.l. IA.

Le riflessioni più recenti della dottrina internazionale confermano la centralità di una *governance* dell'IA ispirata ai principi dello Stato di diritto, soprattutto nel contesto della vigilanza finanziaria. È stato, infatti, condotto uno studio che 'analizza l'impiego di strumenti basati sull'IA da parte della BCE, che propone modello di *governance* basato sul rischio, in grado di adattare i presidi normativi in funzione del grado di impatto dell'IA sui diritti degli individui[182]. Questo *framework*, ispirato all'AI Act, mira a tutelare in modo proporzionato il diritto a una buona amministrazione, valorizzando la trasparenza, la conoscibilità e la responsabilità come requisiti fondamentali per l'impiego di sistemi intelligenti da parte delle autorità di vigilanza.

In questa prospettiva, l'esperienza della CONSOB si colloca in modo coerente e proattivo. La scelta di sviluppare prototipi riconducibili all'intelligenza aumentata rappresenta un primo passo concreto verso l'obiettivo di coniugare efficienza operativa

181 Abriani, N., Schneider, G. (2021), Diritto delle imprese e intelligenza artificiale, *op. cit.*, pp. 27-30.

182 Azzutti, A., Batista, P.M. e Ringe, W.-G. (2024), *Good Administration in AI-Enhanced Banking Supervision: A Risk-Based Approach*, Columbia Journal of European Law, vol. 29, n. 3, pp. 434-496 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4430642).

e tutela dei diritti. È in questa cornice che si inserisce l'impegno della CONSOB, culminato con la riforma organizzativa del 2024[183] che ha previsto, tra l'altro, l'istituzione – mediante delibera n. 23203 del 12 luglio 2024 – della Divisione Informatica e Intelligenza Artificiale (di seguito anche solo DIA), con l'obiettivo di rafforzare la capacità dell'Autorità di presidiare i processi di innovazione tecnologica e di sviluppare strumenti analitici avanzati a supporto delle funzioni istituzionali. A questa struttura sono affidati compiti cruciali per il governo delle infrastrutture digitali, la gestione dei dati e lo sviluppo delle soluzioni di IA. In particolare, tale Divisione è chiamata a progettare, realizzare e gestire sistemi informativi evoluti, anche attraverso l'integrazione di soluzioni di *machine learning*, tecniche di elaborazione automatica del linguaggio naturale e modelli predittivi applicabili ai diversi ambiti di vigilanza. Affinché le potenzialità della DIA possano tradursi in valore concreto per l'azione di vigilanza, è tuttavia essenziale disporre di un patrimonio informativo coerente, accessibile e di qualità. In questo contesto si inserisce il rafforzamento dell'Ufficio Data Governance, cui è affidata la definizione delle politiche di gestione dei dati e il presidio della loro corretta integrazione nei processi decisionali dell'Istituto. Si tratta di funzioni trasversali rispetto alle diverse Divisioni, mirate a garantire la disponibilità di dati affidabili e strutturati, condizione necessaria per alimentare modelli algoritmici, favorire l'interoperabilità dei sistemi e promuovere un approccio sistemico alla vigilanza orientato all'evidenza (*evidence-based supervision*). Tali modifiche organizzative incarnano pienamente le priorità delineate nel Piano Strategico 2024–2026, che individua nella digitalizzazione dei processi e nella valorizzazione dei dati due leve fondamentali per una vigilanza più proattiva, integrata e basata sul rischio. Il nuovo Piano Strategico 2025–2027 della CONSOB conferma e rafforza questa direzione, ponendo tra i suoi obiettivi prioritari il potenziamento della vigilanza *data-driven* e *risk-based*, l'adozione di soluzioni di intelligenza artificiale e la valorizzazione del capitale umano attraverso il reclutamento di risorse con competenze STEM e la formazione continua del personale.

Il futuro della vigilanza potenziata dall'IA passa, dunque, non solo attraverso l'adozione di tecnologie avanzate, ma soprattutto attraverso la costruzione di una cultura regolatoria in grado di governarle. Come mostrano le esperienze più autorevoli a livello europeo, l'equilibrio tra innovazione e *accountability* non è un traguardo tecnico, ma una scelta istituzionale.

183 CONSOB (2024), Piano Strategico 2025–2027, disponibile al link: https://www.consob.it/documents/d/area-pubblica/ps2527.

Conclusioni

Il lavoro è finalizzato a indagare se alla luce del quadro normativo sovranazionale e nazionale, le sperimentazioni SupTech sviluppate dalla CONSOB presentino profili di criticità.

Per rispondere alla domanda di indagine posta, nel Capitolo I, sono state analizzate le principali norme del Regolamento (UE) 2024/1689 in materia di intelligenza artificiale e del d.d.l. nazionale. In particolare, dopo aver fatto luce sui problemi definitori insiti nell'espressione 'intelligenza artificiale', sono stati descritti i contenuti del nuovo regolamento europeo e si è riflettuto sulla portata di tale intervento normativo, il quale è destinato a porre l'Unione in una posizione di *leadership* globale, secondo il cosiddetto 'effetto Bruxelles'; con riferimento al quadro normativo nazionale, d'altronde, si sono approfonditi gli spunti contenuti nel disegno di legge volto a regolamentare l'intelligenza artificiale. Infine, sono stati richiamati i principi giurisprudenziali di conoscibilità, di non esclusività della decisione algoritmica e di non discriminazione.

Prima di analizzare i *proof of concept* sperimentati dalla CONSOB, il Capitolo II è stato dedicato alla spiegazione del fenomeno SupTech, ossia della tecnologia applicata alla vigilanza. Si è fornita poi una panoramica delle principali sperimentazioni intraprese dalle Autorità di vigilanza a livello internazionale, europeo e nazionale.

Nel Capitolo III, inquadrate le fattispecie di abuso di mercato e messo a fuoco il perimetro entro il quale la CONSOB progetta d'implementare i sistemi di IA sono state svolte alcune riflessioni che possono accompagnare l'Autorità in tale processo di digitalizzazione.

L'intelligenza artificiale, se ben governata, può migliorare l'oggettività e la coerenza delle decisioni di vigilanza, riducendo la discrezionalità e rafforzando la fiducia dei cittadini. Tuttavia, l'assenza di spiegabilità e contestabilità può compromettere la legittimità delle scelte automatizzate. Per questo motivo, i sistemi che contribuiscono alla decisione finale devono essere affiancati da un controllo umano competente e informato. Le sfide principali dell'automazione nella vigilanza – imparzialità, trasparenza, responsabilità – impongono lo sviluppo di un *framework* di *AI governance* fondato su tre pilastri: (i) promozione della cultura digitale a tutti i livelli dell'organizzazione; (ii) sostegno all'innovazione, anche attraverso collaborazioni con il mondo accademico e sperimentazioni controllate; (iii) mappatura sistematica dei rischi legati all'uso dell'IA, incluse le possibili derive opache o discriminatorie.

Queste iniziative rappresentano un investimento strategico nella capacità dell'Autorità di coniugare innovazione e affidabilità, ponendo le basi per una vigilanza tecnologicamente avanzata, ma saldamente ancorata ai principi dello Stato di diritto.

Bibliografia

Abriani, N., & Schneider, G. (2021). Diritto delle imprese e intelligenza artificiale. *Bologna: Il Mulino*.

AGCOM (2018). Interim Report indagine conoscitiva del. 309/16/CONS, News vs. Fake nel sistema dell'informazione. Tratto da https://www.agcom.it/sites/default/files/migration/attachment/Allegato%2022-11-2018_0.pdf

AgID (2023). Piano Triennale per l'informatica nella pubblica amministrazione 2024-2026. Tratto da https://www.agid.gov.it/sites/agid/files/2024-06/piano_triennale_per_linformatica_nella_pa_2024-2026.pdf

Allena, M., Vaccari, S. (2022). Diritto al silenzio e autorità di vigilanza dei mercati finanziari. *Riv. dir. banc.* (rivista.dirittobancario.it), n. 3, 689 ss.

AMF (2024). Vérifications à faire concernant votre intermédiaire financier. Tratto da https://www.amf-france.org/fr

Amorosino, S. (2004). Tipologie e funzioni delle vigilanze pubbliche sulle attività economiche. *Diritto amministrativo*, n. 4, 723 ss.

Arena, G. (2008). Le diverse finalità della trasparenza amministrativa. In F. Merloni (A cura di), La trasparenza amministrativa (p. 29 ss.). *Milano: Giuffrè Editore*.

Arenilla Sáez, M. (2021). La administración digital: los riesgos de la desintermediación, las escisiones y las centralizaciones. *Madrid: Instituto Nacional de Administración Pública*.

Armiento, M. (2023). Prove di regolazione dell'intelligenza artificiale: il Regolamento della Banca d'Italia sulla gestione degli esposti. *Giornale di diritto amministrativo* (1), 105-115.

ASIC (2022). Speech by Chair Joseph Longo at the Corporate Counsel Association's Executive Committee webinar, 25 maggio. Tratto da https://asic.gov.au/about-asic/news-centre/speeches/chair-s-remarks-at-corporate-counsel-association-event/

Avanzini, G. (2022). Intelligenza artificiale e nuovi modelli di vigilanza pubblica in Francia e Olanda. *Giornale di diritto amministrativo*, 316 ss.

Azzutti, A., Batista, P., Ringe, W.-G. (2024). Good Administration in AI-Enhanced Banking Supervision: A Risk-Based Approach. *Columbia Journal of European Law*, 29(3), 434-496.

BaFin (2022). Machine learning in risk models. Tratto da https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2022/fa_bj_2202_Maschinelles_Lernen_en.html

Banca d'Italia (2022). Relazione sugli esposti dei clienti delle banche e delle finanziarie-anno 2021. Tratto da https://www.bancaditalia.it/pubblicazioni/relazione-esposti/2022/relazione-sugli-esposti-sul-2021.pdf

Basel Committee on Banking Supervision (2017). Consultative Document, Sound Practices: Implications of fintech developments for banks and bank supervisors. Tratto da https://www.bis.org/bcbs/publ/d415.htm

Bauguess, S. (2017). The Role of Big Data, Machine Learning, and AI in Assessing Risks: a Regulatory Perspective, 21 giugno. Tratto da https://www.sec.gov/newsroom/speeches-statements/bauguess-big-data-ai

Berto, L. (2025). Il parere della Commissione Giustizia del Senato sul disegno di legge sull'intelligenza artificiale. Diritto e Giustizia, *Il quotidiano dell'Informazione Giuridica*.

Berto, L. (2025). Il Senato approva il disegno di legge sull'intelligenza artificiale. Diritto e Giustizia, *Il quotidiano dell'Informazione Giuridica*.

Bindi, E., Pisaneschi, A. (2019). La retroattività in mitius delle sanzioni amministrative Consob. *Giur. comm.*, n. 5, 1015 ss.

Bistolfi, C., Bolognini, L., Pelino, E. (2016). Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali. *Milano: Giuffrè*.

Bonaccorsi di Patti, E., Calabresi, F., De Varti, B., Federico, F., Affinito, M., Antolini, M., Rinna, G. (2022). Intelligenza artificiale nel credit scoring. Analisi di alcune esperienze nel sistema finanziario italiano. *Banca d'Italia Occasional Papers*, n. 721.

Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review*, 107(1), 2-64.

Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World (online edn, Oxford Academic, 2019 ed.). *New York: Oxford University Press*. doi:https://doi.org/10.1093/oso/9780190088583.001.0001

Buono, G., Bonanni, P., Del Mondo, G., Ciriello, A. (2022). Rapporto 4/2022 – Intelligenza artificiale e amministrazioni centrali. *BioLaw Journal* (1), 261 ss.

Camilli, E.L., Clarich, M. (2007). Il procedimento sanzionatorio della CONSOB sotto il riflettore della Corte di Cassazione, nota a: *Cassazione civile*, sez. un., 09 marzo 2007, n. 5395. Giur. comm., fasc. 6, 1158 ss.

Caneschi, G. (2020). Nemo tenetur se detegere anche nei procedimenti amministrativi sanzionatori? La parola alla Corte di giustizia. *Cass. Pen.*, n. 2, 579 ss.

Cariello, P., De Simoni, M., Iezzi, S. (2024). A machine learning approach for the detection of firms linked to organised crime in Italy, based on balance sheet data. *Banca d'Italia Quaderni dell'antiriciclaggio*, n. 22.

Carini, V. (2024). Authority UE e Borse: così l'IA è alleata contro gli abusi. *Il Sole 24 Ore*, 20 marzo, p. 46.

Carloni, E. (2021). Qualità dei dati, big data e amministrazione pubblica. In R. Cavallo Perin (A cura di), L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale. *Quaderni del dipartimento di giurisprudenza dell'Università di Torino,* Vol. 20, p. 118 ss.

Carloni, E. (2022). Le intelligenze artificiali nella pubblica amministrazione e la sfida della trasparenza. In A. Lalli (A cura di), L'amministrazione pubblica nell'era digitale (p. 45 ss.). *Torino: G. Giappichelli*.

Carullo, G. (2021). Decisione amministrativa e intelligenza artificiale. *Il diritto dell'informazione e dell'informatica*, n. 3, 431 ss.

Cassese, S. (2002). La signoria comunitaria sul diritto amministrativo. *Rivista italiana di diritto pubblico comunitario*, p. 291.

Catalano, S. (2021). La vicenda decisa dalla sentenza n. 84 del 2021 della Corte costituzionale: un esempio di "buon dialogo" fra Corti. *Forum di Quad. cost.* (forumcostituzionale.it), n. 4, 295 ss.

Cavallo Perin, R. (2020). Ragionando come se la digitalizzazione fosse data. *Diritto amministrativo*, 305 ss.

Chieppa, R., Giovagnoli, R. (2021). Manuale di diritto amministrativo. *Milano: Giuffrè*.

Chiti, E., Marchetti, B., Rangone, N. (2021). Rapporto 1/2021, L'impiego dell'intelligenza artificiale nell'attività di CONSOB, AGCOM e ARERA. *BioLaw Journal*, n. 4/2021, 211 ss.

Ciocca, P. (2021). Audizione della CONSOB alla Camera dei Deputati, VI Commissione permanente (Finanze), sul "Pacchetto sulla finanza digitale". *CONSOB*. Tratto da https://www.consob.it/documents/1912911/1953802/Audizione_Ciocca_20210608.pdf/56379b1b-ef44-a27c-91fd-5c24274236bc

Clarich, M. (2022). Manuale di diritto amministrativo. *Bologna: Il Mulino*.

Coduti, D. (2021). Il diritto al silenzio nell'intreccio tra diritto nazionale, sovranazionale e internazionale: il caso D.B. c. Consob. *federalismi.it*, n. 22, 121 ss.

Commissione europea (2020). Comunicazione relativa a una strategia in materia di finanza digitale per l'UE. Tratto da https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0591:FIN:IT:PDF

Commissione europea (2021). Study on the Relevance and Impact of Artificial Intelligence for Company Law and Corporate Governance. Tratto da https://op.europa.eu/en/publication-detail/-/publication/13e6a212-6181-11ec-9c6c-01aa75ed71a1/language-en

Commissione europea (2022). Commission Staff Working Document on Common European Data Spaces. Tratto da https://data.consilium.europa.eu/doc/document/ST-6532-2022-INIT/en/pdf

Conigliaro, M. (2022). Lotta all'evasione con l'intelligenza artificiale "Ve.R.A.". *Il fisco*, n. 32-33, 3107 ss.

CONSOB (2023). Piano Strategico 2022-2024. Tratto da https://www.consob.it/web/area-pubblica/piano-strategico

CONSOB (2024). Relazione per l'anno 2023. Tratto da https://www.consob.it/documents/11973/4329955/dsc2024.pdf/292d6b12-0f4a-3fff-71f3-8ca3722ca5a6

CONSOB (2025). Incontro annuale con il mercato finanziario. Discorso del Presidente Prof. Paolo Savona, Milano. Tratto da https://www.consob.it/documents/d/area-pubblica/dsc2025

Consulich, F., Maugeri, M., Milia, C., Poli, T.N., Trovatore, G. (2023). AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie. *CONSOB Quaderni giuridici*, n. 29, maggio.

Consulich, F. (2018). Il prisma del ne bis in idem nelle mani del Giudice eurounitario. *Dir. pen. proc.*, n. 7, 949 ss.

Corte dei conti europea (2024). Relazione speciale 08/2024. Le ambizioni dell'UE in materia di intelligenza artificiale. Tratto da https://www.eca.europa.eu/ECAPublications/SR-2024-08/SR-2024-08_IT.pdf

Costantino, F. (2019). Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data. *Diritto pubblico*, 44 ss.

Daidone, A., Police, A. (2013). Il conflitto in tema di giurisdizione sulle sanzioni della Consob ed i limiti della Corte costituzionale come giudice del riparto. *Giurisprudenza italiana*, 687 ss.

Del Gatto, S. (2020). Potere algoritmico, digital welfare state e garanzie per gli amministrati. I nodi ancora da sciogliere. *Rivista italiana di diritto pubblico comunitario*, n. 6 , 829 ss.

Deodato, C. (2019). Sanzioni formalmente amministrative e sostanzialmente penali: i problemi procedurali connessi all'applicazione delle sanzioni Consob in materia di materia di market abuse (e alcune soluzioni). *Federalismi.it*, n. 23, 28 ss.

Di Castri, S., Hohl, S., Kulenkampff, A., Prenio, J. (2019). The suptech generations. FSI Insights on policy implementation. Tratto da https://www.bis.org/fsi/publ/insights19.pdf

Drezner, D. (2008). All Politics Is Global: Explaining International Regulatory Regimes. *Princeton: Princeton University Press*.

Enarsson, T., Enqvist, L., Naarttijärvi, M. (2021). Approaching the human in the loop – legal perspectives on hybrid human/algorithmic decision-making in three contexts. *Information & Communications Technology Law*, 31(1), 123-153.

Falcone, M. (2023). Ripensare il potere conoscitivo pubblico tra algoritmi e Big data. *Napoli: Editoriale Scientifica*.

Fares, G. (2020). Diritto al silenzio, soluzioni interpretative e controlimiti: la Corte costituzionale chiama in causa la Corte di giustizia. *dirittifondamentali.it*, n. 1, 57 ss.

FCA (2022, 06 23). Data Strategy Update 2022. Tratto da https://www.fca.org.uk/publications/corporate-documents/data-strategy-update-2022

FCA (2024). Artificial Intelligence (AI) update – further to the Government's response to the AI White Paper Corporate. Tratto da https://www.fca.org.uk/publications/corporate-documents/artificial-intelligence-ai-update-further-governments-response-ai-white-paper

Filippucci, F., Gal, P., Jona-Lasinio, C., Leandro, A., Nicoletti, G. (2024). The Impact of Artificial Intelligence on Productivity, Distribution and Growth: Key Mechanisms, Initial Evidence and Policy Challenges. *OECD Artificial Intelligence Papers*(15), aprile.

Finocchiaro, G. (2022). La regolazione dell'intelligenza artificiale. *Rivista trimestrale di diritto pubblico*, n. 4, 1085 ss.

Finocchiaro, G. (2024). Intelligenza artificiale. Quali regole? *Bologna: Il Mulino*.

Flick, G., Napoleoni, V. (2014). Cumulo tra sanzioni penali e amministrative: doppio binario o binario morto? "Materia penale", giusto processo e ne bis in idem nella sentenza della Corte Edu, 4 marzo 2014, sul market abuse. *Rivista AIC*, n. 3.

Floridi, L. (2021). The European Legislation on AI: a Brief Analysis of its Philosophical Approach. Tratto da SSRN: https://ssrn.com/abstract=3873273

Foà, S. (2023). Intelligenza artificiale e cultura della trasparenza amministrativa. Dalle "scatole nere" alla "casa di vetro"? *Diritto amministrativo*, n. 3, 515 ss.

Franca, S. (2022). Il trattamento dei dati nelle sperimentazioni di intelligenza artificiale riguardanti le pubbliche amministrazioni. In A. Pajno, F. Donati, A. Perrucci (A cura di), Intelligenza artificiale e diritto: una rivoluzione? Vol. 2. Amministrazione, responsabilità, giurisdizione (p. 155-186). *Bologna: Il Mulino*.

Fratini, M. (2012). Articolo 195. In M. Fratini, & G. Gasparri (A cura di), Testo unico della finanza (p. 2657 ss.). *Torino: UTET*.

Fredda, R. (2023, 12 11). Analisi e proposte normative nella nuova dimensione del capital market. *CERIDAP*(4), 218-237. doi:10.13130/2723-9195/2023-4-28

FSB (2020). The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions. Tratto da https://www.fsb.org/wp-content/uploads/P091020.pdf

Galetta, D.U. (2020). Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia. *Rivista Italiana di Diritto Pubblico Comunitario*, fasc.3, 501.

Galetta, D., Corvalàn, J. (2019). Intelligenza artificiale per una pubblica amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto. *Federalismi.it*.

Gamero Casado, E. (2021). El enfoque europeo de inteligencia artificial. *Revista de Derecho Administrativo – CDA*(20), 268-289.

Gatta, G. (2018). "Nemo tenetur se detegere" e procedimento amministrativo davanti alla Consob per l'accertamento dell'abuso di informazioni privilegiate: la Cassazione solleva questione di legittimità costituzionale dell'art. 187-quinquiesdecies T.U.F. *Dir. pen. cont.* (dirittopenalecontemporaneo.it).

Genovese, A. (2017). Il controllo del giudice sulla regolazione finanziaria. *Banca borsa tit. cred.*, n. 1, 49 ss.

High-Level Expert Group on AI - AI HLEG (2019). Ethics Guidelines for Trustworthy AI. 8 aprile.

Kaminski, M.E. (2023). Regulating the risk of AI. U of Colorado Law Legal Studies Research Paper No. 22-21, 1347-1411. Tratto da Colorado Law - University of Colorado Boulder: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4195066

IVASS (2024). Relazione sull'attività svolta dall'Istituto nell'anno 2023.

Lalli, A. (2024). La regolazione pubblica delle tecnologie digitali e dell'intelligenza artificiale. *Torino: G. Giappichelli*.

Lazcoz Moratinos, G. (2025). Human Oversight or Monitoring in Article 14 of the Artificial Intelligence Act: a mere mandatory requirement for High-Risk Systems? In L. Cotino Hueso, & D.-U. Galetta (A cura di), The European Union Artificial Intelligence Act. A Systematic Commentary (p. 717-739). *Napoli: Editoriale Scientifica*.

Lembo, D., Limosani, A., Medda, F., Monaco, A., & Scafoglieri, F. (2022). Information Extraction through AI techniques: The KIDs use case at CONSOB. arXiv, 1-4. doi:https://doi.org/10.48550/arXiv.2202.01178

Linciano, N., Caivano, V., Costa, D., Soccorso, P., Poli, T., Trovatore, G. (2022, giugno). L'intelligenza artificiale nell'asset e nel wealth management. *CONSOB Quaderni FinTech*, n. 9.

Lo Sapio, G. (2021). La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione. *Federalismi.it* (16), 114 ss.

Lo Sapio, G. (2022). Intelligenza artificiale: rischi, modelli regolatori, metafore. *Federalismi.it, Federalismi*(27), 232-258.

Logli, A. (2020). Poteri istruttori della Consob e nemo tenetur se detegere. *Giurisprudenza commerciale*, 230 ss.

Macchia, M. (2023). Il Digital Finance Package e l'elogio della regolazione. In V. Felice, Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato (p. 197 ss.). *Torino: G. Giappichelli Editore*, 2023.

Marchetti, B. (2021). The algorithmic administrative decision and the human in the loop. *BioLaw Journal*, n. 2, 381 ss.

MAS (2023). Written reply to Parliamentary Question on use of artificial intelligence in supervision of financial institutions, for Parliament Sitting on 3 October 2023. Tratto da https://www.mas.gov.sg/news/parliamentary-replies/2023/written-reply-to-parliamentary-question-on-use-of-artificial-intelligence-in-supervision-of-fis

MAS (2024). Annual Report 2023/2024 Media Conference on 18 July 2024. Tratto da https://www.mas.gov.sg/news/speeches/2024/mas-annual-report-media-conference-2023-2024

Mazzarisi, P., Ravagnani, A., Deriu, P., Lillo, F., Medda, F., Russo, A. (2022). A machine learning approach to support decision in insider trading detection. *CONSOB Quaderni FinTech*, 11.

McCarthy, J., Minsky, M., Rochester, N. (1955). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence . In *AI Magazine*, 2006, vol. XXVII.

Michetti, M. (2021). Diritto al silenzio e insider trading: il confronto tra Roma e Lussemburgo prosegue sulla via del dialogo (Corte costituzionale, sentenza n. 84/2021). Consulta online (giurcost.org), n. 3, 758 ss.

Mir, O. (2024). The AI Act from the Perspective of Administrative, Law: Much Ado About Nothing? *European Journal of Risk Regulation*, 1-13. doi:10.1017/err.2024.54

Montalenti, P. (2015). Abusi di mercato e procedimento Consob: il caso Grande Stevens e la Sentenza CEDU. *Giur. comm.*, n. 3, 478 ss.

Morrone, A. (2008). (voce) Bilanciamento (giustizia costituzionale). Enciclopedia del Diritto - Annali dal 2007, II.II, 185-204. *Milano: Giuffrè*.

Napoli, C. (2020). Algoritmi, intelligenza artificiale e formazione della volontà pubblica: la decisione amministrativa e quella giudiziaria. *Riv. AIC*(3), 318 ss.

Neves, A. (2023). A necessidade de reescrever o direito administrativo. In Estudos em homenagem ao Professor Doutor Fernando Alves Correia (p. 555-592). *Coimbra: Almedina*.

OECD (2019). Recommendation of the council on artificial intelligence. *Paris: OECD Publishing*.

OECD (2021). Business and Finance Outlook 2021: AI in Business and Finance. *Paris: OECD Publishing*. Tratto da https://doi.org/10.1787/ba682899-en

Pagella, C. (2020). L'inafferrabile concetto di "connessione sostanziale e temporale sufficientemente stretta": la Cassazione ancora sul ne bis in idem e insider trading. *Sistema penale* (sistemapenale.it).

Pagella, C. (2019). Riflessi applicativi del principio di proporzione del trattamento sanzionatorio complessivamente irrogato per i fatti di market abuse e punibilità dell'insider di sé stesso: la Corte di Appello di Milano sul caso Cremonini. *Dir. pen. cont.* (dirittopenalecontemporaneo.it).

Piras, P. (2020). Il tortuoso cammino verso un'amministrazione nativa digitale. *Diritto dell'informazione e dell'Informatica*, fascicolo n. 1, 43.

Ponti, B. (2023). Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità. *Milano: Franco Angeli*.

Prenio, J., Broeders, D. (2019). Innovative technology in financial supervision (suptech) - the experience of early users. *FSI Insights on policy implementation*(9). Tratto da https://www.bis.org/fsi/publ/insights9.htm.

Proietti, G. (2023). Le definizioni di sistemi di intelligenza artificiale nelle proposte legislative europee. Un'analisi critica. *Dialoghi di diritto dell'economia*, 1-41.

Proietti, G. (2024). Definire l'indefinibile? I sistemi di intelligenza artificiale alla ricerca di un inquadramento sistematico. *Contratto e Impresa*(3), 882 ss.

Provenzano, P. (2020). Illecito amministrativo e retroattività "in bonam partem": da eccezione alla regola a regola generale. Banca borsa tit. cred., n. 1, 52 ss.

Puigpelat, O. (2023). The impact of the AI Act on public authorities and on administrative procedures. *CERIDAP*, n. 4, 238-252. doi:10.13130/2723-9195/2023-4-6

Rangone, N. (2022). Le pubbliche amministrazioni alla prova dell'intelligenza artificiale. In A.A.V.V., Liber Amicorum per Marco D'Alberti (p. 477 ss.). *Torino: G. Giappichelli Editore*.

Ravagnani, A., Deriu, P., Russo, A., Medda, F., Mazzarisi, P., Lillo, F. (2024). Dimensionality reduction techniques to support insider trading detection. *CONSOB Quaderni FinTech*, n. 12. Tratto da https://www.consob.it/documents/11973/4032571/fintech12.pdf/cc892fa7-816a-0da7-d2ec-8a26e64a6499

Rossa, S. (2021). Contributo allo studio delle funzioni amministrative digitali. *CEDAM*.

Ruggieri, F., Camaldo, L., De Amicis, G., Di Paolo, G., Marcolini, S., & Presacco, L. (2024). Artificial Intelligence Act: un primo sguardo al regolamento che verrà. *Cassazione penale*, n. 3, 1047- 1062.

Scoletta, M. (2019). Il ne bis in idem "preso sul serio": la Corte EDU sulla illegittimità del doppio binario francese in materia di abusi di mercato (e i possibili riflessi nell'ordinamento italiano). *Dir. pen. cont.* (dirittopenalecontemporaneo.it).

Seminara, S. (2020). L'informazione privilegiata Il testo unico finanziario. In M. Cera, & G. Presti (A cura di), Il testo unico finanziario (p. 2124 ss.). *Bologna: Zanichelli.*

Simoncini, A. (2019). L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà. *BioLaw Journal*, n. 1, 63 ss.

Sims, T. (2025, 06 02). German financial watchdog: AI is helping to catch market abuse. *Reuters.com*. Tratto da https://www.reuters.com/sustainability/boards-policy-regulation/german-financial-watchdog-ai-is-helping-catch-market-abuse-2025-06-02/

Stradella, E. (2018). I poteri normativi dell'esecutivo negli Stati Uniti: alcuni spunti ricostruttivi. *Rivista AIC*, 1-42.

Tiganò, V. (2020). L'estensione del principio costituzionale della retroattività favorevole in materia penale alle sanzioni amministrative punitive contro gli abusi di mercato. *Banca borsa tit. cred.*, n. 1, 62 ss.

Torchia, L. (2022). Lo Stato digitale e il diritto amministrativo. In AA.VV., Liber Amicorum per Marco D'Alberti (p. 477 ss.). *Giappichelli.*

Tripodi, A.F. (2018). Corte europea dei diritti dell'uomo e sistemi sanzionatori in materia di abusi di mercato e di violazioni tributarie: la quiete dopo la tempesta. *Le Società*, n. 1, 80 ss.

Turati, F. (s.d.). Atti del Parlamento italiano, Camera Dei Deputati, sess. 1904-1908, Legislatura XXII, 1° sessione, 2° tornata del 17 giugno 1908, Pres. Marcora, 22962.

Turing, A. (1950). Computing machinery and intelligence. *Mind: a Quarterly Review of Psychology and Philosophy*, VOL. LIX. NO. 236, 433 ss.

Ventoruzzo, M. (2014). Abusi di mercato sanzioni Consob e diritti umani: il caso Grande Stevens e altri c. Italia. *Riv. soc.*, n. 4, 693 ss.

Viganò, F. (2014). Doppio binario sanzionatorio e ne bis in idem: verso una diretta applicazione dell'art. 50 della Carta? *Dir. pen. cont.* (dirittopenalecontemporaneo.it), 219 ss.

Viganò, F. (2016). La Grande Camera della Corte di Strasburgo su ne bis in idem e doppio binario sanzionatorio. *Dir. pen. cont.* (dirit-topenalecontemporaneo.it).

Wang, P. (2019). On Defining Artificial Intelligence. *Journal of Artificial General Intelligence*, 1-37.

World Economic Forum (2017). Annual Report 2016-2017. Tratto da https://www3.weforum.org/docs/WEF_Annual_Report_2016_17.pdf

Riferimenti giurisprudenziali

Conseil Constitutionel, décision n. 2019-796 DC du 27 décembre 2019.

Consiglio di Stato, Ad. Plen., 2/04/2020, n. 10.

Consiglio di Stato, Sez. VI, Sent., 8/04/2019, n. 2270.

Consiglio di Stato, Sez. VI, Sent., 11/04/2017, n. 1692.

Consiglio di Stato, Sez. VI, Sent., 13/12/2019, n. 8472.

Consiglio di Stato, Sez. VI, Sent.,4/02/2020, n. 881.

Corte costituzionale, ord., 10/05/2019, n. 117

Corte costituzionale, sentenza, 16/06/2022, n. 149.

Corte costituzionale, sentenza, 30/04/2021, n. 84.

Corte costituzionale, sentenza 21/03/2019, n. 63.

Corte costituzionale, sentenza, 27/07/2011, n. 236.

Corte di Cassazione civ., Sez. I, Ord., 01/03/2023, n. 6177.

Corte di Cassazione civile, Sez. II, Ord., 16/02/2018, n. 3831.

Corte di Cassazione, II sez. civ., Sent., 9/08/2018 n. 20689.

Corte di Cassazione, Sez. II civile, Sent., 16/04/2018, n. 9254.

Corte di Cassazione, Sez. II civile, Sent., 31/05/2022, n. 17673.

Corte di Cassazione, Sez. Un., Sent., 09/03/2007, n. 5395.

Corte di giustizia UE, sentenza, 7/12/2023, cause riunite C-26/22 e C-64/22 e C-634/21.

Corte di giustizia UE, sentenza del 2/02/2021, DB c. Consob, C-481/19.

Corte di giustizia UE, sentenza, 20/03/2018, C-524/15, Menci.

Corte di giustizia UE, sentenza, 20/03/2018, Di Puma c. Consob, C-596/16 e C-597/16.

Corte di giustizia UE, sentenza, 20/03/2018, Garlsson Real Estate SA c. Consob, C-537/16.

Corte di giustizia UE, sentenza, 26/02/2013, Åkerberg Fransson, C-617/10.

Corte di giustizia UE, sentenza, 5/06/2012, Bonda, C-489/10.

Corte EDU, 8/06/1976, ric. n. 5100/71, Engel e altri c. Paesi Bassi.

Corte EDU, 4/03/2014, ric. n. 18640/2010, Grande Stevens ed altri c. Italia.

Corte EDU, 15/11/2016, ric. nn. 24130/11 e 29758/11, A. e B. c. Norvegia.

State v. Loomis (881 N.W.2d 749 (Wis. 2016).

T.A.R. Lazio Roma, Sez. III bis, Sent. 22/03/2017, n. 3769.

T.A.R. Lazio Roma, Sez. III bis, Sent. 10/09/2018, n. 9224.

T.A.R. Lazio Roma, Sez. III bis, Sent. 10/09/2018, n. 9227.

T.A.R. Lazio Roma, Sez. III bis, Sent. 10/09/2018, n. 9230.

T.A.R. Lazio Roma, Sez. III bis, Sent. 13/09/2019 n. 10964.

T.A.R. Lazio Roma, Sez. III bis, Sent. 13/09/2019 n. 10964.

T.A.R. Lazio Roma, Sez. III bis, Sent. 14/11/2019 n. 13069.

T.A.R. Lazio Roma, Sez. III bis, Sent. 27/05/2019, n. 6606.

Tribunale distrettuale dell'Aja, 5.02.2020, C-09-550982-HA ZA 18-388.

Quaderni FinTech

15 – agosto 2025
Riflessioni in tema di intelligenza artificiale e attività di vigilanza
P. Deriu, S. Racioppi; con presentazione a cura di A. Lalli

14 – luglio 2025
Greenwashing alert system for EU green bonds
The CONSOB–University of Trento prototype
S. Paterlini, A. Nicolodi, M. Gentile, V.F. Manzillo, M.R. Sancilio, P. Deriu

13 – luglio 2024
Il crowdinvesting made in Italy
Un'indagine conoscitiva
V. Caivano, C. Lucarelli, F.J. Mazzocchini, P. Soccorso

12 – febbraio 2024
Dimensionality reduction techniques to support insider trading detection
CONSOB - Scuola Normale Superiore di Pisa

11 – dicembre 2022
A machine learning approach to support decision in insider trading detection
CONSOB - Scuola Normale Superiore di Pisa

10 – luglio 2022
How Covid mobility restrictions modified the population of investors in Italian stock markets
CONSOB - Scuola Normale Superiore di Pisa

9 – giugno 2022
L'intelligenza artificiale nell'*asset* e nel *wealth management*
N. Linciano, V. Caivano, D. Costa, P. Soccorso, T.N. Poli, G. Trovatore; in collaborazione con Assogestioni

8 – aprile 2021
La portabilità dei dati in ambito finanziario
A cura di A. Genovese e V. Falce

7 – settembre 2020
Do investors rely on robots?
Evidence from an experimental study
B. Alemanni, A. Angelovski, D. Di Cagno, A. Galliera, N. Linciano, F. Marazzi, P. Soccorso

6 – dicembre 2019
Valore della consulenza finanziaria e *robo advice* nella percezione degli investitori
Evidenze da un'analisi qualitativa
M. Caratelli, C. Giannotti, N. Linciano, P. Soccorso

5 – luglio 2019

Marketplace lending

Verso nuove forme di intermediazione finanziaria?

A. Sciarrone Alibrandi, G. Borello, R. Ferretti, F. Lenoci, E. Macchiavello, F. Mattassoglio, F. Panisi

4 – marzo 2019

Financial Data Aggregation e Account Information Services

Questioni regolamentari e profili di business

A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano

3 – gennaio 2019

La digitalizzazione della consulenza in materia di investimenti finanziari

Gruppo di lavoro CONSOB, Scuola Superiore Sant'Anna di Pisa, Università Bocconi, Università di Pavia, Università di Roma 'Tor Vergata', Università di Verona

2 – dicembre 2018

Il FinTech e l'economia dei dati

Considerazioni su alcuni profili civilistici e penalistici

Le soluzioni del diritto vigente ai rischi per la clientela e gli operatori

E. Palmerini, G. Aiello, V. Cappelli G. Morgante, N. Amore, G. Di Vetta, G. Fiorinelli, M. Galli

1 – marzo 2018

Lo sviluppo del FinTech

Opportunità e rischi per l'industria finanziaria nell'era digitale

C. Schena, A. Tanda, C. Arlotta, G. Potenza