Andrea Carrisi

Intelligenza Artificiale, architetture di vigilanza e ipotesi di conflitto

L'approccio eurounitario sul tema della regolazione della vigilanza del mercato dell'intelligenza artificiale è caratterizzato dalla tendenza ad accentrare la supervisione con autorità specializzate, pur ammettendo a certe condizioni la designazione di quelle esistenti. Nel settore finanziario, viceversa, il regolamento europeo ritiene allo scopo naturale la designazione dell'autorità nazionale responsabile della vigilanza finanziaria, salvo decisioni in deroga supportate da specifiche circostanze.
Dopo un rapido sguardo sugli ordinamenti esteri, l'articolo si sofferma sull'ordinamento italiano, che con il DDL n. 1146/2024 – diversamente dall'impostazione europea – predilige un accentramento assoluto su AgID e ACN, senza attribuire alcun specifico rilievo all'autorità di vigilanza finanziaria nazionale. Tale scelta, in deroga a quanto stabilito dall'AI Act, solleva interrogativi sui confini di competenza e sulla necessità di un raccordo per garantire una vigilanza coerente ed efficace.

1 Geometria delle competenze della vigilanza. modello eurounitario e modello italiano

Tutela della democrazia, dello Stato di diritto e della sostenibilità ambientale nonché promozione dell'innovazione.

Questi, in estrema sintesi, gli obiettivi di tutela e promozione previsti dal Regolamento (UE) 2024/1689 (d'ora in avanti, anche *AI Act*), il quale stabilisce regole armonizzate sull'intelligenza artificiale, profilando – allo scopo e per quel che qui più interessa – un potere di vigilanza delle dinamiche del relativo mercato.

L'approccio eurounitario e, a cascata, dei singoli stati europei sul tema del controllo sull'intelligenza artificiale è caratterizzato dalla tendenza ad accentrare la supervisione dei diversi mercati con l'istituzione di autorità specifiche e specializzate e che esercitino la propria attività trasversalmente.

Accentramento, però, tendenziale e non assoluto: il regolamento non impone, infatti, l'istituzione di nuove autorità ma consente l'alternativa *designazione* di autorità esistenti. Sul punto l'art. 70, par. 1, *AI Act* prevede che ciascun Stato membro «*istituisce o designa*» come autorità nazionali competenti «*almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato*».

A riguardo, con tecnica normativa di rinvio, l'art. 74, par. 3, precisa che i sistemi di IA ad alto rischio collegati ai prodotti disciplinati dalla normativa di armonizzazione elencata nell'allegato I, sez. A (ad es. dispositivi di protezione individuale, apparecchi che bruciano carburanti gassosi, dispositivi medici, ecc.) sono soggetti alla vigilanza delle autorità responsabili per i relativi mercati, salva la possibilità per gli Stati – in determinate circostanze e purché sia garantito il coordinamento con l'autorità di mercato pertinente – di designare altra autorità.

Allo stesso modo, nel settore finanziario – con riguardo ai sistemi di IA ad alto rischio – le autorità di vigilanza finanziarie sono designate quali autorità competenti ai fini del controllo dell'attuazione della disciplina sull'IA (si v. art. 74, par. 6, primo comma, *AI Act*, secondo cui l'autorità di vigilanza è «*l'autorità nazionale pertinente responsabile della vigilanza finanziaria*»), salvo, anche in questo caso, che gli Stati membri decidano «*in deroga*» ai sensi del successivo par. 7, individuando «*un'altra autorità competente come autorità di vigilanza del mercato*» ma ciò soltanto «*in determinate circostanze e a condizione che sia garantito il coordinamento*».

La preferenza dell'estensione di competenza delle autorità di vigilanza finanziaria si fonda sul presupposto (cfr. considerando n. 158, *AI Act*) che la fornitura di servizi integrati con sistemi di IA non muta la disciplina finanziaria applicabile, in particolare con riguardo alle regole e ai requisiti in materia di *governance* interna e di gestione dei rischi. Da qui, l'*AI Act* – al fine di garantire la coerenza dell'applicazione e dell'esecuzione degli obblighi previsti dallo stesso regolamento e delle regole e dei requisiti in materia di servizi finanziari – attrae nella competenza delle autorità finanziarie anche gli aspetti riguardanti l'intelligenza artificiale.

Le autorità finanziarie dovrebbero allora disporre di tutti i poteri previsti dall'*AI Act* e dal regolamento (UE) 2019/1020 (regolamento sulla vigilanza del mercato e sulla conformità dei prodotti), compresi i poteri per svolgere attività di vigilanza del mercato *ex post*.

Tuttavia, anche in relazione al settore finanziario, l'idea di accen-

trare il controllo non esclude che gli Stati membri decidano diversamente, designando – come detto – un'altra autorità per svolgere i compiti di vigilanza del mercato.

La medesima geometria delle competenze di vigilanza non si riscontra nel DDL n. 1146/2024, nel quale l'accentramento è invece assoluto: l'art. 18 del disegno individua l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN) quali esclusive autorità (*rectius*, agenzie, che paiono ispirate non già al modello delle autorità indipendenti ma a quello degli organismi amministrativi) competenti per la vigilanza sul mercato dell'intelligenza artificiale.

In particolare:

a) l'AgID è responsabile della promozione dell'innovazione e dello sviluppo dell'intelligenza artificiale e provvede a definire le procedure e a esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale;

b) l'ACN, invece, è responsabile per la vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi di intelligenza artificiale; la stessa autorità nazionale è, altresì, responsabile per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza;

c) infine, le due autorità, AgID e ACN, ciascuna per quanto di rispettiva competenza, assicurano l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di intelligenza artificiale conformi alla normazione nazionale ed europea.

Il comma 2 dell'art. 18 prevede poi una forma di coordinamento e collaborazione «*nonché ogni opportuno raccordo*» (con l'istituzione del "Comitato di coordinamento") tra le autorità nazionali per l'intelligenza artificiale (AgID e ACN) e le altre pubbliche amministrazioni e le autorità indipendenti.

Dunque, l'architettura immaginata dal legislatore nazionale – accentrata su due agenzie nazionali trasversali – si discosta da quella progettata dal legislatore europeo, soprattutto con riguardo all'area finanziaria: non è prevista per le autorità finanziarie alcuna riserva di vigilanza sui sistemi di IA – nemmeno ad alto rischio – impiegati nel settore finanziario. Tanto avviene con la previsione di un raccordo, almeno di principio, con le altre autorità ma senza rappresentare alcuna delle "*determinate circostanze*" richieste dal Regolamento per consentire agli Stati di decidere in deroga rispetto a quanto stabilito dall'art. 74, par. 6, *AI Act*.

2 Vigilanza del mercato dell'IA negli ordinamenti esteri

Diversi ordinamenti esteri si son posti (e tutt'ora sono in corso discussioni e approfondimenti) il tema della vigilanza sul mercato dell'intelligenza artificiale, con diversità di metodi.

In tema, il Regno Unito ha adottato un approccio settoriale, affidando alle singole autorità esistenti il compito di vigilare l'integrazione dell'IA nelle diverse attività[145].

Secondo questo approccio, l'organismo di regolamentazione finanziaria *Financial Conduct Authority* (FCA) si occupa dell'utilizzo dell'IA nel contesto dei mercati finanziari, collaborando con le altre autorità: in particolare, per i dati l'ICO, *Information Commissioner's Office*, per la concorrenza la CMA, *Competition and Markets Authority,* e, infine, per le comunicazioni l'Ofcom, *Office of Communications*; collaborazione che si realizza nel contesto del *Digital Regulation Cooperation Forum*, DRCF[146], e avente ad oggetto lo scambio di informazioni e la risoluzione congiunta di questioni intersettoriali.

Nell'area nordamericana, è in corso di approvazione l'*Artificial Intelligence and Data Act* (AIDA, Bill C-27)[147], normativa con la quale il Canada intende regolare o vietare i fenomeni collegati all'utilizzo dell'intelligenza artificiale, segnatamente:

«*(a) to regulate international and interprovincial trade and commerce in artificial intelligence systems by establishing common requirements, applicable across Canada, for the design, development and use of those systems; and*

(b) to prohibit certain conduct in relation to artificial intelligence systems that may result in serious harm to individuals or harm to their interests».

L'AIDA propende per un modello accentrato, attribuendo la vigilanza del mercato dell'IA al Ministro competente (sez. 31, AIDA), con la possibilità di designare un funzionario di alto livello del ministero, l'"*Artificial Intelligence and Data Commissioner*", per assistere il ministro nell'applicazione dell'AIDA (cfr. sez. 33 (1): «*The Minister may designate a senior official of the department over which the Minister presides to be called the Artificial Intelligence and Data Commissioner, whose role is to assist the Minister in the administration and enforcement of this Part*»).

[145] Cfr. *AI Regulation: A Pro-innovation Approach*, in <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach>, 2023.

[146] Fca, *AI Update*, <https://www.fca.org.uk/publication/corporate/ai-update.pdf>, 2024.

[147] Consultabile su <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading>.

In questo modello, l'accentramento non soffre deroghe: la disciplina canadese non prevede disposizioni diverse applicabili all'utilizzo di sistemi di IA nel settore finanziario né in altri settori.

Ancora, nell'ordinamento brasiliano è in corso di approvazione una disciplina normativa (di cui al Bill No. 2338/2023[148]) che pare propendere per un modello di vigilanza accentrata: la competenza spetterebbe ad un organo della pubblica amministrazione (si v. l'art. 4, lett. V, secondo il quale è autorità competente un «*órgão ou entidade da Administração Pública Federal responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional*») che dovrà inoltre regolamentare l'utilizzo di sistemi di IA che comportino l'esposizione a rischi eccessivi (art. 16).

L'autorità competente, inoltre, dovrà coordinarsi con le altre autorità dei diversi settori economici al fine di esercitare i propri poteri (art. 32, lett. VII e, soprattutto, art. 34: «*A autoridade competente e os órgãos e entidades públicas responsáveis pela regulação de setores específicos da atividade econômica e governamental coordenarão suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento desta Lei. § 1º A autoridade competente manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as suas competências regulatória, fiscalizatória e sancionatória*»).

3 Ipotesi di conflitto nell'architettura di vigilanza italiana. Confini di competenza tra Agid, Acn e Consob

L'autorità europea di vigilanza dei mercati finanziari nel *Public statement On the use of Artificial Intelligence (AI) in the provision of retail investment services*[149] del maggio 2024 ha ricondotto i potenziali rischi derivanti dall'utilizzo delle tecnologie basate sull'IA in quattro categorie problematiche:

(i) eccessivo affidamento: il rischio che fornitori di servizi e clienti si affidino eccessivamente all'IA per il processo decisionale e trascurino l'importanza del giudizio umano;

(ii) mancanza di trasparenza e di comprensibilità o interpretabilità del sistema di IA: difetti di trasparenza, comprensibilità e interpreta-

[148] Consultabile su https://clairk.digitalpolicyalert.org/documents/brazil-bill-on-the-use-of-artificial-intelligence-2338-2023-original-language/raw

[149] Consultabile su <https://www.esma.europa.eu/document/public-statement-ai-and-investment-services>.

bilità dei sistemi di intelligenza artificiale pongono problemi di giustiziabilità delle scelte;

(iiii) mancanza di sicurezza e di privacy dei dati: raccolta, archiviazione ed elaborazione dei *big data* richiesti dagli strumenti di IA sollevano preoccupazioni in materia di privacy e sicurezza.

(iv) scarsa qualità dei dati di addestramento e mancanza di affidabilità dei risultati dell'IA: nella consulenza in materia di investimenti e nella prestazione del servizio di gestione del portafoglio, *bias* algoritmici e risultati errati possono condurre a consigli finanziari fuorvianti e all'assunzione di rischi imprevisti.

Presupposto questo panorama, con riferimento al modello di vigilanza immaginato dal disegno di legge nel nostro ordinamento, in particolare sul problema della ripartizione delle competenze, possono immaginarsi alcuni scenari di conflitto.

Si pensi ad un intermediario che implementi un sistema basato sull'intelligenza artificiale per la profilazione degli investitori e che tale IA analizzi grandi quantità di dati (età, reddito, investimenti pregressi, attività sui *social network*, ecc.) per la creazione di profili di rischio molto dettagliati. L'analisi dei dati o la progettazione dell'IA potrebbe essere causa di *bias* ("*algorithmic biases*", cfr. la citata dichiarazione di Esma) e configurare di conseguenza forme di discriminazione basate su tali fattori (ad es. persone anziane avverse al rischio e loro limitazione rispetto a prodotti più redditizi).

In casi come questo, l'Agenzia per l'Italia digitale e l'Agenzia per la cybersicurezza nazionale dovrebbero ritenersi competenti a valutare la conformità del sistema di IA ai requisiti di accuratezza, non discriminazione e trasparenza previsti dall'*AI Act* e a verificare se l'algoritmo di profilazione conduca a discriminazioni nonché se l'intermediario abbia adottato tutte le misure necessarie per mitigare i rischi di *bias*. D'altra parte, l'autorità di vigilanza finanziaria, Consob, è competente a vigilare sul rispetto della normativa in materia di profilazione degli investitori e di raccomandazione degli investimenti, in particolare in ordine al rispetto del criterio di adeguatezza; dunque, a verificare in concreto la proposta da parte dell'intermediario di prodotti finanziari adatti al profilo di rischio e agli obiettivi di investimento dei clienti.

Si pensi, ancora, ad un intermediario che implementi l'intelligenza artificiale per la gestione di fondi di investimento (selezione dei titoli, bilanciamento del portafoglio) e che addestri il sistema con dati sintetici[150].

[150] I dati sintetici sono dati generati mediante algoritmi di apprendimento automatico e che replicano le proprietà statistiche dei dati reali, preservando al contempo la privacy e

In questo caso, le autorità nazionali per l'intelligenza artificiale – AgID e ACN – sarebbero competenti a valutare la qualità del *dataset* sintetico utilizzato per addestrare l'IA e a verificare il rispetto dei requisiti di accuratezza, rappresentatività e non discriminazione. Le stesse autorità, inoltre, dovrebbero poter accertare l'adozione da parte dell'intermediario delle misure di monitoraggio e di aggiornamento dei dati. Spetterebbe, invece, a Consob la valutazione sull'adeguatezza del sistema di gestione del rischio e il rapporto tra utilizzo dei dati sintetici e compromissione della tutela degli investitori. Ancora, di competenza di Consob sarebbe anche la verifica sul rispetto delle regole di trasparenza e informativa nei confronti degli investitori in relazione all'utilizzo di dati sintetici e di forme di IA.

Infine, pur senza esaurire gli scenari ipotizzabili, è possibile immaginare (o meglio, è già noto) l'utilizzo dell'IA nel campo del *trading* ad alta frequenza per l'esecuzione di ordini ad elevatissime velocità al fine di identificare e sfruttare piccole inefficienze di prezzo. Si pensi a errori di progettazione *software* o al verificarsi di particolari scenari che comportino l'esecuzione da parte dell'intelligenza artificiale di una serie di ordini anomali; ordini che amplifichino un crollo improvviso del prezzo di un titolo azionario e determinino un c.d. *flash crash*.

Le agenzie previste dal DDL dovrebbero quindi valutare la conformità del sistema di IA ai requisiti di robustezza, affidabilità e sicurezza di cui all'*AI Act* e verificare se l'algoritmo sia stato progettato e testato adeguatamente per prevenire comportamenti anomali e per gestire situazioni di mercato estreme. Viceversa, Consob dovrebbe valutare se l'intermediario abbia tenuto comportamenti in violazione della disciplina sulla manipolazione del mercato e accertare l'adozione da parte dell'intermediario di misure di gestione del rischio e di prevenzione dei *flash crash*.

La rapida rassegna di casi di implementazione dell'intelligenza artificiale nei sistemi di investimento palesa possibili sovrapposizioni e potenziali conflitti di competenza tra le autorità di vigilanza finanziaria e le autorità di vigilanza del mercato dell'intelligenza artificiale; conflitti, quindi incertezze, che non aiutano nel procedimento di costruzione dell'affidabilità dell'intelligenza artificiale.

In assenza di – invece auspicabili – disposizioni in deroga per il settore finanziario rispetto all'accentramento della vigilanza sull'intelligenza artificiale, sembra quantomeno opportuno prevedere e prestabilire chiare modalità di cooperazione tra le diverse autorità settoriali, tra cui Consob, e le autorità nazionali per l'IA e, soprattutto, meccanismi di risoluzione dei

la riservatezza delle informazioni sensibili.

possibili conflitti di competenza, anche in relazione alla tutela di interessi ritenuti preminenti.